ITU Publications

Union internationale des télécommunications
Secteur du développement

Lignes directrices sur la protection en ligne des enfants à l'intention des décideurs

2020

Lignes directrices sur la protection en ligne des enfants à l'intention des décideurs

2020

Remerciements

Les présentes lignes directrices ont été élaborées par l'Union internationale des télécommunications (UIT) et un groupe de travail composé d'auteurs collaborateurs issus d'institutions de premier rang actives dans le secteur des technologies de l'information et de la communication (TIC) ainsi que dans les domaines concernant la protection (en ligne) des enfants. Parmi ces institutions figurent notamment:

ECPAT International, réseau Global Kids Online, Partenariat mondial visant à mettre fin à la violence à l'égard des enfants, projet HABLATAM, réseau Insafe pour des Centres Internet plus sûrs (Insafe), INTERPOL, Centre international pour les enfants disparus et exploités (ICMEC, *International Centre for Missing & Exploited Children*), International Disability Alliance, Union internationale des télécommunications (UIT), Fondation Internet Watch (IWF), London School of Economics, Bureau de la Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants et Rapporteuse spéciale sur la vente et l'exploitation sexuelle d'enfants, Privately SA, RNW Media, Centres Internet plus sûrs du Royaume-Uni (*UK Safer Internet Centres*), Alliance mondiale WePROTECT et Fondation World Childhood USA.

Le groupe de travail était placé sous la présidence de M. David Wright (*UK Safer Internet Centres/ SWGfL*) et la coordination de Mme Fanny Rotino (UIT).

Les présentes lignes directrices n'auraient pas vu le jour sans la disponibilité, l'enthousiasme et le dévouement des auteurs contributeurs. De précieuses contributions ont aussi été reçues des entités suivantes: COFACE-Families Europe, Conseil de l'Europe, Commissaire australien à la sécurité en ligne (*Australian eSafety Commissioner*), Commission européenne, Groupe e-Worldwide (e-WWG), Organisation de coopération et de développement économiques (OCDE), et Youth and Media du Berkman Klein Center for Internet & Society de l'Université d'Harvard. Des gouvernements nationaux et des acteurs du secteur privé qui ont tous pour objectif de faire de l'Internet un endroit meilleur et plus sûr pour les enfants et les jeunes ont également apporté leur contribution.

L'UIT remercie les partenaires énumérés ci-dessous (par ordre alphabétique) pour leur précieuse contribution en temps et en réflexion.

- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Conseil de l'Europe)
- John Carr (ECPAT International)
- Julia Fossi et Ella Serry (Commissaire à la sécurité en ligne)
- Manuela Marta (Commission européenne)
- Salma Abbasi (e-WWG)
- Amy Crocker et Serena Tommasino (Partenariat mondial visant à mettre fin à la violence à l'égard des enfants)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Insafe)[1]

[1] *Dans le cadre du programme Connecting Europe Facility (CEF), le réseau European Schoolnet s'occupe, pour le compte de la Commission européenne, de la plate-forme Better Internet for Kids, et notamment de la coordination du réseau Insafe des Centres Internet plus sûrs. De plus amples renseignements sont disponibles à l'adresse* www.betterinternetforkids.eu.

- Lucy Richardson (International Disability Alliance)
- Matthew Dompier (INTERPOL)
- Fanny Rotino (UIT)
- Tess Leyland (IWF)
- Sonia Livingstone (London School of Economics et Global Kids Online)
- Elettra Ronchi (OCDE)
- Manus De Barra (Bureau de la Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants)
- Deepak Tewari (Privately SA)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (Rapporteuse spéciale des Nations Unies sur la vente et l'exploitation sexuelle d'enfants)
- David Wright (UK Safer Internet Centres/SWGfL)
- Iain Drennan et Susannah Richmond (Alliance mondiale WePROTECT)
- Lina Fernandez et Joanna Rubinstein (Fondation World Childhood USA)
- Sandra Cortesi (Youth and Media)

ISBN

978-92-61-30122-4 (version papier)

978-92-61-30452-2 (version électronique)

978-92-61-30112-5 (version EPUB)

978-92-61-30462-1 (version MOBI)

Avant d'imprimer ce rapport, pensez à l'environnement.

Avant-propos

Dans un monde où l'Internet est présent dans presque tous les aspects de la vie moderne, il est devenu de plus en plus urgent pour chaque pays d'assurer la sécurité des jeunes utilisateurs en ligne.

L'UIT a élaboré son tout premier ensemble de lignes directrices sur la protection en ligne des enfants en 2009. Depuis lors, l'Internet a évolué au-delà de l'imaginable. L'Internet est devenu une ressource ludique et didactique infiniment plus riche pour les enfants, mais il est également devenu un environnement beaucoup plus dangereux pour eux, où ils ne peuvent s'aventurer sans être accompagnés.

Les nombreux risques auxquels les enfants sont exposés comprennent les atteintes à la vie privée et l'accès à des contenus violents et inappropriés, le piratage en ligne et la menace de la manipulation psychologique à des fins sexuelles (*grooming*), ainsi que les abus sexuels et l'exploitation sexuelle. Les menaces se multiplient et les auteurs agissent de plus en plus souvent en même temps sur des "cyberterritoires" relevant de nombreuses juridictions différentes, ce qui limite l'efficacité des interventions et des recours déployés au niveau national.

En outre, la pandémie mondiale de COVID-19 a entraîné une augmentation du nombre d'enfants utilisant l'Internet pour la première fois, afin de poursuivre leur scolarité et de maintenir des liens sociaux. Les contraintes imposées par le virus se sont traduites non seulement par le fait que nombre de jeunes enfants ont commencé à interagir en ligne bien plus tôt que leurs parents ne l'avaient prévu, mais aussi par l'impossibilité des parents de surveiller leurs enfants du fait de leurs obligations professionnelles, exposant ainsi les plus jeunes au risque d'accéder à des contenus inappropriés ou d'être pris pour cible par des agresseurs pour la production de matériel montrant des abus sexuels sur des enfants.

Aujourd'hui plus que jamais, une action collaborative et coordonnée au niveau international est nécessaire pour assurer la sécurité des enfants en ligne, avec la participation active et l'appui d'un large éventail de parties prenantes, qu'il s'agisse des acteurs du secteur des télécommunications, notamment les plates-formes du secteur privé, les fournisseurs de services et les opérateurs de réseau, des gouvernements ou de la société civile.

Partant de ce constat, les États Membres de l'UIT avaient demandé en 2018 que l'on ne se contente pas de mettre à jour régulièrement les lignes directrices sur la protection en ligne des enfants, comme pour les versions précédentes. Au lieu de cela, cette nouvelle édition est une version entièrement repensée, réécrite et remaniée des lignes directrices afin de tenir compte des transformations majeures qui ont redéfini les contours de l'environnement numérique dans lequel évoluent les enfants.

Cette nouvelle édition aborde les évolutions récentes des technologies et plates-formes numériques, mais comble également une lacune de taille en traitant de la situation des enfants handicapés, pour qui l'Internet constitue un moyen essentiel de participer, et de s'intégrer, pleinement à la société. Les besoins particuliers des enfants migrants et des enfants issus d'autres groupes vulnérables ont également été pris en considération.

Nous espérons que ces lignes directrices constitueront pour les décideurs une base solide pour la définition de stratégies nationales inclusives et multipartites, notamment en menant des consultations ouvertes et en dialoguant avec les enfants, afin d'élaborer des mesures mieux ciblées et des actions plus efficaces.

Lors de l'élaboration de ces nouvelles lignes directrices, l'UIT et ses partenaires se sont efforcés de concevoir un cadre souple, adaptable et facilement exploitable, en s'appuyant sur des normes internationales et des objectifs communs, en particulier la Convention relative aux droits de l'enfant et les Objectifs de développement durable (ODD) fixés par les Nations Unies. Conformément à l'esprit de l'UIT et à son rôle en tant qu'organisation internationale, je suis fière de pouvoir dire que ces lignes directrices révisées sont le fruit d'une collaboration mondiale, puisqu'elles ont été corédigées par des experts du monde entier provenant d'une vaste communauté multi-parties prenantes.

Je me réjouis également de vous présenter notre nouvelle mascotte de la protection en ligne des enfants: Sango, un personnage sympathique, qui aime s'amuser et qui n'a peur de rien, conçu entièrement par un groupe d'enfants dans le cadre du nouveau programme international de l'UIT pour la sensibilisation des jeunes.

À une période où de plus en plus de jeunes rejoignent la communauté en ligne, ces lignes directrices revêtent plus d'importance que jamais. Les décideurs, les acteurs du secteur privé, les parents et les éducateurs – sans parler des enfants eux-mêmes – ont tous un rôle crucial à jouer. Je suis reconnaissante, comme toujours, de votre soutien, et je me réjouis que notre collaboration étroite se poursuive sur cette question d'une importance majeure.

Doreen Bogdan-Martin
Directrice, Bureau de développement des télécommunications

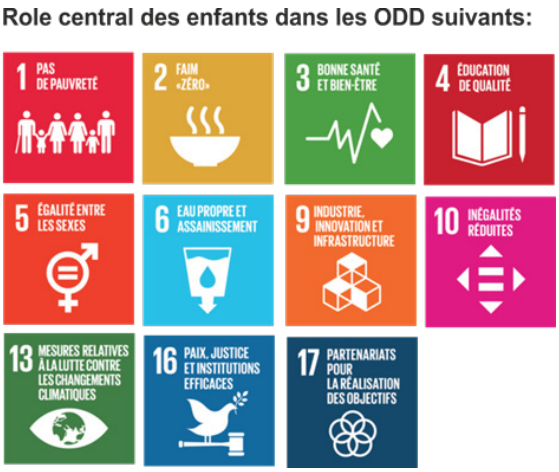
Préface

Il y a trente ans, la quasi-totalité des gouvernements se sont engagés à respecter, à protéger et à promouvoir les droits de l'enfant. La Convention des Nations Unies relative aux droits de l'enfant est le traité international relatif aux droits de l'homme le plus largement ratifié de l'histoire. Bien que des progrès notables aient été accomplis ces trois dernières décennies, des difficultés considérables subsistent et les enfants sont désormais exposés à des risques inédits.

En 2015, tous les pays ont renouvelé leur engagement en faveur des enfants dans le cadre du Programme de développement durable à l'horizon 2030 et des 17 Objectifs de développement durable (ODD) de portée universelle. À titre d'exemple, l'Objectif 16.2 vise à mettre un terme, d'ici à 2030, à la maltraitance, à l'exploitation et à toutes les formes de violence et de torture dont sont victimes les enfants. La protection des enfants est un dénominateur commun de 11 ODD sur 17. L'UNICEF met les enfants au cœur du Programme 2030, comme l'illustre la Figure 1.

Figure 1: Les enfants, les TIC et les ODD

#ICT4SDG



Dans le Programme de développement durable à l'horizon 2030, il est reconnu que les technologies de l'information et de la communication (TIC) peuvent jouer un rôle essentiel dans la réalisation des ODD. L'expansion des TIC et l'interdépendance mondiale des activités peuvent contribuer à accélérer les progrès de l'humanité, à réduire la fracture numérique et à donner naissance à des sociétés du savoir. Le programme définit en outre des cibles spécifiques pour l'utilisation des TIC au service du développement durable s'agissant de l'éducation (Objectif 4), de l'égalité entre les sexes (Objectif 5), de l'infrastructure (Objectif 9 – accès universel et financièrement abordable à l'Internet) et des partenariats et des moyens de mise en œuvre (Objectif 17)[1]. Les TIC ont le potentiel de transformer profondément l'économie tout entière, en jouant un rôle moteur dans la réalisation de chacun des 17 ODD. Les TIC ont déjà apporté leur pierre à l'édifice en donnant à des milliards de personnes partout dans le monde les moyens dont ils ont besoin – en leur donnant accès à des ressources éducatives et aux soins de santé, ainsi qu'à des services comme l'administration publique en ligne et les réseaux sociaux, entre autres.

[1] PNUD, Objectifs de développement durable | PNUD, undp.org, page consultée le 24 juin 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals.html; Houlin Zhao, "Le rôle fondamental des TIC dans la réalisation des ODD", *UIT,* Revue "Nouvelles de l'UIT", 48, page consultée le 24 juin 2020, https://www.itu.int/en/itunews/Documents/2017/2017-03/2017_ITUNews03-en.pdf.

L'essor spectaculaire des technologies de l'information et de la communication a créé des possibilités sans précédent pour les enfants et les jeunes de communiquer, de se connecter, d'échanger, d'apprendre, d'accéder aux informations et d'exprimer leurs opinions sur des thèmes qui ont des incidences sur leur quotidien et sur celui de leur communauté.

Cependant, un accès plus large et plus facile à l'Internet et à la technologie mobile s'accompagne aussi de défis importants pour la sécurité et le bien-être des enfants – tant dans le monde réel que dans le monde virtuel.

Pour réduire les risques que comporte le monde numérique et, dans le même temps, permettre à de plus en plus d'enfants et de jeunes de tirer parti des avantages qu'il offre, les gouvernements, la société civile, les communautés locales, les organisations internationales et les entreprises doivent agir de concert pour servir un même objectif. En particulier, les décideurs ont un rôle essentiel à jouer afin d'atteindre un objectif international: assurer la protection en ligne des enfants.

En vue de relever les défis que pose le développement rapide des TIC et de résoudre les problèmes qui en découlent en matière de protection des enfants, l'UIT a lancé en novembre 2008 l'initiative sur la protection en ligne des enfants (COP). Cette initiative internationale multi-parties prenantes vise à réunir des partenaires de tous les secteurs, à l'échelle mondiale, pour donner aux enfants du monde entier les moyens de naviguer en toute sécurité sur l'Internet.

En outre, la Conférence de plénipotentiaires de l'UIT tenue à Dubaï en 2018 a réaffirmé l'importance de l'initiative sur la protection en ligne des enfants, en reconnaissant qu'elle constitue un moyen de sensibiliser davantage l'opinion à ce thème, d'échanger les bonnes pratiques en la matière et de fournir une assistance et un appui aux États Membres, en particulier les pays en développement, dans l'élaboration et la mise en œuvre de feuilles de route sur la protection en ligne des enfants. La Conférence a également reconnu combien il est important d'assurer la protection en ligne des enfants, dans le cadre de la Convention des Nations Unies relative aux droits de l'enfant et d'autres traités relatifs aux droits de l'homme, en encourageant la collaboration entre toutes les parties prenantes qui contribuent à assurer la protection en ligne des enfants.

La Conférence a reconnu le Programme de développement durable à l'horizon 2030, qui aborde plusieurs aspects de la protection en ligne des enfants dans les ODD, en particulier les ODD 1, 3, 4, 5, 9, 10 et 16. Elle a en outre reconnu la Résolution 175 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires, concernant l'accessibilité des télécommunications/TIC pour les personnes handicapées, y compris les personnes ayant des besoins particuliers, et la Résolution 67 (Rév.Buenos Aires, 2017) de la Conférence mondiale de développement des télécommunications (CMDT), sur le rôle du Secteur du développement des télécommunications de l'UIT (UIT-D) dans la protection en ligne des enfants.

Fin 2019, la Commission UIT/UNESCO sur le large bande au service du développement durable a publié le Rapport sur la protection en ligne des enfants, qui contient des recommandations concrètes sur la manière de rendre l'Internet plus sûr pour les enfants.

En 2009, l'UIT a publié le premier ensemble de lignes directrices sur la protection en ligne des enfants, dans le cadre de l'initiative sur la protection en ligne des enfants. Au cours de la dernière décennie, ces lignes directrices ont été traduites dans de nombreuses langues et utilisées par un grand nombre de pays dans le monde, servant ainsi de référence pour l'élaboration de feuilles de route et de stratégies nationales sur la protection en ligne des enfants. Des organismes nationaux, des organisations de la société civile, des établissements accueillant des enfants,

des entités du secteur privé et de nombreuses autres parties prenantes s'en sont inspirés dans le cadre des efforts mobilisés pour assurer la protection en ligne des enfants.

En particulier, ces lignes directrices ont été utilisées en vue de la rédaction, de l'élaboration et de la mise en œuvre de stratégies nationales de protection en ligne des enfants dans de nombreux États Membres, à l'instar des pays suivants: Cameroun, Gabon, Gambie, Ghana, Kenya, Ouganda, Sierra Leone et Zambie (dans la région Afrique); Bahreïn et Oman (dans la région des États arabes); Brunéi Darussalam, Cambodge, Kiribati, Indonésie, Malaisie, Myanmar et Vanuatu (dans la région Asie-Pacifique); et Bosnie-Herzégovine, Géorgie, Moldova, Monténégro, Pologne et Ukraine (dans la région Europe).

De plus, ces lignes directrices ont préparé le terrain pour l'organisation de manifestations régionales, comme la Conférence régionale sur la protection en ligne des enfants (ACOP) placée sous le thème "Autonomisation des citoyens numériques de demain" et organisée à Kampala (Ouganda) en 2014, et la Conférence régionale de l'ASEAN sur la protection en ligne des enfants organisée en 2020 à Bangkok (Thaïlande).

En vertu de la Résolution 179 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires, l'UIT, en collaboration avec les partenaires et les parties prenantes de l'initiative sur la protection en ligne des enfants, ont été chargés d'actualiser les quatre ensembles de lignes directrices, en tenant compte de l'évolution technique du secteur des télécommunications, y compris les lignes directrices concernant les enfants handicapés et les enfants ayant des besoins particuliers.

En conséquence, les présentes lignes directrices, qui ont été largement mises à jour et revues par des spécialistes et les parties prenantes compétentes, offrent un vaste ensemble de recommandations pour assurer la protection des enfants dans le monde numérique. Elles sont le fruit d'une collaboration multi-parties prenantes et mettent à profit le savoir, l'expérience et les compétences spécialisées de nombreuses organisations et personnalités du monde entier œuvrant dans le domaine de la protection en ligne des enfants. Elles visent à poser les jalons d'un monde virtuel plus sûr et plus sécurisé pour les générations à venir, et sont destinées à servir de prototype qui pourra être adapté et utilisé conformément aux lois et aux coutumes nationales ou locales. De plus, ces lignes directrices abordent des questions qui concernent tous les enfants et tous les adolescents de moins de 18 ans, compte tenu des besoins propres à chaque tranche d'âge. Elles visent en outre à répondre aux besoins des enfants, quelles que soient leurs conditions de vie, ainsi que des enfants ayant des besoins particuliers et des enfants handicapés. Ces lignes directrices permettent également de renforcer le champ d'application de la protection en ligne des enfants, en ce qu'elles prennent en compte tous les risques, toutes les menaces et tous les dangers que les enfants peuvent rencontrer en ligne, et recherchent le juste équilibre avec les bienfaits que le monde numérique peut apporter au quotidien des enfants.

Nous espérons non seulement que les présentes lignes directrices favoriseront l'édification d'une société de l'information plus inclusive, mais aussi qu'elles permettront aux États Membres de l'UIT de satisfaire aux obligations souscrites pour protéger et réaliser les droits des enfants tels qu'ils sont énoncés dans la Convention des Nations Unies relative aux droits de l'enfant[2], adoptée par l'Assemblée générale des Nations Unies aux termes de sa Résolution 44/25 du 20 novembre 1989, et dans le Document final du Sommet mondial sur la société de l'information (SMSI)[3].

Par la publication des présentes lignes directrices, l'initiative sur la protection en ligne des enfants appelle toutes les parties prenantes à mettre en œuvre des politiques et des stratégies qui protègeront les enfants dans le cyberespace et à promouvoir un accès en toute sécurité à toutes les possibilités extraordinaires qui sont offertes en ligne.

---

2 UNICEF, "Convention sur les droits de l'enfant", unicef.org, page consultée le 24 juin 2020, https://www.unicef.org/fr/convention-droits-enfant.

3 Cette édition du SMSI s'est tenue en deux phases: à Genève (10-12 décembre 2003) et à Tunis (16-18 novembre 2005). Elle s'est conclue par un engagement ambitieux, à savoir celui "d'édifier une société à dimension humaine, inclusive et privilégiant le développement, une société de l'information, dans laquelle chacun [a] la possibilité de créer, d'obtenir, d'utiliser et de partager l'information et le savoir".

Table des matières

Liste des tableaux, des figures et des encadrés

Tableaux

Figures

Encadrés

1 Tour d'horizon du document

1.1 Objectif

Les gouvernements nationaux ont une obligation d'assurer la protection des enfants, tant dans le monde réel que dans le monde virtuel. D'une certaine façon, étant donné que les nouvelles technologies font partie intégrante de la vie d'un très grand nombre d'enfants et de jeunes, de diverses manières importantes, la distinction rigide entre les événements du monde réel et les événements du monde virtuel n'a plus lieu d'être, les deux étant aujourd'hui de plus en plus imbriqués et interdépendants.

Les décideurs[1] et toutes les autres parties prenantes concernées ont un rôle particulièrement important à jouer. Au vu de la vitesse à laquelle les technologies évoluent, bon nombre de méthodes traditionnelles d'élaboration des politiques ne sont plus pertinentes. Les décideurs sont appelés à élaborer un cadre juridique souple, inclusif et en adéquation avec sa mission, compte tenu de l'évolution rapide du monde numérique, afin d'assurer la protection en ligne des enfants.

Les présentes lignes directrices visent à offrir aux décideurs des États Membres de l'UIT un cadre accessible et souple, pour comprendre et remplir leur obligation juridique d'assurer la protection des enfants, dans le monde réel – et physique – et le monde virtuel.

Pour ce faire, les lignes directrices traitent de plusieurs questions importantes pour les décideurs:

1) Qu'est-ce que la protection en ligne des enfants?
2) Pourquoi, en tant que décideur, dois-je me soucier de la protection en ligne des enfants?
3) Quel est le contexte juridique, socio-politique et de développement de mon pays?
4) Comment les décideurs devraient-ils commencer à envisager et à concevoir une stratégie efficace et durable en matière de protection en ligne des enfants dans leur pays?

Ce faisant, les lignes directrices s'inspirent des modèles, des cadres et des ressources existants pour offrir un cadre et un aperçu des bonnes pratiques appliquées dans le monde.

1.2 Champ d'application

Le champ d'application de la protection en ligne des enfants s'étend à tout danger auquel les enfants sont exposés en ligne, couvrant ainsi un large éventail de risques qui constituent une menace pour la sécurité et le bien-être des enfants. Il s'agit d'un défi complexe qui doit être abordé sous différents aspects, notamment sous l'angle de la législation, de la gouvernance, de l'éducation, de la politique et de la société.

De plus, la protection en ligne des enfants doit se fonder sur une compréhension des risques, des menaces et des dangers, tant généraux que propres à un pays, auxquels les enfants sont confrontés dans le cyberespace. Pour ce faire, il faut formuler des définitions claires et établir des paramètres précis à des fins d'intervention, pour prendre en compte et distinguer les actes qui constituent un crime et les actes qui, même s'ils ne sont pas illégaux, constituent néanmoins une menace pour le bien-être d'un enfant.

[1] Dans le présent document, on entend par "décideurs" toutes les parties prenantes qui sont chargées d'élaborer et de mettre en œuvre des politiques, en particulier au sein d'un gouvernement.

À cette fin, les présentes lignes directrices offrent un aperçu des menaces et des dangers auxquels les enfants sont exposés dans le cyberespace aujourd'hui. Cela étant dit, force est de constater que les délais nécessaires à l'élaboration de politiques et les méthodes traditionnelles utilisées ne permettent pas de suivre le rythme effréné auquel la technologie et son lot de menaces et de dangers évoluent actuellement. À l'ère du numérique, les décideurs doivent édifier des cadres juridiques et politiques suffisamment souples et inclusifs pour résoudre les problèmes existants et, dans la mesure du possible, anticiper les défis qui se feront jour. Pour ce faire, il est nécessaire de travailler en collaboration avec chacune des parties prenantes, y compris le secteur des TIC, la communauté des chercheurs, la société civile, le grand public et les enfants eux-mêmes. Ce processus peut être étayé par l'examen des principes fondamentaux de la protection en ligne des enfants.

1.3 Principes fondamentaux

Nous avons défini onze principes transversaux qui, ensemble, contribueront à élaborer une stratégie nationale de protection en ligne des enfants globale et tournée vers l'avenir.

Ces principes sont énumérés suivant un lien logique et non par ordre d'importance.

Une stratégie de protection en ligne des enfants devrait:

1) reposer sur une vision globale intégrant le secteur public, le secteur privé et la société;
2) découler d'une compréhension et d'une analyse transversales de l'environnement numérique dans son ensemble, tout en étant adaptée à la situation d'un pays et à ses priorités;
3) respecter les droits fondamentaux des enfants, tels qu'énoncés dans la Convention des Nations Unies relative aux droits de l'enfant et d'autres conventions et lois internationales essentielles, et être compatible avec ces droits;
4) respecter les lois et les stratégies nationales existantes, similaires et associées qui sont en vigueur, telles que les lois sur la maltraitance faite aux enfants ou les stratégies sur la sécurité des enfants, et être compatible avec ces lois et ces stratégies;
5) respecter les droits et les libertés civils des enfants, qui ne doivent pas être sacrifiés au profit de la protection des enfants;
6) être élaborée moyennant la participation active de toutes les parties prenantes concernées, y compris les enfants, afin de tenir compte de leurs besoins et de leurs responsabilités, et de répondre aux besoins des minorités et des groupes marginalisés;
7) être conçue de façon à s'aligner sur les programmes plus vastes des gouvernements visant la prospérité économique et sociale, et renforcer autant que possible la contribution des TIC au développement durable et à l'inclusion sociale;
8) recourir aux instruments politiques les plus adaptés à disposition pour réaliser son objectif, compte tenu des conditions propres au pays concerné;
9) être établie au plus haut niveau des pouvoirs publics, qui seront chargés d'assigner les rôles et les responsabilités pertinents et d'attribuer des ressources humaines et des ressources financières suffisantes;
10) contribuer à édifier un environnement numérique digne dans lequel les enfants, les parents/personnes s'occupant d'enfants et les parties prenantes peuvent avoir confiance;
11) orienter les efforts déployés par les parties prenantes pour autonomiser et doter les enfants des compétences numériques nécessaires pour qu'ils puissent se protéger en ligne.

1.4 Utilisation des présentes lignes directrices

Les présentes lignes directrices tiennent compte des éléments de recherche pertinents ainsi que des modèles et des supports existants, et fournissent des recommandations claires en vue de l'élaboration d'une stratégie nationale en matière de protection en ligne des enfants.

- La Section 2 présente la protection en ligne des enfants et donne une vue d'ensemble des travaux de recherche menés récemment, y compris des aspects relatifs aux technologies nouvelles et émergentes, et aux principales menaces et aux principaux dangers pour les enfants.
- La Section 3 définit les modalités de préparation d'une stratégie nationale en matière de protection en ligne des enfants, y compris les parties prenantes concernées, les exemples existants de mesures prises en réponse aux menaces et aux dangers en ligne et les avantages de disposer d'une stratégie nationale.
- La Section 4 porte sur les recommandations relatives aux cadres et à la mise en œuvre.
- La Section 5 donne un aperçu des listes de vérification nationales pour l'élaboration d'une stratégie nationale en matière de protection en ligne des enfants.
- La Section 6 répertorie les documents de référence utiles.

2 Introduction

En 2019, plus de la moitié de la population mondiale utilisait l'Internet. Le premier groupe d'internautes est composé des moins de 44 ans, avec une utilisation tout aussi élevée chez les 16 à 24 ans que chez les 35 à 44 ans. Au niveau mondial, un enfant sur trois utilise l'Internet (0-18 ans)[2]. Dans les pays en développement, les enfants et les jeunes sont les premiers utilisateurs de l'Internet[3], et selon les estimations, leur nombre sera multiplié par deux au cours des cinq prochaines années. Aujourd'hui, les nouvelles générations grandissent avec l'Internet et la plupart des jeunes se connectent via la technologie de réseau mobile, en particulier dans les pays du Sud[4].

Bien que l'accès à l'Internet soit fondamental pour la réalisation des droits des enfants, des disparités d'accès subsistent, notamment aux niveaux régional et national, ainsi qu'entre les hommes et les femmes, limitant ainsi les perspectives pour les jeunes filles, les enfants handicapés, les enfants issus des minorités et d'autres groupes vulnérables. Concernant la fracture numérique entre les hommes et les femmes, les travaux de recherche montrent que dans toutes les régions, hormis aux États-Unis d'Amérique, le nombre d'internautes hommes dépasse largement celui d'internautes femmes. Dans de nombreux pays, les filles ne bénéficient pas des mêmes possibilités d'accès que les garçons, et lorsque c'est le cas, leur utilisation de l'Internet est beaucoup plus surveillée et limitée, et leur sécurité peut être menacée lorsqu'elles

[2] OCDE, "New Technologies and 21st Century Children: Recent Trends and Outcomes" (Nouvelles technologies et enfants du XXIe siècle: Tendances et résultats récents), Document de travail de l'OCDE sur l'éducation, numéro 179 (Direction de l'éducation et des compétences, OCDE), page consultée le 24 juin 2020, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En.

[3] Ofcom, "Children and Parents: Media Use and Attitudes Report 2018" (Enfants et parents: Rapport 2018 sur l'utilisation des médias et les comportements), page consultée le 24 juin 2020, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf.

[4] UIT, "Rapport – Mesurer la société de l'information", page consultée le 24 juin 2020, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

essaient d'accéder à l'Internet[5]. À l'évidence, les enfants et les jeunes qui ne possèdent pas de compétences numériques ou qui parlent des langues minoritaires ne peuvent pas trouver facilement de contenus pertinents en ligne, et les enfants issus des zones rurales maîtrisent moins les outils numériques, passent plus de temps en ligne (en particulier pour jouer) et sont moins encadrés et surveillés par leurs parents[6].

Toutefois, on ne peut débattre des risques et des menaces sans reconnaître le caractère particulièrement enrichissant et édifiant de la technologie numérique. L'Internet et les technologies numériques sont en train de révolutionner nos modes de vie et ont ouvert un large éventail de nouvelles manières de communiquer, jouer à des jeux, écouter de la musique et effectuer toutes sortes d'activités culturelles, éducatives ou de perfectionnement des compétences. L'Internet peut offrir un accès essentiel à la santé et aux services éducatifs, ainsi qu'aux informations sur des sujets qui sont importants pour les jeunes, mais qui peuvent être tabous dans la société dans laquelle ils vivent.

Les enfants et les jeunes comptent souvent parmi les premiers à adopter les nouvelles possibilités offertes par l'Internet et à s'y adapter et, en tant que tels, ils sont également exposés à divers problèmes affectant leur sécurité et leur bien-être, que la société a le devoir de reconnaître et de résoudre. Il est important de discuter ouvertement avec les enfants et les jeunes des risques auxquels ils sont confrontés en ligne.

La discussion donne naissance à un cadre où les enfants et les jeunes peuvent apprendre comment reconnaître les risques, éviter ou affronter les dangers s'ils en rencontraient, et connaître les bienfaits et les possibilités qu'offre l'Internet.

Dans de nombreuses régions du monde, les jeunes ont une bonne compréhension de certains des risques auxquels ils sont exposés en ligne[7, 8]. À titre d'exemple, il ressort des travaux de recherche que la majorité des enfants et des jeunes sont en mesure de distinguer le cyberharcèlement des plaisanteries ou des vexations en ligne. Bien qu'ils soient conscients que le cyberharcèlement revêt une dimension publique et qu'il vise à nuire, réussir à trouver un juste équilibre pour qu'un enfant puisse profiter de toutes les possibilités et les risques qu'un enfant peut rencontrer en ligne reste une gageure[9].

Pour les États Membres de l'UIT, assurer la protection en ligne des enfants et des jeunes reste une priorité, qu'il faut équilibrer soigneusement avec des mesures visant à promouvoir les

---

5 GAGE, "Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income Countries" (Les adolescents et les médias numériques: utilisations, risques et perspectives dans les pays à revenu faible et à revenu intermédiaire), page consultée le 24 juin 2020, https://www.gage.odi.org/publication/digital-media-risks-opportunities/.

6 Livingstone, S., Kardefelt Winther, D., et Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report* (Rapport comparatif de Global Kids Online, Rapport de recherche du Centre Innocenti), Centre de recherche de l'UNICEF – Innocenti, Florence, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html. Les résultats observés peuvent être surprenants. À titre d'exemple, les recherches effectuées par le projet HABLATAM dans cinq pays d'Amérique latine ont montré qu'au sein des communautés vulnérables, les enfants peuvent utiliser des plates-formes de rencontre, des sites de jeux vidéo et des réseaux sociaux pour réaliser des transactions financières à des fins illégales. Réseau Conectados al Sur, "Hablatam", Projet Hablatam 2020, page consultée le 24 juin 2020, https://hablatam.net/.

7 Depuis 2016, l'UIT organise des consultations sur le thème de la protection en ligne des enfants, avec des parties prenantes représentant des enfants et des adultes, sur des questions importantes telles que le cyberharcèlement, la maîtrise des outils numériques et les activités des enfants en ligne.

8 UIT, Consultation avec les jeunes, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.

9 UNICEF, "Global Kids Online Comparative Report (2019)."

possibilités en ligne pour les enfants et les jeunes[10], et qu'il faut assumer de façon à protéger les enfants et les jeunes, sans pour autant nuire à leur accès ou à l'accès du grand public à l'information, ou à la capacité des individus d'exercer leur liberté de parole, d'expression et d'association.

À l'évidence, des investissements spécifiques et des solutions originales sont nécessaires pour affronter les risques auxquels les enfants et les jeunes sont exposés, notamment en raison de la fracture numérique entre les enfants et les adultes, qui limite la capacité des parents, des enseignants et des tuteurs à prodiguer des conseils. Dans le même temps, alors que les enfants et les adolescents grandissent et deviennent à leur tour des adultes, des parents et des membres actifs de la société, ils ont la possibilité – inouïe et immanquable – de réduire la fracture numérique.

À la lumière de ce qui précède, les mesures de renforcement de la confiance dans l'Internet doivent figurer au premier plan des politiques publiques. Les pouvoirs publics et la société doivent dialoguer avec les enfants et les jeunes pour comprendre leurs points de vue et stimuler un véritable débat public sur les risques et les perspectives qui se présentent. Le fait d'aider les enfants et les jeunes à gérer les risques en ligne peut être une solution efficace, mais les gouvernements doivent aussi s'assurer qu'il existe des services d'appui adaptés pour ceux qui sont font effectivement de mauvaises expériences en ligne, et que les enfants sachent comment accéder à ces services.

Certains pays peinent à allouer les ressources suffisantes pour résoudre les questions liées à la maîtrise des outils numériques et à la sécurité en ligne des enfants. Toutefois, les enfants disent eux-mêmes que les parents, les enseignants, les entreprises du secteur des technologies et les pouvoirs publics jouent un rôle important dans l'élaboration de solutions permettant d'assurer leur sécurité en ligne. Les États Membres de l'UIT ont aussi indiqué compter sur un soutien considérable pour renforcer le partage de connaissances et déployer des efforts coordonnés pour assurer la sécurité en ligne des enfants[9].

À l'heure actuelle, les enfants et les jeunes évoluent dans un environnement numérique de plus en plus complexe, et l'adoption de l'intelligence artificielle pour l'apprentissage automatique, l'analyse des mégadonnées, la robotique et la réalité virtuelle et augmentée, ainsi que l'Internet des objets, sont en passe de révolutionner l'utilisation des médias par les enfants. Il est donc nécessaire d'élaborer des politiques et d'investir pour les enfants, les parents et les communautés d'aujourd'hui comme de demain.

2.1 Qu'est-ce que la protection en ligne des enfants?

Les technologies en ligne offrent aux enfants et aux jeunes de nombreuses possibilités de communiquer, d'acquérir de nouvelles compétences, d'exercer leur créativité et de contribuer à instaurer une société meilleure. Mais elles peuvent aussi être porteuses de nouveaux risques, par exemple en les exposant à des problèmes de respect de la vie privée, de contenu illicite, de harcèlement, de cyberintimidation, d'utilisation abusive des données personnelles ou de manipulation psychologique à des fins sexuelles (*grooming*), voire d'abus sexuels.

[10] UIT, "Celebrating 10 Years of Child Online Protection" (L'initiative sur la protection en ligne des enfants célèbre ses dix ans d'existence), Revue "Nouvelles de l'UIT", 6 février 2018, https://news.itu.int/celebrating-10-years-child-online-protection/.

Les présentes lignes directrices proposent une approche globale pour lutter contre toutes les menaces et tous les dangers potentiels auxquels les enfants et les jeunes peuvent être exposés lorsqu'ils acquièrent des compétences numériques. Elles reconnaissent que toutes les parties prenantes compétentes ont un rôle à jouer dans la résilience, le bien-être et la protection des jeunes utilisateurs dans le monde numérique, tout en leur permettant de tirer parti des possibilités que l'Internet peut offrir.

Garantir la protection des enfants et des jeunes relève de la responsabilité de chacun et toutes les parties prenantes concernées ont le devoir d'assurer un avenir durable pour tous. À cette fin, les décideurs, les entités du secteur privé, les parents, les personnes s'occupant d'enfants, les éducateurs et d'autres acteurs doivent faire en sorte que les enfants et les jeunes puissent exprimer leur potentiel, tant dans le monde réel que dans le monde virtuel.

La protection en ligne des enfants, bien qu'elle ne fasse pas l'objet d'une définition universelle, vise à adopter une approche globale, afin de créer des espaces numériques sûrs, adaptés à l'âge, inclusifs et participatifs à l'intention des enfants et des jeunes, caractérisés par:

- une capacité de réaction, d'appui et d'auto-assistance face à une menace;
- la prévention des dangers;
- un équilibre dynamique entre la nécessité d'assurer une protection et le fait d'offrir aux enfants la possibilité de devenir des citoyens numériques;
- l'exercice des droits et des responsabilités des enfants et de la société.

En outre, compte tenu de l'évolution rapide de la technologie et de la société, et dans la mesure où l'Internet ne connaît pas de frontières, la protection en ligne des enfants doit relever d'une approche souple et adaptable pour être efficace. Bien que ces lignes directrices permettent de mieux comprendre les principaux risques auxquels sont exposés les enfants et les jeunes en ligne (contenus dangereux et illicites, harcèlement, cyberintimidation, utilisation abusive des données personnelles, ou manipulation psychologique à des fins sexuelles, abus sexuels et exploitation sexuelle des enfants, entre autres), avec les innovations technologiques, de nouveaux problèmes se feront jour, caractérisés par des différences selon les régions. Toutefois, la meilleure façon de résoudre ces problèmes sera de mener une action conjointe réunissant la communauté mondiale, de nouvelles solutions devant être trouvées.

2.2 Les enfants à l'ère du numérique

L'Internet a transformé nos modes de vie. Cette technologie fait partie intégrante du quotidien des enfants et des jeunes, de sorte qu'il est impossible d'envisager le monde numérique et le monde physique de manière séparée. À l'heure actuelle, les enfants et les jeunes représentent un tiers des internautes, et l'UNICEF estime que 71% des jeunes sont déjà connectés.

Pour les enfants et les jeunes, une telle connectivité a été synonyme d'une autonomisation sans précédent. Le monde en ligne leur permet de surmonter les difficultés et les handicaps, et a fourni de nouveaux terrains de jeu pour se divertir, apprendre, participer et bâtir des relations. Aujourd'hui, les plates-formes numériques sont utilisées pour un éventail d'activités et offrent souvent des expériences multimédias.

L'accès à cette technologie et l'acquisition des compétences nécessaires pour l'utiliser et la maîtriser sont indispensables à l'épanouissement des jeunes, pour qui le premier contact avec les technologies a lieu à un âge précoce. Les décideurs doivent comprendre que souvent, les

enfants et les jeunes commencent à utiliser des plates-formes et des services avant d'avoir atteint l'âge minimum requis, raison pour laquelle il faut commencer à les éduquer tôt.

Les enfants et les jeunes veulent participer au débat et ont des avis précieux à échanger, en tant qu'"enfants du numérique". Les décideurs et les professionnels doivent associer les enfants et les jeunes à un débat permanent sur l'environnement en ligne, afin d'appuyer leurs droits.

Accès à l'Internet

En 2019, plus de la moitié de la population mondiale utilisait l'Internet (53,6%), avec 4,1 milliards d'utilisateurs selon les estimations. À l'échelle de la planète, un tiers des internautes sont des enfants âgés de moins de 18 ans[1]. Dans certains pays à faible revenu, cette proportion monte à un internaute sur deux, tandis que dans les pays à revenu élevé, elle est d'environ un internaute sur cinq. D'après l'UNICEF, 71% des jeunes sont déjà connectés dans le monde[2]. Par conséquent, les enfants et les jeunes sont désormais présents sur l'Internet de manière considérable, permanente et persistante[3]. L'Internet sert d'autres objectifs d'ordre social, économique et politique, et représente désormais un produit ou un service familial ou grand public qui fait partie intégrante du quotidien des familles, des enfants et des jeunes.

En 2017, au niveau régional, l'accès des enfants et des jeunes à l'Internet était largement lié au niveau de revenu. Les pays à faible revenu ont tendance à compter moins d'internautes enfants que les pays à revenu élevé.

Dans la plupart des pays, les enfants et les jeunes passent plus de temps en ligne le week-end qu'en semaine. Les adolescents (15-17 ans) sont ceux qui passent le plus de temps en ligne, soit en moyenne 2,5 à 5,3 heures, selon le pays.

Utilisation de l'Internet

Chez les enfants et les jeunes, le dispositif le plus utilisé pour accéder à l'Internet est le téléphone mobile, suivi des ordinateurs de bureau et des ordinateurs portables. Les enfants et les jeunes passent en moyenne environ deux heures par jour en ligne durant la semaine, et approximativement le double le samedi et le dimanche. Certains se sentent connectés en permanence, mais de nombreux autres n'ont toujours pas accès à l'Internet depuis leur domicile.

---

1 Livingstone, S., Carr, J., et Byrne, J. (2015) *One in three: Internet Governance and Children's Rights*. Global Commission on Internet Governance: Paper Series. London: CIGI et Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 Commission sur le large bande, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online" (2019) (Sécurité en ligne des enfants: réduire autant que faire se peut le risque de violence, d'abus et d'exploitation en ligne), *Commission "Le large bande au service du développement durable"*, octobre 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 Livingstone, Carr, et Byrne, "One in Three: Internet Governance and Children's Rights."

Dans la pratique, la plupart des enfants et des jeunes qui utilisent l'Internet y accèdent via plusieurs dispositifs. Ainsi, les enfants et les jeunes qui se connectent au moins une fois par semaine utilisent parfois jusqu'à trois dispositifs différents. Les enfants plus âgés et les enfants issus des pays riches utilisent en général plus de dispositifs, et les garçons utilisent un peu plus de dispositifs que les filles, dans chaque pays étudié.

L'activité la plus populaire – tant chez les filles que chez les garçons – est le visionnage de clips vidéo. Plus des trois quarts des enfants et des jeunes qui utilisent l'Internet disent regarder des vidéos en ligne au moins une fois par semaine, seuls ou avec d'autres membres de leur famille. On peut considérer que de nombreux enfants et de nombreux jeunes ont une "vie sociale active" en ce qu'ils utilisent plusieurs plates-formes de réseaux sociaux, telles que Facebook, Twitter, TikTok ou Instagram.

Les enfants et les jeunes participent aussi à la vie politique en ligne et font entendre leur voix via des blogs.

Le niveau général de participation aux jeux en ligne varie d'un pays à l'autre et dépend approximativement des possibilités d'accès à l'Internet des enfants et des jeunes, tandis que 10 à 30% des enfants et des jeunes utilisant l'Internet participent à des activités créatives en ligne chaque semaine.

À des fins éducatives, de nombreux enfants et de nombreux jeunes de tous âges utilisent l'Internet chaque semaine pour faire leurs devoirs, ou même pour rattraper les cours ou rechercher des informations en ligne sur la santé. Les enfants plus âgés semblent avoir davantage soif d'information que les plus jeunes.

2.3 Les effets de la technologie sur l'expérience numérique des enfants

L'Internet et la technologie numérique sont à la fois une source de possibilités et de risques pour les enfants et les jeunes. À titre d'exemple, lorsque les enfants utilisent les réseaux sociaux, ils ont de nombreuses possibilités d'explorer, d'apprendre, de communiquer et de développer des compétences essentielles. Aux yeux des enfants, les réseaux sociaux sont des plates-formes qui leur permettent d'explorer leur propre identité dans un environnement sûr. Il est important pour les jeunes de disposer des compétences utiles et de savoir comment résoudre des questions ayant trait à leur vie privée et à leur réputation.

"Je sais que tout ce que nous publions sur l'Internet reste pour toujours et que cela peut avoir des conséquences pour notre vie future", Un garçon, 14 ans, Chili.

Toutefois, il est ressorti des consultations que la plupart des enfants utilisent les réseaux sociaux avant d'avoir atteint l'âge minimum de treize ans[11] et que les systèmes de vérification de l'âge sont généralement défaillants ou inexistants. Ainsi, les enfants peuvent être exposés à des risques accrus. Lorsqu'ils souhaitent acquérir des compétences numériques et devenir des citoyens du numérique, en accordant une attention particulière au respect de leur vie privée, les enfants ont tendance à envisager la question de la vie privée en se souciant de leurs amis et de leurs connaissances ("Qu'est-ce que mes amis peuvent voir?") plutôt que des inconnus et

[11] Réseau Conectados al Sur, "Hablatam"; UNICEF, "Global Kids Online Comparative Report (2019)".

des tiers. Associés à la curiosité naturelle des enfants et à leur tendance à être moins vigilants vis-à-vis des risques, ces facteurs peuvent rendre les enfants plus vulnérables au regard de la manipulation psychologique à des fins sexuelles, de l'exploitation sexuelle, du harcèlement ou d'autres types de contenus ou de contacts préjudiciables.

La pratique largement répandue consistant à échanger des images et des vidéos via des applications mobiles, et en particulier l'utilisation par les enfants de plates-formes de *streaming* en direct, posent d'autres problèmes liés à la vie privée et aux risques. Certains enfants produisent des images à caractère sexuel d'eux-mêmes, de leurs amis et de leurs frères et sœurs, et les partagent en ligne. Certains, en particulier les enfants plus âgés, peuvent percevoir cette pratique comme l'exploration naturelle de leur sexualité et de leur identité sexuelle, tandis que d'autres, en particulier les enfants plus jeunes, sont souvent contraints de le faire par un adulte ou par un autre enfant. Dans tous les cas, le contenu qui en résulte est illégal dans de nombreux pays et peut exposer les enfants au risque de poursuites judiciaires, ou être utilisé en vue d'exploiter davantage l'enfant.

De la même manière, les jeux en ligne permettent aux enfants d'exercer pleinement leur droit fondamental de jouer, tout comme de nouer des relations, de passer du temps avec leurs amis et de se faire de nouveaux amis, et de développer des compétences importantes. Dans la plupart des cas, une telle activité peut avoir des effets positifs. Toutefois, de plus en plus d'éléments indiquent que si elles ne sont pas surveillées ou gérées par un adulte responsable, les plates-formes de jeux en ligne peuvent aussi présenter des risques pour les enfants, allant des troubles dus aux jeux, des risques financiers, de la collecte et de la monétisation des données personnelles des enfants, au cyberharcèlement, au discours haineux, à la violence et à l'exposition à des comportements ou des contenus inappropriés[12], en passant par la manipulation psychologique à des fins sexuelles au moyen d'images ou de vidéos réelles, générées par ordinateur ou même de réalité virtuelle, qui mettent en scène et banalisent les abus sexuels et l'exploitation sexuelle des enfants.

En outre, les progrès technologiques ont donné naissance à l'Internet des objets, dans le cadre duquel de plus en plus de dispositifs divers et variés peuvent se connecter, communiquer et fonctionner en réseau via l'Internet. Ces dispositifs peuvent aussi être des jouets, des interphones de surveillance des bébés et des dispositifs fondés sur l'intelligence artificielle, qui sont susceptibles de présenter des risques s'agissant de la confidentialité et des contacts non désirés.

2.4 Principales menaces auxquelles les enfants sont exposés en ligne

Les adultes et les enfants sont exposés à un éventail de risques et de dangers en ligne. Cependant, les enfants constituent un groupe beaucoup plus vulnérable. Certains enfants sont aussi plus vulnérables que d'autres, selon le groupe auquel ils appartiennent, à l'instar des enfants handicapés[13] ou des enfants migrants. Les décideurs ont le devoir de garantir que tous les enfants puissent grandir et bénéficier d'une éducation dans un environnement numérique sûr. La Convention des Nations Unies relative aux droits de l'enfant souligne le caractère vulnérable des enfants et la nécessité de les protéger contre toute forme d'exploitation.

[12] UNICEF, "Global Kids Online Comparative Report (2019)". (UNICEF, 2019)

[13] Lundy et al., "Deux clics en avant et un clic en arrière", Rapport sur les enfants en situation de handicap dans l'environnement numérique (Conseil de l'Europe, octobre 2019), https://rm.coe.int/deux-clics-en-avant-et-un-clic-en-arriere-rapport-sur-les-enfants-en-s/168098bd10.

L'environnement numérique offre aux enfants des possibilités intéressantes dans plusieurs domaines, mais peut dans le même temps renfermer des risques susceptibles de blesser profondément les enfants et de nuire à leur bien-être. Par exemple, d'aucuns se disent inquiets, pour les adultes comme pour les enfants, que l'Internet puisse être utilisé pour porter atteinte à la vie privée, diffuser de fausses informations ou pire, permettre d'accéder à des contenus pornographiques.

Il est indispensable en l'espèce de faire une distinction entre les risques et les dangers pour les enfants. En effet, toutes les activités qui peuvent comporter des risques ne sont pas dangereuses, et tous les risques ne se traduisent pas forcément par un préjudice pour les enfants. C'est le cas, par exemple, de l'échange d'images ou de messages à caractère sexuel (*sexting*), qui est un moyen pour les jeunes d'explorer la sexualité et les relations, sans nécessairement leur porter préjudice.

Figure 2: Classification des menaces auxquelles les enfants sont exposés en ligne[14]

	Contenu (l'enfant est destinataire (de contenus produits de masse))	Contacts (l'enfant participe (à une activité initiée par un adulte)	Comportements (l'enfant est acteur (auteur/victime))
Agressif	Contenu violent/gore	Harcèlement, prédation	Intimidation, comportements hostiles entre enfants
Sexuel	Contenu pornographique	Manipulation psychologique, abus sexuel lors de rencontres avec des inconnus	Harcèlement sexuel, messages à caractères sexuels
Valeurs	Contenu raciste/haineux	Prosélytisme idéologique	Contenu potentiellement préjudiciable créé par des utilisateurs
Commercial	Publicité, marketing intégré	Exploitation et utilisation abusive des données personnelles	Jeux d'argent, violation des droits d'auteur

Source: EU Kids Online (Livingstone, Haddon, Görzig, et Ólafsson (2011))

L'avènement de l'ère du numérique fait naître de nouveaux défis pour la protection des enfants. Il faut doter les enfants des moyens de naviguer dans le monde virtuel en toute sécurité et d'en tirer le plus grand profit.

Les décideurs doivent veiller à ce que la législation, les garanties et les outils pertinents soient en place afin de permettre aux enfants de grandir et d'apprendre en toute sécurité. Il est fondamental que les enfants soient dotés des compétences nécessaires pour identifier les menaces et comprendre pleinement les incidences et les subtilités de leur comportement en ligne.

Lorsqu'ils sont en ligne, les enfants peuvent être confrontés à une multitude de menaces venant d'organisations, d'adultes et d'autres enfants.

[14] Livingstone, S., Haddon, L., Görzig, A., et Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. (Risques et sécurité sur l'Internet: Les perspectives qui s'offrent aux enfants européens. Résultats complets.) LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.

Contenu et manipulation

- L'exposition à des contenus inappropriés voire délictueux peut pousser les enfants à avoir des réactions extrêmes, telles que l'automutilation et des comportements destructeurs et violents. L'exposition à des contenus de ce type peut également entraîner la radicalisation ou l'adhésion à des idées racistes ou discriminatoires. Il est reconnu que de nombreux enfants ne respectent pas la limite d'âge imposée pour accéder à certains sites web.
- L'exposition à des informations inexactes ou incomplètes limite la compréhension que les enfants peuvent avoir du monde qui les entoure. La tendance qui consiste à personnaliser les contenus sur la base du comportement de l'utilisateur peut être à l'origine de "bulles de filtre" (*filter bubbles*), réduisant ainsi la capacité des enfants de s'épanouir et d'accéder à un large éventail de contenus.
- L'exposition à des contenus filtrés par des algorithmes, à des fins de manipulation, peut avoir une influence considérable sur l'épanouissement, les opinions, les valeurs et les habitudes d'un enfant. Isoler les enfants dans des "chambres d'écho" (*echo chambers*) ou dans des "bulles de filtre" (*filter bubbles*) les empêche d'accéder à des opinions et des idées diverses et variées.

Contact avec des adultes ou d'autres enfants

Les enfants peuvent être exposés à de nombreuses menaces liées à des contacts avec d'autres enfants ou des adultes.

- Les actes de harcèlement en ligne peuvent se répandre plus largement et plus rapidement qu'hors ligne. Ils peuvent s'exercer à toute heure du jour ou de la nuit, empiétant ainsi sur des espaces auparavant "sûrs", et de manière anonyme.
- Les enfants qui sont maltraités dans le monde réel sont susceptibles de l'être aussi dans le monde virtuel. De fait, les enfants handicapés sont exposés à un risque accru en ligne, étant donné que les recherches montrent que les enfants handicapés risquent davantage de subir des abus de tout type, en particulier des abus sexuels. Parmi les abus figurent des actes d'intimidation, de harcèlement, d'exclusion et de discrimination du handicap existant ou ressenti de l'enfant, ou à des aspects liés à son handicap, par exemple la façon dont il se comporte ou parle, ou les équipements ou les services qu'il utilise.
- Diffamation et atteinte à la réputation: les images et les vidéos peuvent être modifiées et partagées avec des milliards de personnes. Les commentaires inappropriés peuvent être accessibles pendant des décennies et quiconque peut les visualiser.
- Les enfants peuvent être pris pour cible, manipulés psychologiquement à des fins sexuelles ou agressés via l'Internet par une personne qui se trouve dans le même pays ou à l'autre bout du monde, et qui se fait souvent passer pour quelqu'un d'autre. Ces agressions peuvent avoir des conséquences prenant différentes formes, l'enfant pouvant par exemple se radicaliser ou envoyer des contenus sexuellement explicites de lui-même sous la contrainte.
- Les enfants peuvent subir des pressions, être piégés ou être contraints d'effectuer des achats avec ou sans l'autorisation du payeur.
- Les publicités non sollicitées soulèvent des problèmes en matière de consentement et de vente des données.

Comportement de l'enfant susceptible d'avoir des incidences

- Les actes de harcèlement en ligne peuvent être particulièrement perturbants et préjudiciables, dans la mesure où ils peuvent se propager à plus grande échelle et être largement relayés, et où les contenus diffusés de manière électronique peuvent resurgir à tout moment, d'où le risque qu'il soit plus difficile pour une victime de cyberharcèlement de tourner la page. Les actes de harcèlement en ligne peuvent véhiculer des images préjudiciables ou des propos blessants, et les contenus sont disponibles 24 heures sur 24. Le harcèlement en ligne peut avoir lieu 24 heures sur 24 et 7 jours sur 7, et donc envahir

la sphère privée de la victime même lorsqu'elle se trouve dans un lieu normalement "sûr", par exemple à son domicile. Les informations personnelles peuvent être manipulées, les images modifiées et transférées à d'autres personnes et ainsi de suite. De plus, ce harcèlement peut être anonyme. La divulgation d'informations personnelles comporte un risque de dommages physiques, notamment en cas de rencontres dans la vie réelle de connaissances faites en ligne, qui pourraient entraîner des agressions physiques et/ou sexuelles.

- La violation de ses propres droits ou de ceux des autres, par le biais du plagiat ou du téléchargement de contenus sans autorisation, y compris la prise ou le téléchargement de photos inappropriées sans autorisation.
- La violation du droit d'auteur d'autrui, par exemple en téléchargeant de la musique, des films ou des programmes télévisuels pour lesquels il faudrait payer, dans la mesure où une telle pratique peut porter préjudice à la victime du vol.
- L'utilisation compulsive et excessive de l'Internet et/ou des jeux en ligne, au détriment d'activités sociales et/ou d'extérieur importantes pour la santé, le renforcement de la confiance, le développement de relations sociales et le bien-être en général.
- Une tentative visant à blesser, à harceler ou à intimider autrui, notamment en se faisant passer pour quelqu'un d'autre, souvent un autre enfant.
- Une pratique de plus en plus répandue chez les adolescents est le "sexting", c'est-à-dire le partage d'images ou de messages à caractère sexuel via des téléphones mobiles. Ces images et ces messages sont souvent échangés entre partenaires ayant une relation ou entre partenaires potentiels, mais finissent parfois par être transmis beaucoup d'autres personnes. Il est peu probable que les adolescents comprennent bien les répercussions de tels comportements et les risques potentiels qui y sont associés

2.5 Principaux dangers auxquels les enfants sont exposés en ligne

La section précédente fait état des menaces que les enfants sont susceptibles de rencontrer en ligne. La présente section met en évidence les dangers qui peuvent découler de ces menaces.

Dangers

D'après les études de l'UNICEF sur l'utilisation de l'Internet, les catégories suivantes sont considérées comme des risques et des dangers:

- Sévices auto-infligés et automutilation:
  - contenu suicidaire
  - discrimination
- Exposition à des contenus inappropriés:
  - exposition à des contenus extrémistes/violents/sanglants
  - marketing intégré
  - jeux d'argent en ligne
- Environ 20% des enfants ayant participé à une enquête sur la question ont dit avoir vu, durant l'année écoulée, des sites web ou des discussions en ligne concernant des personnes qui se sont automutilées ou se sont infligées des blessures.
- Radicalisation:
  - persuasion idéologique
  - discours haineux
- La probabilité qu'un enfant dise avoir été perturbé par un discours haineux ou des contenus sexuels en ligne, avoir été la cible d'un comportement blessant est plus élevée dans le cas du monde en ligne, ou lors d'une rencontre en personne avec une connaissance faite en ligne dans un premier temps, que dans le monde réel.
- Abus sexuels et exploitation sexuelle:
  - production de contenus par des enfants
  - manipulation psychologique à des fins sexuelles
  - contenus montrant des abus sexuels sur des enfants
  - traite d'enfants
  - voyage et tourisme sexuel visant les enfants

Une étude réalisée en 2017 concernant des enfants au Danemark, en Hongrie et au Royaume-Uni a révélé que pour 6% des enfants, des photos explicites d'eux avaient été partagées sans leur autorisation.

En 2019, la Fondation Internet Watch (IWF) a recensé plus de 132 000 pages web dont il a été confirmé qu'elles comportaient des images et des vidéos montrant des abus sexuels sur des enfants. Chaque page web pouvait contenir jusqu'à des milliers d'images de ce type d'abus.

Les risques liés à la violence en ligne, comme la diffusion de photos de nus sans consentement et le cyberharcèlement sexuel, sont caractérisés par des rapports déséquilibrés entre les garçons et les filles. En effet, les filles subissent généralement plus de pressions que les garçons à l'égard des comportements sexuels, avec des conséquences plus grandes et plus graves.

- Violation et utilisation abusive des données personnelles:
  - piratage
  - fraude et vol

De nombreuses personnes connaissent bien les escroqueries et les piratages en ligne, mais les atteintes à la vie privée concernant les activités en ligne d'un enfant sont considérées comme une autre violation. Souvent, les adultes contrarient les jeunes en passant au crible leur téléphone mobile et en surveillant leurs activités en ligne. À titre d'exemple, les signalements faits par des enfants au Brésil montrent que les garçons comme les filles, quel que soit l'âge, considèrent que les parents contrôlent davantage l'utilisation de l'Internet par les filles. Les tentatives d'explication laissent penser que les filles peuvent être dans certains cas plus vulnérables à cause des structures sociétales au sein desquelles elles évoluent, en particulier concernant leur sécurité, dans un contexte où la frontière entre les interactions en ligne et celles hors ligne devient de plus en plus floue.

- Cyberintimidation, traque et harcèlement: activité hostile et violente envers les pairs

Les salons de discussion en ligne et les sites de réseaux sociaux peuvent ouvrir la voie à des actes de violence et d'intimidation, dans la mesure où des utilisateurs anonymes, y compris des jeunes, participent à des discussions en étant agressifs ou insultants. Dans sept pays d'Europe (Belgique, Danemark, Irlande, Italie, Portugal, Roumanie et Royaume-Uni), Livingstone, Mascheroni, Ólafsson et Haddon[1] ont observé qu'en moyenne, 8% des enfants avaient été victimes de cyberharcèlement en 2010, contre 12% en 2014.

Il est essentiel de souligner que les enfants vulnérables sont plus souvent victimes de cyberharcèlement.

[1] Livingstone, S., Mascheroni, G., Ólafsson, K., et Haddon, L., (2014) *Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile*. (Risques et perspectives en ligne pour les enfants: comparaison des résultats des travaux de EU Kids Online et de Net Children Go Mobile), London: London School of Economics and Political Science, www.eukidsonline.net et hYp://www.netchildrengomobile.eu/.

Zoom sur: Des inégalités qui se creusent

En 2017, environ 60% des enfants n'étaient pas connectés dans la région Afrique, contre seulement 4% des enfants en Europe. Dans chaque région du monde, les internautes hommes sont plus nombreux que les internautes femmes, et l'utilisation de l'Internet par les filles est

souvent surveillée et limitée. Avec l'expansion du large bande aux zones du monde qui ne sont pas encore connectées, ces inégalités ne cesseront de se creuser[15].

Il se peut que les enfants qui utilisent des téléphones mobiles plutôt que des ordinateurs aient une expérience en ligne de qualité inférieure. Les enfants qui parlent des langues minoritaires sont souvent dans l'incapacité de trouver des contenus utiles en ligne, et les enfants issus de zones rurales sont plus exposés aux vols de mots de passe ou d'argent.

Les travaux de recherche montrent que de nombreux adolescents dans le monde doivent surmonter des barrières majeures pour être présents en ligne. Pour bon nombre d'entre eux, les difficultés d'accès (mauvaise connectivité, coûts prohibitifs des données et des dispositifs et absence d'équipements appropriés) constituent encore des obstacles de taille.

Avec l'expansion du large bande à un coût financièrement abordable aux pays en développement, il devient urgent de mettre en place des mesures pour réduire autant que possible les risques et les menaces auxquels les enfants sont exposés, tout en leur permettant de tirer le meilleur parti de tous les avantages qu'offre le monde numérique.

Zoom sur: Les contenus montrant des abus sexuels sur des enfants

L'ampleur du problème

L'Internet a révolutionné la portée et la nature de la production, de la distribution et de la disponibilité de contenus montrant des abus sexuels sur des enfants. En 2018, des entreprises du secteur des technologies implantées aux États-Unis d'Amérique ont signalé plus de 45 millions d'images et de vidéos en ligne dont on suspectait qu'elles mettaient en scène des abus sexuels sur des enfants du monde entier. Il s'agit d'une industrie mondiale et l'ampleur et la gravité des abus vont croissant malgré les efforts déployés pour y mettre fin.

Historiquement, dans un monde hors ligne, les personnes qui voulaient se procurer du matériel montrant des abus sexuels sur des enfants devaient prendre des risques considérables et payer un prix élevé pour y accéder. Grâce à l'Internet, ces personnes peuvent désormais accéder à ce type de matériel de manière relativement simple et s'adonner à des pratiques de plus en plus risquées. Les caméras sont plus petites et davantage présentes dans chaque aspect de notre quotidien, et il n'a donc jamais été aussi facile de produire des contenus montrant des abus sexuels sur des enfants et d'acheter des contenus montrant des abus sans contact physique.

Il est impossible de déterminer la taille ou la forme que revêt précisément cette industrie clandestine et illégale. Toutefois, il ne fait aucun doute que les images illégales qui sont en circulation aujourd'hui se comptent par millions. Pratiquement tous les enfants concernés ont vu les images les mettant en scène être dupliquées. En 2018, la Fondation IWF a étudié la fréquence à laquelle les images d'un enfant connu pour avoir été sauvé en 2013 refaisaient surface. Pendant les trois mois de surveillance, les analystes de la Fondation ont recensé ces images 347 fois, soit 5 fois par jour ouvrable.

La situation actuelle

[15] Commission sur le large bande, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online" (2019) (Sécurité en ligne des enfants: réduire autant que faire se peut le risque de violence, d'abus et d'exploitation en ligne).

Chaque fois qu'une image mettant en scène un enfant victime d'abus s'affiche une ou plusieurs fois en ligne, ou chaque fois qu'elle est téléchargée par quelqu'un, cet enfant est une nouvelle fois victime d'abus. Les victimes sont contraintes de vivre le reste de leur vie avec ces images qui ne s'effacent pas et continuent de circuler.

Dès la découverte de matériel montrant des abus sexuels sur des enfants ou d'une page web hébergeant ce type de matériel, il importe de supprimer ou de bloquer le contenu le plus vite possible. Le caractère mondial de l'Internet rend la tâche difficile: en effet, une personne peut produire du matériel dans un pays et l'héberger dans un autre, à l'intention de consommateurs qui se trouvent dans un autre pays encore. Sans une véritable coopération internationale, les avis de recherche et les mandats d'arrêt publiés par un pays restent presque toujours sans effet.

L'innovation au sein du monde numérique évolue à un rythme tel que le terrain de jeu des criminels change constamment. Certaines menaces se sont faites jour récemment, notamment concernant les éléments suivants:

- L'essor du chiffrement permet aux criminels de manipuler et de partager des contenus par le biais de canaux cachés, tout en compliquant la détection et l'application de la loi.
- Des forums consacrés à la manipulation psychologique des enfants à des fins sexuelles se multiplient dans des parties cachées de l'Internet, banalisant et encourageant ce type de comportement, la fourniture de "nouveaux contenus" étant souvent une condition pour pouvoir accéder à ces forums.
- Actuellement, le développement rapide de l'Internet permet aux utilisateurs de se connecter dans des domaines pour lesquels il reste encore à élaborer/appliquer une stratégie globale en matière de protection ou l'infrastructure pertinente.
- Les enfants utilisent des dispositifs sans supervision dès leur plus jeune âge et les comportements sexuels en ligne sont banalisés. La quantité d'images autoproduites montrant des abus augmente chaque année.

Zoom sur: Les contenus autoproduits

Les enfants et les adolescents peuvent prendre des photos ou faire des vidéos compromettantes d'eux-mêmes. Si cette pratique en soi n'est pas forcément illégale et peut s'inscrire dans le cadre d'un développement sexuel sain et ordinaire, il existe des risques que des contenus de ce type soient diffusés, en ligne ou hors ligne, pour nuire aux enfants ou leur extorquer des faveurs. Bien que certains enfants puissent subir des pressions ou être contraints à partager des images à caractère sexuel, d'autres (en particulier les adolescents) peuvent produire volontairement des contenus à caractère sexuel. Pour autant, cela ne signifie pas qu'ils consentent à l'utilisation de ces images à des fins d'exploitation ou d'utilisation abusive et/ou de distribution, ou qu'ils en sont responsables.

Le "sexting" désigne "l'autoproduction d'images à caractère sexuel"[16] ou "l'échange de messages ou d'images à caractère sexuel" et "la création, le partage et le transfert d'images de nus ou de semi-nus à caractère sexuel, via des téléphones mobiles et/ou l'Internet"[17].

[16] Karen Cooper et al., "Adolescents and Self-Taken Sexual Images: A Review of the Literature" (Adolescents et images à caractère sexuel autoproduites: une étude documentaire), *Computers in Human Behaviour* 55 (février 2016): 706-16, https://doi.org/10.1016/j.chb.2015.10.003.

[17] Jessica Ringrose et al., "A Qualitative Study of Children, Young People and "Sexting": A Report Prepared for the NSPCC" (Étude qualtitative sur les enfants, les jeunes et le "sexting": Rapport préparé pour la société NSPCC) (London, UK: National Society for the Prevention of Cruelty to Children, 2012), http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x.

Cette pratique consiste à produire soi-même des contenus sexuellement explicites[18] et "varie considérablement en fonction du contexte, du message et de l'intention"[19].

Le "sexting" est probablement la forme la plus courante de contenus sexuellement explicites autoproduits mettant en scène des enfants, et est souvent le fait d'adolescents consentants qui tirent satisfaction d'une telle expérience, mais il existe aussi de nombreuses formes de "sextos" non désiré. Il s'agit des aspects non consentis de cette pratique, par exemple le fait de partager ou de recevoir des photos, des vidéos ou des messages sexuellement explicites et non désirés, envoyés par des personnes connues ou des inconnus qui essaient d'entrer en contact avec l'enfant, d'exercer une pression sur lui ou de le manipuler à des fins sexuelles. Le "sexting" peut aussi être une forme de harcèlement sexuel consistant à exercer une pression sur un enfant pour qu'il envoie une photo à son/sa petit(e) ami(e) ou à un autre enfant, qui la transmet ensuite à un réseau de contacts sans avoir obtenu son consentement.

Zoom sur: Le cyberharcèlement

Si le harcèlement est un fléau qui existait déjà bien avant l'invention l'Internet, l'ampleur, la portée et la continuité du harcèlement pratiqué en ligne peuvent accentuer davantage ce qui est déjà une expérience perturbante et souvent toxique pour les victimes. Par définition, le cyberharcèlement consiste à se servir d'ordinateurs, de téléphones portables et d'autres dispositifs électronique pour blesser quelqu'un volontairement et de manière répétée. Il se produit parallèlement à un harcèlement dans la vie réelle, à l'école ou ailleurs. Le cyberharcèlement peut avoir en outre une dimension raciste, religieuse ou sexiste et prolonger le mal causé dans la vie réelle, par exemple moyennant le piratage de compte, et la diffusion de photos et de vidéos en ligne, et ce d'autant plus que les messages blessants et les contenus sont disponibles 24 heures sur 24 et 7 jours sur 7. Puisqu'il s'agit généralement d'un problème social plutôt que d'un acte criminel, les politiques visant à lutter contre le cyberharcèlement doivent appliquer une approche globale associant les écoles, les familles et surtout les enfants.

Zoom sur: La manipulation psychologique à des fins sexuelles et le chantage sexuel en ligne

Ces dernières années, les progrès rapides de la technologie et l'accès grandissant à l'Internet et aux communications numériques ont conduit inévitablement à un accroissement des risques d'actes criminels perpétrés en ligne et ciblant des enfants. Parmi ces nouvelles formes d'exploitation sexuelle d'enfants en ligne figurent la manipulation psychologique à des fins sexuelles (*grooming*) et le chantage sexuel (*sextortion*) pratiqués en ligne. La manipulation psychologique exercée en ligne à des fins sexuelles désigne de manière générale le processus par lequel un adulte se lie d'amitié avec un enfant (âgé de moins de 18 ans) et exerce une influence sur celui-ci, par le biais de l'Internet ou d'autres technologies numériques, en vue de faciliter les interactions sexuelles avec l'enfant, que ce soit avec ou sans contact physique. Tout au long du processus de manipulation, l'agresseur tente de rendre l'enfant docile afin de

[18] Office des Nations Unies contre la drogue et le crime (ONUDC), "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children" (Étude sur les effets des nouvelles technologies de l'information sur la maltraitance et l'exploitation des enfants) (Vienne: ONU, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf, page 22.

[19] Cooper et al., "Adolescents and Self-Taken Sexual Images".

garder secrète la situation et d'éviter toute identification et toute répression[20]. Il est important de reconnaître que dans certains cas, l'agresseur est un autre enfant.

INTERPOL signale que l'Internet facilite la manipulation psychologique à des fins sexuelles en ce qu'il regroupe un nombre considérable de cibles potentielles facilement accessibles, et qu'il permet aux manipulateurs de se présenter d'une manière qui soit attirante pour les enfants. Les pédocriminels qui sévissent en ligne ont recours à la manipulation, à la coercition et à la séduction pour réduire les inhibitions et inciter les enfants à avoir une activité sexuelle. Le manipulateur commence de façon prémédité par identifier une victime potentielle vulnérable et rassembler des informations sur le soutien familial dont bénéficie l'enfant, puis exerce une pression ou joue sur la honte/peur pour abuser sexuellement de l'enfant. Parfois, les manipulateurs utilisent du matériel à caractère pornographique ou pédopornographique en vue de vaincre les réticences de leurs cibles potentielles, en présentant la pédopornographie comme une activité somme toute naturelle et ordinaire. L'Internet a modifié la façon dont les individus interagissent et a redéfini le concept "d'ami". Un manipulateur peut devenir l'ami d'un enfant en ligne très facilement et rapidement, ce qui nous oblige à repenser les messages classiques qui mettent en garde contre le "danger des inconnus".

La manipulation psychologique exercée en ligne à des fins sexuelles a été reconnue formellement pour la première fois en 2007, dans un instrument juridique international, à savoir la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote). L'Article 23 érige en infraction la "sollicitation d'enfants à des fins sexuelles", qui suppose une proposition intentionnelle de rencontre avec un enfant dans le but de commettre à son encontre des activités sexuelles illégales, suivie "d'actes matériels conduisant à ladite rencontre". Dans de nombreux cas de manipulation de ce type, les enfants sont victimes d'abus sexuels et exploités sexuellement en ligne – la "rencontre" requise par la Convention de Lanzarote et par de nombreuses lois nationales existantes est entièrement virtuelle. Pourtant, une rencontre virtuelle est tout aussi dangereuse pour l'enfant qu'une rencontre physique. Il est indispensable d'ériger également en infraction les cas où "l'abus sexuel n'aboutit pas à une rencontre en personne, mais est commis en ligne"[21].

Le chantage sexuel (*sextortion*)[22] peut être considéré comme un aspect de la manipulation en ligne ou comme une infraction à part entière. Si le chantage sexuel peut se produire sans qu'il n'y ait manipulation, celle-ci peut dans certains cas aboutir au chantage sexuel[23]. Le chantage sexuel peut être pratiqué lors du processus de manipulation psychologique en ligne lorsqu'un prédateur exerce une manipulation et une influence sur l'enfant, en usant de

---

20 Centre international pour les enfants disparus et exploités (ICMEC), "Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review" (Manipulation psychologique des enfants en ligne à des fins sexuelles: Examen de la législation type à l'échelle mondiale), 1ère édition (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

21 Comité de Lanzarote, Comité des Parties à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, *Sollicitation d'enfants à des fins sexuelles par le biais des technologies de l'information et de la communication ("grooming") – Avis sur l'Article 23 de la Convention de Lanzarote et sa note explicative*, 17 juin 2015, *disponible à l'adresse* https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html (page consultée le 30 juin 2020).

22 National Center for Missing and Exploited Children (NCMEC), "Sextortion" (Chantage sexuel), disponible à l'adresse http://www.missingkids.com/theissues/onlineexploitation/sextortion (page consultée le 30 juin 2020).

23 Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels, Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants, Luxembourg, 28 janvier 2016, D.4iii, 29, *disponible à l'adresse* http://luxembourgguidelines.org/fr/version-francaise/.

menaces, d'intimidations et de contraintes pour l'enjoindre d'envoyer des images de lui-même à caractère sexuel (contenu autoproduit)[24]. Si la victime ne cède pas aux demandes (faveurs sexuelles, envoi d'images intimes supplémentaires ou d'argent, ou autres types de demandes), ses images pourront être publiées en ligne afin de l'humilier, de l'intimider ou de le contraindre à produire d'autres contenus sexuellement explicites[25].

Le chantage sexuel est considéré comme une "agression sexuelle virtuelle" en raison de ses effets émotionnels et psychologiques similaires à ceux d'une agression sexuelle pour les victimes[26]. Dans certains cas, les victimes sont tellement traumatisées qu'elles ont tenté de s'automutiler ou de se suicider pour mettre fin à la situation.

Europol a noté qu'il est difficile de recueillir des informations qui permettent d'évaluer la portée des actes de chantage sexuel d'enfants et que ce phénomène peut donc être largement sous-estimé[27]. De plus, l'absence de terminologie et de définitions communes pour la manipulation psychologique et le chantage sexuel en ligne constitue un obstacle à la collecte de données pertinentes et à une compréhension de la véritable ampleurs de ces problèmes à l'échelle mondiale.

2.6 Enfants vulnérables

Les enfants et les jeunes peuvent être vulnérables pour une multitude de raisons différentes. Des recherches effectuées en 2019 ont montré que "la vie numérique des enfants vulnérables fait rarement l'objet de la même attention nuancée et sensible que l'hostilité de la 'vie réelle' tend à susciter". De plus, le rapport indique que dans le meilleur des cas, les enfants et les jeunes vulnérables reçoivent les mêmes conseils généraux sur la sécurité en ligne que tous les autres enfants et jeunes, alors même que l'intervention de spécialistes est nécessaire.

Les enfants migrants, les enfants souffrant du trouble du spectre de l'autisme (TSA) et les enfants handicapés constituent trois exemples de groupes vulnérables mais il en existe, bien sûr, de nombreux autres.

Enfants migrants

Les enfants et les jeunes de familles de migrants arrivent souvent dans un pays (ou y vivent déjà) avec leur propre vécu et attentes sur le plan socio-culturel. Si la technologie est souvent perçue comme un moyen de faciliter la connexion et la participation, les risques et les possibilités qui se présentent en ligne peuvent différer considérablement selon les contextes. En outre,

[24] Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels, Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants, Luxembourg, 28 janvier 2016, D.4iii, 29, *disponible à l'adresse* http://luxembourgguidelines.org/fr/version-francaise/.

[25] Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels, Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants, Luxembourg, 28 janvier 2016, D.4iii, 29, *disponible à l'adresse* http://luxembourgguidelines.org/fr/version-francaise/.

[26] Benjamin Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault" (Chantage sexuel: cybersécurité, adolescents et agression sexuelle à distance) (Brookings Institution, 11 mai 2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

[27] Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (Coercition et extorsion en ligne à des fins sexuelles en tant que crime à l'encontre des enfants: point de vue de l'application de la loi) (Centre européen de lutte contre la cybercriminalité, mai 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

il ressort des données empiriques et des recherches que les médias numériques assurent en général une fonction essentielle:

- Ils sont importants pour l'orientation (pendant le voyage lorsque l'on se rend dans un autre pays).
- Ils assurent une fonction centrale aux fins d'appropriation et de familiarisation avec la société/culture du pays hôte.
- Les médias sociaux peuvent jouer un rôle fondamental pour maintenir le contact avec la famille et les autres, et pour accéder à des informations générales.

Parallèlement aux nombreux aspects positifs, les médias numériques peuvent aussi présenter des défis pour les migrants, notamment en ce qui concerne:

- L'infrastructure: il est important de réfléchir à des espaces sûrs en ligne de sorte que les enfants et les jeunes migrants puissent bénéficier d'un environnement sûr et respectueux de la vie privée.
- Les ressources: les migrants dépensent l'essentiel de leur argent dans des cartes téléphoniques à prépaiement.
- L'intégration: parallèlement à l'accès aux technologies, les enfants et les jeunes migrants doivent aussi recevoir une bonne éducation dans le domaine du numérique.

Enfants souffrant du trouble du spectre de l'autisme (TSA)

Le spectre de l'autisme tombe dans deux catégories essentielles du processus de diagnostic du comportement défini dans la cinquième édition du Manuel diagnostique et statistique des troubles mentaux (DSM-5):

- caractère restreint et répétitif des comportements ("le besoin de similitude");
- déficit des interactions sociales et de la communication;
- lien fréquent avec une déficience intellectuelle, des particularités du langage et d'autres particularités similaires.

La technologie et l'Internet offrent des possibilités infinies aux enfants et aux jeunes pour apprendre, communiquer et jouer. Toutefois, ces avantages s'accompagnent de nombreux risques auxquels les enfants et les jeunes souffrant de TSA peuvent être davantage exposés:

- L'Internet peut offrir aux enfants et aux jeunes autistes des possibilités de nouer des relations sociales et susciter des intérêts particuliers, ce qui n'est pas forcément le cas dans la vie réelle.
- Les défis liés aux interactions sociales, par exemple la difficulté à comprendre les intentions des autres, peuvent exposer davantage ce groupe à des "amis" ayant de mauvaises intentions.
- Les problèmes rencontrés en ligne sont souvent liés aux caractéristiques fondamentales de l'autisme. Ainsi, des orientations concrètes et précises permettraient d'améliorer l'expérience en ligne des utilisateurs, même si les problèmes sous-jacents demeurent.

Enfants handicapés

Les enfants handicapés rencontrent des risques en ligne de la même façon que les enfants qui ne le sont pas, mais ils peuvent aussi être confrontés à des risques spécifiquement liés à leur handicap. Les enfants handicapés sont souvent exclus ou stigmatisés, et se heurtent à des obstacles (d'ordre physique, économique, social ou comportemental), de sorte qu'ils ne peuvent participer aux activités de leur communauté. Ces expériences peuvent porter un enfant handicapé à rechercher des interactions sociales et des amitiés dans le cyberespace, ce qui peut être positif pour l'enfant et lui permettre de gagner en assurance et de se forger un

réseau de soutien. Toutefois, l'enfant peut se trouver davantage à la merci de la manipulation psychologique, de la sollicitation en ligne et/ou du harcèlement sexuel. En effet, des travaux de recherche montrent que les enfants qui sont confrontés à des difficultés dans le monde réel et ceux qui souffrent de troubles psychologiques sont davantage exposés à ce genre d'incidents[28].

Dans l'ensemble, les enfants qui sont maltraités dans le monde réel sont susceptibles de l'être aussi dans le monde virtuel. Par conséquent, les enfants handicapés sont exposés à un risque accru en ligne, alors même qu'ils ont davantage besoin d'être connectés. Il ressort des travaux de recherche que les enfants handicapés risquent davantage de subir des abus de tout type[29], en particulier des abus sexuels[30]. Parmi les abus figurent des actes d'intimidation, de harcèlement, d'exclusion et de discrimination fondée sur le handicap existant ou ressenti de l'enfant, ou sur des aspects liés à son handicap, par exemple la façon dont il se comporte ou parle, ou les équipements ou les services qu'il utilise.

Les criminels qui pratiquent la manipulation psychologique, la sollicitation en ligne et/ou le harcèlement sexuel à l'encontre d'enfants handicapés peuvent être non seulement des personnes qui ciblent les enfants, mais aussi des personnes qui cible spécifiquement les enfants handicapés. Il peut s'agir par exemple de "fétichistes" – c'est-à-dire de personnes qui ne sont pas en situation de handicap et qui sont attirées sexuellement par des personnes handicapées (le plus souvent les amputés et les personnes utilisant des équipements d'aide à la mobilité), certains se faisant même passer pour des personnes handicapées[31]. Ces criminels peuvent notamment télécharger des photos et des vidéos d'enfants handicapés (qui semblent inoffensives) et/ou les diffuser sur des forums spécialisés ou des comptes de réseaux sociaux. Souvent, les outils qui permettent de signaler des abus sur des forums ou des réseaux sociaux ne disposent pas des moyens spécialisés ou appropriés pour traiter ce genre de pratiques.

D'aucuns sont inquiets que le "sharenting", une pratique consistant pour les parents à partager des informations sur leurs enfants et des photos en ligne, puisse porter atteinte à la vie privée d'un enfant, favoriser les actes d'intimidation à son encontre, le mettre dans l'embarras ou avoir des conséquences négatives pour sa vie future[32]. Les parents d'enfants handicapés peuvent partager ce type d'information pour solliciter un appui ou un conseil, exposant ainsi les enfants handicapés à un risque accru de subir des conséquences préjudiciables.

Certains enfants handicapés peuvent avoir des difficultés à utiliser les plates-formes en ligne, voire en être exclus, parce que ces plates-formes sont conçues d'une façon qui ne leur est

---

28 Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content" (Sollicitation, harcèlement et contenu problématique), *Berkman Center for Internet & Society, Harvard University*, Décembre 2008, 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

29 UNICEF, "La situation des enfants dans le monde: Les enfants handicapés," 2013, https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

30 Katrin Mueller-Johnson, Manuel P. Eisner, et Ingrid Obsuth, "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors" (Agression sexuelle sur des jeunes en situation de handicap physique: examen des taux de prévalence, et facteurs de risque et de protection), *Journal of Interpersonal Violence* 29, N° 17 (novembre 2014): 3180-3206, https://doi.org/10.1177/0886260514534529.

31 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder" (Fétichistes, prétendants et aspirants: deux cas de maladies handicapantes factices), *Sexual and Disability* 15, N° 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

32 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy" (Vie privée de l'enfant à l'ère du web 2.0 et 3.0: défis et perspectives pour les politiques), Innocenti Discussion Paper 2017-03 (Centre de recherche de l'UNICEF – Innocenti), page consultée le 1er juillet 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

pas accessible (c'est le cas, par exemple, des applications qui ne permettent pas d'augmenter la taille du texte), parce qu'ils se sont vu refuser les facilités demandées (logiciel de lecture d'écran ou commandes informatiques adaptatives, par exemple), ou parce qu'ils ont besoin d'un appui adéquat (accompagnement sur les modalités d'utilisation des équipements ou soutien individuel pour apprendre à gérer les interactions sociales[33], par exemple).

En ce qui concerne les risques liés à un contrat ou à la signature des conditions générales, les enfants handicapés sont plus susceptibles d'accepter des conditions juridiques qui peuvent parfois échapper à la compréhension même des adultes.

2.7 Perception que les enfants ont des risques en ligne

Une exposition à la violence dans le monde entier, un accès à des contenus, des biens et des services inappropriés, des problèmes d'utilisation excessive, des questions liées à la protection des données et à la vie privée sont autant de risques que les enfants ont mentionnés[34].

Les adolescents signalent un éventail de préoccupations concernant leur utilisation des technologies numériques. Ce sont notamment les inquiétudes les plus courantes liées à la sécurité en ligne, comme la crainte d'interagir avec des inconnus en ligne, d'accéder à des contenus inappropriés ou d'être exposés à des logiciels malveillants ou à des virus. D'autres concernent la fiabilité de leur accès aux technologies, l'intrusion de leurs parents dans leur vie "privée" en ligne, et leur utilisation des outils numériques[35].

Les travaux de recherche du réseau EU Kids Online révèlent que la pornographie et les contenus violents figurent au premier rang des préoccupations en ligne des enfants en Europe. De manière générale, les garçons semblent plus contrariés par la violence, tandis que les filles se sentent plus exposées aux risques liés aux contacts[36]. Les préoccupations quant aux risques sont plus marquées chez les enfants issus de pays où les niveaux d'utilisation et de risque sont particulièrement élevés.

En Amérique latine, il est ressorti des consultations menées auprès des enfants que les principales préoccupations concernent les atteintes à la vie privée, la violence et le harcèlement[37]. Les enfants signalent être contactés par des personnes qu'ils ne connaissent pas – surtout lorsqu'ils jouent à des jeux en ligne. Dans de telles situations, il semble que la principale stratégie adoptée consiste à ne pas entrer en contact avec la personne et/ou à la bloquer. Les filles sont confrontées au harcèlement sur les réseaux sociaux dès leur plus jeune âge. Elles parviennent à surmonter ces formes de violences par elles-mêmes, en bloquant les utilisateurs et en modifiant les paramètres de confidentialité. Il arrive que le harcèlement soit pratiqué par des utilisateurs

---

33 Des lignes directrices sur ces droits sont énoncées dans la Convention relative aux droits des personnes handicapées, en particulier l'Article 9 (accessibilité) et l'Article 21 (liberté d'expression et d'opinion, et accès à l'information).

34 Amanda Third et al., "Children's Rights in the Digital Age" (Droits de l'enfant à l'ère du numérique), (Melbourne: Young and Well Cooperative Research Centre, septembre 2014), http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

35 Amanda Third et al., "Young and Online: Children's Perspectives on Life in the Digital Age" (Jeunes et connectés: perspectives pour les enfants à l'ère du numérique), The State of the World's Children 2017 Companion Report (Sydney: Western Sydney University, 2017). Ce rapport fait la synthèse des opinions recueillies auprès de 490 enfants âgés de 10 à 18 ans, issus de 26 pays différents, pour un total de 24 langues officielles.

36 Livingstone, S. (2014) *EU Kids Online: Findings, methods, recommendations* (EU Kids Online: Résultats, méthodes et recommandations). LSE, London: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.

37 Conectados al Sur network, "Hablatam".

qui ne parlent pas l'espagnol, mais qui parviennent à leur envoyer des images, des demandes d'amitié, ou à commenter leurs publications. Certains garçons disent avoir reçu eux aussi ce genre de sollicitations.

Dans de nombreuses régions du monde, les enfants ont une bonne compréhension de certains des risques auxquels ils sont exposés en ligne[38]. Il ressort des travaux de recherche que la majorité des enfants sont en mesure de distinguer le cyberharcèlement des plaisanteries ou des vexations en ligne, et qu'ils sont conscients que le cyberharcèlement revêt une dimension publique et qu'il vise à nuire[39].

3 Jeter les bases d'une stratégie nationale en matière de protection en ligne des enfants

En vue d'élaborer une stratégie nationale en matière de protection en ligne des enfants pour promouvoir la sécurité en ligne des enfants et des jeunes, les gouvernements nationaux et les instances décisionnelles doivent recenser les bonnes pratiques en la matière et collaborer avec les principales parties prenantes.

Les sections suivantes présentent les acteurs et les parties prenantes traditionnels, ainsi que le rôle et les responsabilités qu'ils pourraient assumer en matière de protection en ligne des enfants.

3.1 Acteurs et parties prenantes

Les décideurs peuvent identifier des individus, des groupes et des organisations ayant les compétences requises et représentant chacun de ces acteurs et chacune de ces parties prenantes au sein de leur juridiction. Il importe d'avoir une bonne compréhension de chacune des activités en cours, planifiées ou envisagées pour coordonner et orchestrer, au niveau national, les stratégies en matière de protection en ligne des enfants.

Enfants et jeunes

Les enfants et les jeunes du monde entier font montre d'une très grande capacité d'adaptation en ce qui concerne l'utilisation des nouvelles technologies. À la fois plate-forme de travail, de jeu et de communication, l'Internet est de plus en plus présent dans les écoles.

D'après le dernier rapport de l'Alliance ChildFund, seulement 18,1% des enfants interrogés pensent que les personnes qui gouvernent agissent en vue de les protéger. Il est important que les décideurs collaborent avec les enfants à cet égard et qu'ils reconnaissent le droit des enfants d'être entendus (Article 12 de la Convention relative aux droits de l'enfant).

Pour être en mesure de protéger les enfants, les décideurs devraient harmoniser la définition du terme "enfant" dans tous les documents juridiques. Par définition, un enfant devrait désigner tout individu âgé de moins de dix-huit ans, conformément à l'Article 1 de la Convention des Nations Unies relative aux droits de l'enfant, aux termes de laquelle "un enfant s'entend de tout

[38] Depuis 2016, l'UIT organise des consultations sur le thème de la protection en ligne des enfants, avec des parties prenantes représentant des enfants et des adultes, sur des questions importantes telles que le cyberharcèlement, la maîtrise des outils numériques et les activités des enfants en ligne.

[39] UNICEF, "Global Kids Online Comparative Report (2019)".

être humain âgé de moins de dix-huit ans". Les entreprises ne devraient pas être autorisées à traiter comme un adulte tout individu âgé de moins de 18 ans mais suffisamment âgé au regard de la loi pour autoriser le traitement des données. Cette définition étroite ne s'appuie sur aucune donnée relative aux étapes décisives du développement de l'enfance. Elle porte atteinte aux droits de l'enfant et représente une menace pour sa sécurité.

Bon nombre d'enfants peuvent sembler à l'aise avec l'utilisation des technologies, mais nombreux sont ceux qui ne se sentent pas en sécurité[40] en ligne et ont plusieurs préoccupations[41] concernant l'Internet.

Les enfants et les jeunes manquent d'expérience de la vie en général, ce qui peut les rendre vulnérables à de nombreux risques. Ils sont en droit d'attendre une aide et une protection. Il est important de se rappeler également que tous les enfants et les jeunes n'expérimenteront pas l'Internet et les nouvelles technologies de la même manière. Les enfants qui ont des besoins particuliers en raison d'incapacités physiques ou autres sont, par exemple, plus vulnérables dans le cyberespace et nécessitent une assistance complémentaire.

Des enquêtes ont révélé à maintes reprises qu'il pouvait exister des décalages très importants entre ce que les adultes pensent et ce que les enfants et les jeunes font réellement dans le cyberespace. La moitié des enfants interrogés ont déclaré que, dans leur pays, les adultes n'écoutent pas leur avis sur des questions qui comptent pour eux[42]. Pour cette raison, il est important de trouver des mécanismes appropriés – quelles que soient les dispositions prises au niveau national pour élaborer des politiques dans ce domaine – pour que les enfants et les jeunes puissent s'exprimer et qu'il soit tenu compte de la façon dont ils utilisent vraiment la technologie.

Parents, tuteurs et éducateurs

Les parents, tuteurs et éducateurs passent le plus de temps avec les enfants. Il faudrait leur permettre d'acquérir une éducation numérique afin qu'ils comprennent le cyberspace et qu'ils soient capables de protéger les enfants et de leur apprendre comment se protéger.

Il incombe en particulier aux établissements d'enseignement d'apprendre aux enfants comment naviguer en ligne en toute sécurité, qu'ils utilisent l'Internet à l'école, chez eux ou ailleurs. Les décideurs devraient quant à eux inclure dans les programmes scolaires nationaux un volet sur la maîtrise des outils numériques aussi tôt que possible (3-18 ans). De cette manière, les enfants pourraient être en mesure de se protéger, connaîtraient leurs droits et partant, utiliseraient l'Internet en tant que catalyseur du savoir[43].

Il convient de rappeler aux décideurs que les parents et les tuteurs sont presque toujours pour leurs enfants le premier, le dernier et le meilleur moyen de défense et d'assistance. Pourtant,

---

40 Alliance ChildFund, "Violence against children as explained by children" (La violence à l'égard des enfants expliquée par les enfants), Save Voices Big Dreams, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

41 Conseil de l'Europe, "Ce monde est le nôtre: l'avis des enfants sur la protection de leurs droits dans l'environnement numérique", Rapport sur les consultations avec les enfants (Conseil de l'Europe, Division des droits des enfants, octobre 2017), https://edoc.coe.int/en/children-and-the-internet/8012-ce-monde-est-le-notre-lavis-des-enfants-sur-la-protection-de-leurs-droits-dans-lenvironnement-numerique-.html#.

42 Alliance ChildFund, "Violence against children as explained by children".

43 UNICEF, "Policy Guide on Children and Digital Connectivity" (Guide des politiques sur les enfants et la connectivité numérique) (Policy Lab, Data, Research and Policy, United Nations Children's Fund, juin 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

lorsque l'on pénètre la sphère de l'Internet, ils peuvent sembler quelque peu perdus. Les écoles ont là encore un rôle majeur à jouer pour dialoguer avec les parents et les tuteurs et les sensibiliser à la fois aux risques et aux nombreux effets positifs engendrés par les nouvelles technologies. Toutefois, les écoles ne doivent pas constituer l'unique moyen de s'adresser aux parents et aux tuteurs. Il est en effet important d'utiliser tout l'éventail des canaux disponibles pour sensibiliser le plus grand nombre possible de parents et de tuteurs. Ainsi, les entreprises ont un rôle important à jouer en vue de fournir un appui les utilisateurs ou leurs clients. Les parents et les tuteurs peuvent choisir de gérer les activités en ligne et l'accès à l'Internet de leur enfant, discuter avec lui du bon comportement à avoir et du bon usage des technologies et comprendre ce qu'il fait en ligne, de sorte que les discussions en famille abordent les expériences du monde virtuel et celles du monde réel comme un tout.

Les parents et les tuteurs doivent aussi servir d'exemple à leurs enfants quant à la façon d'utiliser leurs dispositifs et de se comporter correctement sur l'Internet.

Il convient de rappeler aux décideurs que les parents et les tuteurs devraient être consultés afin de connaître leur perception, leur expérience et leur compréhension de la protection en ligne de leurs enfants.

Enfin, les décideurs, en coopération avec d'autres institutions publiques, peuvent élaborer des campagnes de sensibilisation du public, notamment des parents, des personnes qui s'occupent d'enfants et des éducateurs. Les bibliothèques municipales, les centres de santé et même les centres commerciaux et d'autres grands centres de commerce peuvent offrir un espace accessible pour la présentation d'informations sur la sécurité en ligne et les compétences numériques. Lorsqu'ils mettent en œuvre ces initiatives, les gouvernements doivent s'assurer que les conseils sont donnés de manière neutre, qu'ils ne servent aucun intérêt privé et qu'ils couvrent un large éventail de questions qui se posent au sein de l'espace numérique.

Professionnels

Les professionnels du secteur figurent parmi les principaux acteurs de l'écosystème, étant donné qu'ils possèdent les connaissances techniques que les décideurs doivent examiner et comprendre pour élaborer le cadre juridique. Par conséquent, il va de soi que les décideurs associent les professionnels au processus d'élaboration des lois sur la protection en ligne des enfants.

En outre, il importe d'encourager les entreprises à suivre une approche qui intègre la sécurité dès la conception lorsqu'elles mettent au point une nouvelle technologie. Il est clair que les sociétés qui développent ou fournissent actuellement des produits et des services fondés sur les nouvelles technologies devraient aider les utilisateurs à comprendre leurs modalités de fonctionnement ainsi que la manière de les utiliser correctement et en toute sécurité.

Les entreprises ont également un devoir d'information vis-à-vis des enfants et des adolescents, de leurs parents ou de leurs tuteurs et de la communauté au sens large, sur les questions liées aux activités et à la sécurité en ligne. En agissant ainsi, les parties prenantes du secteur pourront en savoir plus sur les inquiétudes des autres parties prenantes ainsi que sur les risques et les dangers auxquels les utilisateurs finals sont exposés. Forts de ces renseignements, les professionnels pourraient améliorer les produits et les services existants, et recenser les dangers potentiels.

Grâce aux progrès récents en matière d'intelligence artificielle, les entreprises ont commencé à élaborer des mécanismes d'équilibre davantage solides pour identifier l'utilisateur et offrir aux

enfants un environnement favorisant un comportement positif en ligne. Ces progrès pourraient aussi présenter de nouveaux risques pour les enfants.

Dans certains pays, l'Internet est régi par un cadre d'autoréglementation ou de réglementation commune. Toutefois, certains pays envisagent, ou ont déjà mis en œuvre, des cadres juridique et réglementaire, qui prévoient notamment l'obligation pour les sociétés de détecter, de bloquer et/ou de supprimer les dangers auxquels sont exposés les enfants sur les plates-formes ou les services, et de mettre à disposition des mécanismes de signalement et d'assistance clairs.

Chercheurs et organisations non gouvernementales

Au sein des universités et du monde de la recherche, il n'est pas rare de trouver une multitude d'universitaires et de chercheurs qui étudient et connaissent parfaitement les conséquences sociales et techniques de l'Internet. Ces acteurs apportent une contribution précieuse aux gouvernements nationaux et aux décideurs chargés d'élaborer des stratégies fondées sur des données factuelles et probantes. Ils peuvent également servir de contrepoids intellectuel face aux entreprises dont les intérêts sont parfois court-termistes et de nature commerciale.

De la même manière, les organisations non gouvernementales (ONG) sont une mine précieuse de compétences spécialisées et d'informations permettant de sensibiliser les enfants, les parents, les éducateurs et les personnes s'occupant d'enfants, et de leur fournir des services, pour contribuer à promouvoir les activités liées à la sécurité en ligne et, de manière générale, à œuvrer en faveur de l'intérêt général.

Organismes d'application de la loi

Aussi merveilleuse soit-elle, la technologie attire malgré elle les criminels et les comportements antisociaux. Force est de constater que l'Internet a considérablement accru la circulation de matériel montrant des abus sexuels sur des enfants et d'autres dangers. Les prédateurs sexuels utilisent l'Internet pour entrer en contact avec les enfants et les attirer dans leurs filets, dans le monde virtuel comme dans le monde réel. Les actes d'intimidation et les autres formes de harcèlement peuvent avoir de graves conséquences sur la vie des enfants, et l'Internet a ouvert de nouvelles portes dans ce domaine.

Il est dès lors essentiel, au vu de ces éléments, d'associer pleinement les organismes d'application de la loi à l'élaboration des stratégies globales visant à rendre l'Internet plus sûr pour les enfants et les adolescents. Les agents de la force publique ont besoin d'une formation adaptée pour pouvoir mener des enquêtes sur les cybercrimes commis contre les enfants et les adolescents. Ils doivent disposer des compétences techniques nécessaires et pouvoir accéder aux moyens de police scientifiques pour pouvoir extraire et interpréter les données issues des ordinateurs ou de l'Internet, le plus rapidement possible.

Les organismes d'application de la loi doivent par ailleurs instaurer des mécanismes clairs permettant aux enfants et aux jeunes de signaler des cas d'abus ainsi qu'à toute autre personne de signaler un incident ou une inquiétude concernant la sécurité en ligne d'un enfant ou d'un jeune. À titre d'exemple, de nombreux pays ont mis en place des lignes d'assistance téléphonique pour permettre de signaler plus facilement des cas relatifs à du matériel montrant des abus sexuels sur des enfants. Des mécanismes similaires existent pour le signalement d'autres problèmes, par exemple les cas de harcèlement. Les décideurs devraient travailler en coopération avec l'Association internationale des centres de téléassistance Internet (INHOPE), pour aider à évaluer et traiter les signalements concernant des contenus montrant des abus

sexuels sur des enfants et permettre à des organisations du monde entier de tirer parti de l'assistance de l'Association INHOPE lorsqu'elles mettent en place des lignes d'assistance téléphonique là où il n'y en a pas. Les décideurs devraient veiller à ce qu'il existe des canaux de communication ouverts entre les organismes d'application de la loi et les autres parties prenantes. Les forces de police sont la principale source auprès de laquelle obtenir du matériel montrant des abus sexuels sur des enfants saisi sur le territoire national. Elles entament ensuite une procédure d'enquête pour déterminer s'il est possible d'identifier des victimes au niveau local. En cas d'échec, le matériel est transmis à INTERPOL et enregistré dans la base de données internationale sur l'exploitation sexuelle des enfants (ICSE). Compte tenu de la portée mondiale de cette menace, les décideurs doivent garantir une coopération internationale entre les organismes d'application de la loi du monde entier. On pourrait ainsi réduire la durée des processus formels et permettre aux agents d'obtenir une réponse plus rapide.

Services sociaux

Les enfants et les jeunes qui ont été maltraités ou abusés en ligne (par exemple, une photo d'eux indécente ou illégale a été diffusée en ligne) ont très souvent besoin d'un appui ou de conseils spécialisés sur le long terme. Il peut aussi s'avérer nécessaire de mettre en place des services ou un suivi thérapeutique pour les auteurs des abus, en particulier pour lorsqu'il sont jeunes et ont pu également subir des abus dans le monde virtuel ou réel. Les professionnels des services sociaux devront recevoir une formation adaptée pour être en mesure de dispenser ce type d'aide, qu'il convient de fournir aussi bien via des canaux en ligne que des canaux hors ligne.

Services de santé

Les soins de santé nécessaires après tout cas de violence à l'encontre d'un enfant devraient être couverts par l'assurance maladie de base au niveau national. Les établissements de santé devraient signaler obligatoirement les abus. Les professionnels de la santé devraient être suffisamment équipés et informés afin de pouvoir fournir un appui aux enfants à cet égard. Il faudrait élargir le champ d'action des services de santé pour inclure un appui à la santé mentale et au bien-être des enfants.

Ministères

La politique de protection en ligne des enfants relèvera de la juridiction d'un certain nombre de ministères. Il est donc important de susciter la collaboration de tous les ministères concernés afin que toute stratégie nationale et tout plan d'action soient couronnés de succès. Il peut s'agir, notamment, des entités publiques suivantes:

- Ministère de l'intérieur
- Ministère de la santé
- Ministère de l'éducation
- Ministère de la justice
- Ministère du numérique/de l'information
- Régulateurs

Les régulateurs sont les mieux placés pour contribuer au rôle de contrôleur et de comptable, en collaboration avec les institutions gouvernementales. Il peut s'agir notamment des régulateurs s'occupant des médias et de la protection des données.

Opérateurs de réseaux large bande, mobiles et WiFi

Les opérateurs peuvent détecter, bloquer et signaler des contenus illicites dans leur réseau et fournir des outils, des services et des configurations accessibles aux familles, que les parents pourront utiliser pour choisir comment gérer l'accès de leurs enfants. Il est important que les fournisseurs s'assurent également que les libertés civiles et la vie privée sont respectées.

Droits de l'enfant

Les institutions indépendantes spécialisées dans la défense des droits fondamentaux des enfants peuvent jouer un rôle crucial pour assurer la sécurité des enfants en ligne. Même si elles ont des mandats différents, ces institutions sont habilitées à:

- surveiller les effets du droit, des politiques et de la pratique sur la protection des droits de l'enfant;
- promouvoir la mise en œuvre des normes internationales en matière de droits de l'homme au niveau national;
- enquêter sur des cas de violation des droits de l'enfant;
- fournir aux tribunaux des services d'expert sur les droits de l'enfant;
- veiller à ce que les opinions des enfants soient prises en considération dans les affaires touchant à leurs droits fondamentaux, y compris pour l'élaboration de lois et de politiques pertinentes;
- promouvoir la compréhension et la connaissance par la population des droits de l'enfant; et
- organiser des activités d'éducation et de formation en matière de droits de l'homme.

Il est important d'organiser des consultations directes avec les enfants. C'est un droit qui leur est accordé en vertu de l'Article 12 de la Convention des Nations Unies relative aux droits de l'enfant. Les fonctions de conseil, d'enquête, de sensibilisation et d'éducation des institutions indépendantes spécialisées dans la défense des droits fondamentaux des enfants sont toutes utiles pour éviter les dangers que les enfants peuvent rencontrer en ligne et intervenir le cas échéant. C'est pourquoi ces institutions devraient occuper une place centrale dans l'élaboration d'une approche exhaustive et fondée sur les droits pour renforcer les cadres juridique, réglementaire et politique régissant la protection en ligne des enfants, y compris en engageant des consultations directes avec les enfants, conformément au droit qui leur est accordé en vertu de l'Article 12 de la Convention des Nations Unies relative aux droits de l'enfant.

Récemment, il a été observé que certaines juridictions ont mis en place – ou envisagé de mettre en place – des entités étatiques chargées spécialement d'appuyer les droits de l'enfant en ligne, y compris de protéger les enfants contre les violences ou les dangers. Lorsqu'elles existent, ces entités devraient participer étroitement aux efforts déployés pour renforcer les mesures visant à assurer la protection en ligne des enfants au niveau national.

3.2 Mesures appliquées en matière de protection en ligne des enfants

Plusieurs initiatives ont été élaborées en vue d'agir aux niveaux national et international face à la place de plus en plus grande qu'occupent les TIC dans la vie des enfants du monde entier et aux risques inhérents pour les plus jeunes dans nos sociétés.

Modèles nationaux

Au niveau national, il convient de mettre en avant plusieurs législations qui couvrent des aspects importants d'un cadre exhaustif en matière de protection en ligne des enfants. Il s'agit notamment, mais non exclusivement:

- de la Directive sur les services de médias audiovisuels (AVMSD) (révisée en 2018, Union européenne); et
- du Règlement général sur la protection des données (GDPR) (2018, Union européenne).

Dans le cadre des mesures réglementaires et institutionnelles prises par les États Membres pour lutter contre les menaces à l'égard de la sécurité et du bien-être des enfants en ligne, des initiatives innovantes ont vu le jour. Il n'existe pas de solution unique aux problèmes que posent le matériel montrant des abus sexuels sur des enfants, le cyberharcèlement et d'autres dangers auxquels les enfants sont exposés en ligne, mais il convient de noter que de nouvelles approches ont été expérimentées ces dernières années.

Code de conception adaptée à l'âge (2019, Royaume-Uni)

Début 2019, le Bureau du commissaire à l'information a publié des propositions relatives à son "code de conception adaptée à l'âge" en vue de renforcer la protection en ligne des enfants. Le code proposé est axé sur l'intérêt supérieur de l'enfant, tel qu'énoncé dans la Convention des Nations Unies relative aux droits de l'enfant, et définit plusieurs attentes à l'égard des entreprises, notamment à ce que des mesures solides de vérification de l'âge soient appliquées, que les services de localisation soient par défaut désactivés pour les enfants, que les entreprises recueillent et conservent seulement la quantité minimale de données personnelles concernant les enfants, que les produits intègrent des principes de sécurité dès la conception, et que les explications soient compréhensibles et adaptées à l'âge.

Loi sur les communications numériques préjudiciables (révisée en 2017, Nouvelle-Zélande)

La loi de 2015 a érigé spécifiquement en délit les abus perpétrés en ligne. Elle aborde un large éventail de dangers, allant du cyberharcèlement à la pornodivulgation (*revenge porn*). Cette loi vise à empêcher, à prévenir et à réduire les communications numériques préjudiciables, en rendant illégale la publication d'une communication numérique dans le but de causer une détresse émotionnelle grave à autrui, et définit une série de dix principes applicables aux communications. Elle met à disposition des utilisateurs les moyens de déposer une plainte devant un organisme indépendant si ces principes sont bafoués ou de saisir la juridiction compétente pour qu'elle prononce une ordonnance à l'encontre de l'auteur ou de l'hôte de la communication si le problème n'est pas résolu.

Commissaire à la sécurité en ligne (2015, Australie)

Le Commissaire à la sécurité en ligne (*eSafety Commissioner*) est le tout premier organisme public spécifiquement dédié à la sécurité en ligne. Créé en 2015, eSafety assure une fonction législative de direction, de coordination, d'éducation et de conseil pour les questions liées à la sécurité en ligne afin de veiller à ce que tous les Australiens aient une expérience sûre, positive et participative en ligne. eSafety administre des dispositifs d'investigation qui concernent un éventail de préjudices, dont des actes de cyberharcèlement graves à l'encontre d'enfants, des abus fondés sur des images et des contenus interdits. Il est habilité à mener des enquêtes et à prendre des mesures en cas de plaintes ou de signalements concernant ces types de danger et, dans certains cas, à publier des notifications à l'intention de particuliers et de services en

ligne pour obtenir le retrait du matériel. En plus de ses compétences en matière d'enquête, eSafety adopte une approche faisant intervenir tous les acteurs de la société, qui s'appuie sur des initiatives et des interventions sociales, culturelles et techniques. Les efforts qu'il déploie en matière de prévention, de protection et d'anticipation offrent une approche exhaustive de la sécurité en ligne.

Modèles internationaux

Aux niveaux international et transnational, des recommandations et des normes ont été publiées par différentes parties prenantes. Les présentes lignes directrices se fondent sur les travaux menés dans le cadre des initiatives et des travaux suivants:

Lignes directrices relatives à la mise en œuvre du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants.

Lignes directrices du Conseil de l'Europe relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique[44].

Ces lignes directrices s'adressent à tous les États Membres du Conseil de l'Europe et ont pour objet de fournir une assistance aux États Membres et aux autres parties prenantes concernées dans les efforts déployés pour adopter une approche exhaustive et stratégique afin de faire respecter autant que possible tous les droits de l'enfant dans l'environnement numérique. Parmi les nombreux sujets couverts figurent la protection des données personnelles, la fourniture de contenus adaptés aux enfants compte tenu de l'évolution de leurs capacités, les services téléphoniques d'urgence (*helpline*) et les lignes d'assistance téléphonique (*hotline*) et, la vulnérabilité et la résilience, ainsi que le rôle et les responsabilités des entreprises commerciales. De plus, aux termes des lignes directrices, les États sont appelés à collaborer avec les enfants, notamment dans les processus de prise de décision, pour veiller à ce que les politiques nationales couvrent comme il convient les progrès au sein de l'environnement numérique. Ces lignes directrices sont actuellement disponibles dans 19 langues. Elles seront assorties d'une version adaptée aux enfants ainsi que d'un manuel à l'intention des décideurs, qui fournira des indications concrètes sur les modalités d'application.

Conseil de l'Europe – Convention de Lanzarote

La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote) appelle les États à apporter une réponse globale à la violence sexuelle à l'encontre des enfants, en adoptant une approche fondée sur la prévention, la protection, le droit pénal et la promotion d'une coopération nationale et internationale (approche des "4P"). Les activités relatives à l'environnement numérique prévues au titre de la Convention ont été clairement définies par le Comité des Parties à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (ci-après le "Comité de Lanzarote"), avec l'adoption d'un certain nombre de documents, dont un Avis sur les images et/ou vidéos d'enfants sexuellement suggestives ou explicites produites, partagées ou reçues par des enfants (6 juin 2019); un Avis interprétatif sur l'applicabilité de la Convention de Lanzarote aux infractions sexuelles commises à l'encontre des enfants et facilitées par

[44] Conseil de l'Europe (2020), L'environnement numérique, https://www.coe.int/fr/web/children/the-digital-environment. Les lignes directrices du Conseil de l'Europe relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique sont le tout premier ensemble de normes en la matière adoptées par un organe intergouvernemental (CM/Rec, 2018).

l'utilisation des technologies de l'information et de la communication (TIC) (12 mai 2017); une Déclaration sur les adresses Internet faisant la publicité ou la promotion de matériels ou d'images en rapport avec des abus sexuels à l'encontre d'enfants ou de toutes autres infractions établies conformément à la Convention de Lanzarote (16 juin 2016); et un Avis sur l'Article 23 de la Convention de Lanzarote – Sollicitation d'enfants à des fins sexuelles par le biais des technologies de l'information et de la communication ("grooming"). Le Comité de Lanzarote assure le suivi de la mise en œuvre de la Convention. Ainsi, le deuxième cycle de suivi thématique du Comité est axé sur la protection des enfants contre l'exploitation sexuelle et les abus sexuels facilités par les TIC, avec la publication future d'un rapport sur cette question en 2020. En 2019, la Convention comptait 46 États parties, dont la Tunisie – premier État non-membre à adhérer à la Convention.

Autres lignes directrices du Conseil de l'Europe

D'autres normes et outils du Conseil de l'Europe contribuent aux acquis communautaires en vue de l'élaboration d'un cadre complet à l'intention de toutes les parties prenantes. La Convention du Conseil de l'Europe sur la cybercriminalité contient des obligations qui imposent aux Parties d'ériger en infraction pénale un ensemble d'infractions liées aux contenus montrant des abus sexuels sur les enfants. À l'heure actuelle, cette Convention a été ratifiée par 64 États parties. Le Conseil de l'Europe se concentre, entre autres, sur l'autonomisation des enfants et de ceux qui les entourent afin qu'ils puissent naviguer en toute sécurité dans l'environnement numérique. Pour ce faire, elle a élaboré des outils pédagogiques, dont un Manuel entièrement révisé sur les compétences dans le domaine de l'Internet (2017), un Manuel pédagogique sur la citoyenneté numérique (2019) et des manuels à l'intention des parents (La parentalité à l'ère du numérique – Conseils aux parents pour la protection en ligne des enfants contre l'exploitation sexuelle et les abus sexuels (2017); La citoyenneté numérique... et votre enfant: ce que tout parent a besoin de savoir et de faire (2019)). Enfin, le Conseil de l'Europe a effectué des recherches en menant des consultations auprès des enfants sur leurs droits dans l'environnement numérique (Ce monde est le nôtre: l'avis des enfants sur la protection de leurs droits dans l'environnement numérique (2017)) et a effectué, en collaboration avec des enfants, les premières recherches axées sur l'expérience des enfants handicapés dans le monde numérique (Deux clics en avant et un clic en arrière – Rapport sur les enfants en situation de handicap dans l'environnement numérique (2019)).

Rapport sur la sécurité en ligne des enfants

Rapport "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online" (Sécurité en ligne des enfants: réduire autant que faire se peut le risque de violence, d'abus et d'exploitation en ligne) et Déclaration universelle sur la sécurité en ligne des enfants[45].

Recommandations de l'OCDE sur la protection en ligne des enfants (2012/révisées en 2019-2020)

Il convient de mettre en avant d'autres initiatives nationales et transnationales qui favorisent la coopération internationale ainsi que les efforts nationaux en vue d'élaborer des stratégies en matière de protection en ligne des enfants. Il s'agit notamment des initiatives suivantes:

Base de données internationale sur l'exploitation sexuelle des enfants

[45] Commission "Le large bande au service du développement durable" (2019), *The State of Broadband 2019: Broadband as Foundation for Sustainable Development* (La situation du large bande en 2019: le large bande en tant que fondement du développement durable) https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

Gérée par INTERPOL, la base de données internationale sur l'exploitation sexuelle des enfants (ICSE) est un outil efficace de renseignement et d'enquête qui permet à des enquêteurs spécialisés d'échanger des données avec leurs collègues du monde entier. Disponible via le système mondial sécurisé de communication policière d'INTERPOL (I-247), la base de données ICSE utilise un logiciel évolué de comparaison d'images pour faire le lien entre des victimes, des agresseurs et des lieux. Les utilisateurs certifiés dans les pays membres peuvent accéder à la base de données ICSE en temps réel – pour consulter les contenus existants; télécharger de nouvelles données; trier, classer et harmoniser les contenus; effectuer des analyses et communiquer avec d'autres experts du monde entier pour donner suite à des demandes ayant trait aux enquêtes sur l'exploitation sexuelle d'enfants.

Alliance mondiale WePROTECT

L'Alliance mondiale WePROTECT est une initiative mondiale qui rassemble les ressources, les compétences et les influences nécessaires pour révolutionner la manière dont l'exploitation sexuelle d'enfants en ligne est traitée dans le monde. Il s'agit d'un partenariat entre des gouvernements, des entreprises internationales du secteur des technologies et des organisations de la société civile qui, du fait de son caractère multipartite, n'a pas son pareil dans ce domaine. L'Alliance mondiale WePROTECT vise à identifier et à protéger davantage de victimes, à arrêter davantage d'auteurs de ce type d'agression, et à mettre fin à l'exploitation sexuelle d'enfants en ligne.

L'Alliance mondiale WePROTECT a mis au point un certain nombre d'instruments, en particulier un modèle d'intervention nationale et une stratégie d'intervention mondiale. L'Appendice 3 contient des informations supplémentaires à cet égard.

L'Indice 2020 de la sécurité en ligne de l'enfant

L'Institut DQ a élaboré l'Indice 2020 de la sécurité en ligne de l'enfant (COSI), qui constitue la toute première plate-forme mondiale d'analyse en temps réel pour aider les pays à mieux suivre la situation de la sécurité en ligne des enfants à l'échelle nationale.

L'Indice COSI se fonde sur six piliers, lesquels composent le cadre de l'Indice COSI. Les piliers un (cyberrisque) et deux (discipline dans l'utilisation des outils numériques) ont trait à une utilisation judicieuse de la technologie numérique. Les piliers trois (compétences numériques) et quatre (orientation et éducation) portent sur l'autonomisation. Les deux derniers piliers (infrastructure sociale et connectivité) concernent l'infrastructure.

3.3 Exemples de mesures prises pour lutter contre les dangers en ligne

On trouvera dans l'Appendice 4 un certain nombre d'exemples de mesures prises pour lutter contre les dangers en ligne. Ces exemples illustrent aussi bien des mesures éducatives que des mesures législatives et d'identification des dangers en ligne.

3.4 Avantages d'une stratégie nationale en matière de protection en ligne des enfants

Harmonisation des lois

L'adoption par tous les pays d'une législation appropriée pour lutter contre l'usage abusive des TIC, notamment à des fins criminelles, est essentielle pour instaurer la cybersécurité dans le monde. Les menaces pouvant provenir de toutes parts, les défis à relever ne connaissent pas de frontière et appellent une coopération internationale, une assistance en matière d'enquête ainsi que des dispositions communes de fond et de procédure. Il est donc important que les pays harmonisent leurs cadres législatifs pour combattre la cybercriminalité, protéger les enfants en ligne et faciliter la coopération internationale[46].

Le développement de législations nationales appropriées, la mise en place d'un cadre juridique contre la cybercriminalité et l'harmonisation au niveau international sont autant d'étapes vers le succès des stratégies nationales dédiées à la protection des enfants dans le cyberespace. À cet égard, il faut tout d'abord mettre en place les dispositions de fond en droit pénal afin d'ériger en délit les actes de fraude informatique, d'accès illicite, d'atteinte à l'intégrité des données ou à la propriété intellectuelle et de détention de matériel montrant des abus sexuels sur des enfants, tout en veillant à ne pas sanctionner à tort les enfants. Le fait que de telles dispositions existent dans le code pénal pour des actes similaires commis dans le monde réel ne signifient pas que ces dispositions peuvent également être appliquées aux actes commis dans le monde virtuel. La législation nationale en vigueur doit par conséquent être passée au crible pour que soient repérés les éventuels vides. L'étape suivante consiste à identifier et à définir les termes et les documents législatifs qui pourraient aider les pays à édicter des règles de procédure et des lois harmonisées contre la cybercriminalité. De tels instruments pratiques peuvent également être utilisés par les pays pour élaborer un cadre juridique sur la cybersécurité et des lois correspondantes. L'UIT œuvre en ce sens avec les États Membres et les différentes parties prenantes et contribue grandement à promouvoir l'harmonisation des lois contre la cybercriminalité au niveau mondial.

Compte tenu du rythme soutenu de l'innovation technique, l'autoréglementation et la réglementation commune ont été présentées comme des solutions potentielles à l'obsolescence de la réglementation existante et au caractère chronophage du processus législatif. Toutefois, à des fins d'efficacité, les régulateurs/décideurs doivent définir clairement des objectifs et des problèmes à résoudre en matière de protection en ligne des enfants, mettre en place un processus et une méthode d'examen clairs pour évaluer l'efficacité des mesures d'autoréglementation et de réglementation commune et, dans le cas où ces mesures ne permettraient pas de résoudre les problèmes définis, entamer un processus législatif en bonne et due forme pour y parvenir. De plus, les mesures d'autoréglementation ayant fait leurs preuves pourraient être adoptées progressivement dans le droit formel, dans le cadre du processus législatif, pour servir de filet de sécurité juridique et éviter un recul ou une cessation de l'adhésion à certaines initiatives d'autoréglementation.

Coordination

Il est probable, au vu de la diversité des acteurs et des parties prenantes, qu'il existe déjà un éventail d'activités et de mesures visant à protéger les enfants en ligne, mais que celles-ci aient été mises en œuvre de manière isolée. Il est important d'en avoir connaissance pour comprendre quels sont les efforts actuellement menés pour élaborer une stratégie nationale relative à la protection en ligne des enfants. La stratégie permettra de coordonner et d'orienter les efforts en orchestrant aussi bien les activités existantes que les nouvelles activités.

[46] Commission "Le large bande au service du développement durable" (2019).

4 Recommandations sur les cadres et la mise en œuvre

Les gouvernements doivent mettre fin à toutes les manifestations de violence à l'encontre d'enfants dans le cyberespace. Toutefois, les mesures prises pour protéger les enfants dans la sphère numérique ne devraient pas limiter indûment l'exercice d'autres droits, comme le droit à la liberté d'expression, le droit d'accès à l'information ou le droit à la liberté d'association. Plutôt que de réprimer la curiosité naturelle et l'esprit d'innovation des enfants, de peur qu'ils ne soient exposés à des risques en ligne, il est essentiel de mettre à profit l'ingéniosité des enfants et de renforcer leur résilience, tout en explorant les possibilités offertes par le monde numérique.

Dans de nombreux cas, les actes de violence à l'égard d'enfants sont commis par d'autres enfants. Dans de telles situations, les gouvernements devraient, dans la mesure du possible, adopter une approche réparatrice, afin de réparer le préjudice subi, tout en évitant de traiter les enfants comme des criminels. Les gouvernements devraient promouvoir l'utilisation des TIC pour prévenir et résoudre la violence, par exemple en développant des technologies et des ressources à l'intention des enfants pour leur permettre d'accéder à l'information, de bloquer les contenus préjudiciables et de signaler les cas de violence lorsqu'ils se produisent[47].

Pour faire face au défi mondial de la sécurité en ligne des enfants, les gouvernements doivent faciliter la communication entre les entités concernées et coopérer ouvertement pour éradiquer les dangers auxquels les enfants sont exposés en ligne.

4.1 Recommandations sur les cadres

4.1.1 Cadre juridique

Les gouvernements devraient examiner et, si nécessaire, actualiser leur cadre juridique, afin d'appuyer la mise en œuvre pleine et entière des droits de l'enfant dans l'environnement numérique. Un cadre juridique complet devrait couvrir les mesures de prévention; l'interdiction de toute forme de violence à l'égard des enfants dans l'environnement numérique; la fourniture de moyens de recours, de réparation et de réintégration efficaces pour traiter les violations des droits des enfants; l'établissement de mécanismes de conseil, de signalement et de plainte adaptés aux enfants; et les mécanismes de responsabilisation pour lutter contre l'impunité[48].

Chaque fois que possible, la législation devrait aborder la technologie de manière neutre, de sorte que son applicabilité ne soit pas effritée par de futurs progrès technologiques[49].

Pour que la législation soit appliquée de manière efficace, les gouvernements doivent mettre en place des mesures complémentaires, notamment des initiatives de sensibilisation et de

---

47 Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants, *Rapport annuel de la Représentante spéciale du Secrétaire général chargée de la question de la violence à l'encontre des enfants au Conseil des droits de l'homme,* A/HRC/31/20 (Janvier 2016), paragraphes 103 et 104.

48 Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants, *Technologies de l'information et de la communication, Internet et violence contre les enfants: réduire autant que possible les risques et aider les enfants à tirer pleinement parti des possibilités offertes,* 2014 (New York: Nations Unies), p. 55.

49 Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants, *Technologies de l'information et de la communication, Internet et violence contre les enfants: réduire autant que possible les risques et aider les enfants à tirer pleinement parti des possibilités offertes,* 2014 (New York: Nations Unies), p. 64.

mobilisation de la société civile, des initiatives et des campagnes d'éducation et des activités de renforcement des capacités des professionnels travaillant avec ou pour les enfants.

Lors de l'élaboration de lois pertinentes, il est aussi important de garder à l'esprit que les enfants ne constituent pas un groupe homogène. Il se peut que des réponses différentes soient nécessaires pour des enfants appartenant à différents groupes d'âge, ainsi que pour des enfants qui ont des besoins particuliers ou sont davantage susceptibles de subir un préjudice, que ce soit dans la sphère numérique ou par son intermédiaire.

Les gouvernements devraient instaurer un environnement juridique et réglementaire clair et prévisible qui permette aux entreprises et à des tiers de s'acquitter de leurs responsabilités de protéger les droits des enfants dans le cadre de leurs activités, que ce soit dans leur pays ou à l'étranger[50].

Les éléments suivants pourront être utiles aux décideurs lorsqu'ils examineront le champ d'application de tout cadre juridique ou de toute disposition en la matière:

- manipulation psychologique à des fins sexuelles ou autres formes d'incitation, d'extorsion ou de coercition exercées à l'encontre d'enfants à des fins de contact sexuel ou d'activité sexuelle inappropriés;
- possession, production et distribution de matériel montrant des abus sexuels sur des enfants, indépendamment de l'intention de le diffuser ou non;
- harcèlement, intimidation, abus ou discours haineux en ligne;
- matériel terroriste en ligne;
- cybersécurité;
- idée selon laquelle ce qui est illégal dans le monde réel l'est également dans le monde virtuel.

4.1.2 Cadres politique et institutionnel

Pour garantir la réalisation des droits de l'enfant dans l'environnement numérique, les gouvernements doivent trouver un équilibre entre, d'une part, l'optimisation des avantages que les enfants tirent de l'utilisation des TIC et, d'autre part, la réduction, autant que possible, des risques associés à ces avantages. Un tel équilibre peut être obtenu en intégrant des mesures pour protéger les enfants en ligne dans les plans nationaux pour le large bande[51] et en développant une stratégie distincte et multidimensionnelle de protection en ligne des enfants. Ce travail devrait faire partie intégrante de chaque cadre politique existant présentant un intérêt du point de vue des droits ou de la protection des enfants, et compléter en outre les politiques nationales relatives à la protection des enfants, en offrant un cadre spécifique pour tous les risques et tous les dangers auxquels les enfants sont exposés, afin d'instaurer un environnement numérique sûr, inclusif et propice à l'autonomisation[52].

Les gouvernements devraient mettre en place un cadre de coordination national assorti d'un mandat clair et faisant suffisamment autorité pour coordonner toutes les activités liées aux droits des enfants, aux médias numériques et aux TIC, aux niveaux intersectoriel, national, régional et local. Les gouvernements devraient définir des objectifs assortis d'échéances et un processus transparent pour évaluer et suivre les progrès accomplis et doivent s'assurer que

50 ONU, Comité des droits de l'enfant, *Observation générale N° 16*, paragraphe 53.
51 The State of the Broadband 2019 (La situation du large bande en 2019), Recommandation 5.6, page 78. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.
52 Des dispositions types concernant la protection des enfants dans le cadre de plans nationaux pour le large bande sont données dans le Chapitre 10 du Rapport sur la sécurité en ligne des enfants.

les ressources humaines, techniques et financières nécessaires sont mises à disposition pour permettre l'application efficace du cadre[53].

Les gouvernements devraient créer une plate-forme multi-parties prenantes pour guider l'élaboration, la mise en œuvre et le suivi du programme national en matière de numérique à l'intention des enfants. Une telle plate-forme devrait rassembler les représentants des parties prenantes les plus importantes, notamment: les enfants et les jeunes; les associations de parents/de personnes s'occupant d'enfants; les administrations pertinentes d'un gouvernement; les secteurs de l'éducation, de la justice, de la santé et de la protection sociale; les institutions nationales de défense des droits de l'homme et les organismes de réglementation compétents; la société civile; les entreprises; les établissements universitaires; et les associations professionnelles pertinentes.

4.1.3 Cadre réglementaire

Un gouvernement est responsable des violations des droits de l'enfant causées par une entreprise ou auxquelles une entreprise a contribué lorsqu'il n'a pas pris les mesures nécessaires, appropriées et raisonnables pour prévenir et réparer ces violations ou lorsqu'il a de toute autre manière collaboré à leur commission ou les a tolérées[54].

Aux termes des Principes directeurs relatifs aux entreprises et aux droits de l'homme, il est indiqué que les entreprises doivent mettre à disposition des mécanismes de réparation et de réclamation qui sont légitimes, accessibles, prévisibles, équitables, compatibles avec les droits de l'homme, transparents, fondés sur la participation et le dialogue, et qui constituent une source d'apprentissage permanent. Les mécanismes de réclamation mis en place par les entreprises permettent de trouver une issue différente, rapide et adaptée à certaines situations et il est parfois dans l'intérêt des enfants qu'ils soient saisis en cas de problème relatif à la conduite de l'entreprise. Dans tous les cas, il devrait être possible de saisir la justice ou d'obtenir un contrôle judiciaire des recours administratifs et autres procédures[55]. Il convient d'envisager des mécanismes qui permettent de créer des services sûrs et adaptés à l'âge des enfants afin que les utilisateurs puissent faire part de leurs inquiétudes.

Malgré l'existence de mécanismes de réclamation internes, les gouvernements devraient mettre en place des mécanismes de contrôle des violations des droits des enfants, à des fins d'enquête et de réparation, en vue de mieux rendre compte de la responsabilité des TIC et d'autres entreprises concernées, et de renforcer la responsabilité des institutions réglementaires dans l'élaboration de normes qui sont pertinentes au regard des droits des enfants et des TIC[56]. Cela est particulièrement important étant donné que d'autres procédures de réparation mises à la disposition des personnes lésées par les activités des entreprises – poursuites civiles et autres voies judiciaires permettant de demander réparation – sont souvent lourdes et coûteuses[57].

---

53 Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants, *Rapport annuel de la Représentante spéciale du Secrétaire général chargée de la question de la violence à l'encontre des enfants* (Décembre 2014), Document A/HRC/28/55, et *Technologies de l'information et de la communication, Internet et violence contre les enfants : réduire autant que possible les risques et aider les enfants à tirer pleinement parti des possibilités offertes,* 2014 (New York: Nations Unies), paragraphe 88.

54 ONU, Comité des droits de l'enfant, *Observation générale N° 16*, paragraphe 28.

55 ONU, Comité des droits de l'enfant, *Observation générale N° 16*, paragraphe 71.

56 ONU, Comité des droits de l'enfant, *Rapport de 2014 sur la Journée de débat général*, paragraphe 96.

57 Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/32/38 (2016), paragraphe 71.

Le Comité des droits de l'enfant de l'ONU a souligné le rôle que pourraient jouer les institutions nationales de défense des droits de l'homme dans ce domaine, en indiquant comment elles pourraient être chargées de recevoir des plaintes concernant des violations commises par des entreprises, d'enquêter sur celles-ci et d'intervenir en qualité de médiateur; de mener des enquêtes publiques sur les cas de violations massives; et de procéder à la révision des textes de loi pour veiller à ce que ceux-ci soient conformes aux dispositions de la Convention relative aux droits de l'enfant. Le Comité a en outre indiqué que, si nécessaire, "les États devraient élargir le mandat de ces institutions de façon à y intégrer la question des droits de l'enfant et des entreprises". Il est particulièrement important que chaque mécanisme de plainte soit adapté aux enfants, qu'il garantisse le respect de la vie privée et la protection des victimes, et qu'il permette d'effectuer des activités de contrôle, de suivi et de vérification au service des enfants victimes.

À titre d'exemple, une institution nationale de défense des droits de l'homme ou un autre organisme de réglementation pourrait offrir aux enfants des recours utiles en cas de cyberharcèlement. Les mécanismes internes de réparation et de réclamation s'avèrent parfois inefficaces dans de tels cas car, malgré le caractère choquant et préjudiciable du contenu, celui-ci est rarement couvert par la législation nationale et aucune disposition clairement définie ne permet de demander à l'hôte du contenu de procéder à son retrait. Habiliter une autorité publique à recevoir des plaintes concernant des cas de cyberharcèlement et à intervenir auprès des hôtes des contenus pour obtenir le retrait du matériel concerné constituerait une mesure de sauvegarde importante pour les enfants[58]. Cette solution aurait l'avantage de permettre une intervention rapide – ce qui est d'une importance cruciale dans le contexte du cyberharcèlement – et de fournir une base juridique claire pour traiter la question du retrait de matériel de cyberharcèlement.

Lorsqu'ils définissent un cadre pour leur approche de la réglementation de l'environnement numérique, les gouvernements doivent aussi avoir conscience des incidences d'une telle réglementation sur l'exercice de tous les droits de l'homme, y compris la liberté d'expression[59].

Les gouvernements devraient obliger les entreprises à prendre les précautions qui s'imposent en matière de respect des droits de l'enfant. Les entreprises seraient ainsi tenues de définir, de prévenir et d'atténuer l'incidence de leurs activités sur les droits de l'enfant, notamment lorsqu'elles font affaire avec d'autres entités ou opèrent à l'échelle internationale[60].

De plus, les gouvernements devraient envisager des mesures complémentaires, par exemple veiller à ce que les entités privées dont les activités sont susceptibles d'avoir une incidence sur les droits des enfants dans l'environnement numérique respectent les normes les plus strictes en matière de prévention et d'intervention en cas de violation des droits, pour pouvoir prétendre à un financement ou à des contrats.

4.2 Recommandations sur la mise en œuvre

Les gouvernements devraient s'assurer que les enfants victimes de violations de leurs droits ont accès à des mécanismes de réparation efficaces, et notamment qu'ils bénéficient d'une assistance

58 Bertrand de Crombrugghe, "Rapport du Conseil des droits de l'homme sur sa trente et unième session" (ONU, Conseil des droits de l'homme, 2016).
59 Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/32/38 (2016), paragraphe 45.
60 ONU, Comité des droits de l'enfant, *Observation générale N° 16*, paragraphe 62.

pour demander une réparation rapide et appropriée pour le préjudice subi, moyennant une indemnisation le cas échéant. Les gouvernements devraient également fournir une assistance et un appui adéquats aux enfants victimes de violations liées aux médias numériques et aux TIC, y compris des services complets pour garantir la réadaptation et la réintégration totales de l'enfant, et empêcher que des enfants ne soient à nouveau victimes d'abus[61].

Des mécanismes de conseil, de signalement et de plainte sûrs, adaptés aux enfants et facilement accessibles, comme les lignes téléphoniques d'urgence, devraient être prévus par la loi et faire partie du système national de protection de l'enfant. Il est important de s'assurer que ces services sont connectés à tout service réglementaire afin d'aider à simplifier les interactions d'un enfant avec des organismes institutionnels à un moment où il pourrait être en détresse. Les lignes téléphoniques d'urgence sont particulièrement utiles s'agissant des sujets extrêmement sensibles, comme les abus sexuels, dont les enfants peuvent avoir des difficultés à parler avec d'autres enfants, leurs parents, les personnes qui s'occupent d'eux ou des enseignants. Les lignes téléphoniques d'urgence jouent aussi un rôle fondamental étant donné qu'elles orientent les enfants vers des services spécifiques, tels que les services juridiques, les foyers d'hébergement, les forces de police ou les centres de réhabilitation[62].

En outre, les gouvernements doivent comprendre et surveiller le comportement des agresseurs pour accroître les taux de détection des agresseurs et réduire le risque de récidive de ceux qui sont reconnus coupables. Il s'agit de mettre en place des lignes téléphoniques d'urgence qui offrent des services de conseil et de soutien gratuits et anonymes, par téléphone ou par conversation en ligne, à l'intention des personnes qui se sentent attirées sexuellement par les enfants (sentiments ou pensées) – qui sont des agresseurs potentiels. Aider les agresseurs à changer de comportement permet de réduire autant que possible le risque de récidive.

Les mécanismes statutaires de traitement des plaintes constituent également un élément essentiel du cadre pour des recours efficaces.

Les régulateurs devraient réaliser des mesures et des études indépendantes pour évaluer comment les plates-formes signalent et traitent les problèmes liés à la protection de l'enfant. Les régulateurs disposent de technologies qui leur permettent de surveiller les plates-formes de manière indépendante. Il faudrait encourager les fournisseurs de services à publier des rapports sur la transparence.

En collaboration avec la communauté internationale et le secteur privé, les gouvernements devraient élaborer un ensemble de mesures universel que les parties prenantes pourront utiliser pour mesurer tous les aspects pertinents de la sécurité en ligne des enfants.

4.2.1 Exploitation sexuelle

Les décideurs pourront accorder une attention particulière aux éléments concrets suivants lors de l'examen des menaces et des préjudices auxquels sont exposés les enfants, en particulier

61 ONU, Comité des droits de l'enfant, *Rapport de 2014 sur la Journée de débat général*, paragraphe 106.

62 Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants, *[…] réduire autant que possible les risques et aider les enfants à tirer pleinement parti des possibilités offertes,* 2014, p. 51 et p. 65.

s'agissant des contenus montrant des abus sexuels sur des enfants, des contenus autoproduits, de la manipulation psychologique à des fins sexuelles, du chantage sexuel et d'autres risques en ligne:

- Mesures en vue d'interrompre ou de réduire le trafic de matériel montrant des abus sexuels sur des enfants, par exemple en créant une ligne d'assistance téléphonique nationale ou un portail de signalement comme celui de la Fondation IWF, et en déployant des mesures qui permettront de bloquer l'accès à des contenus en ligne dont on sait qu'ils contiennent du matériel montrant des abus sexuels sur des enfants ou en font la promotion.
- Vérification de l'existence de procédures nationales permettant d'avoir l'assurance que tous les contenus montrant des abus sexuels sur des enfants découverts dans un pays sont transmis à une ressource nationale centralisée qui dispose de pouvoirs législatifs pour ordonner aux entreprises de retirer les contenus concernés.
- Stratégies pour éradiquer la demande de matériel montrant des abus sexuels sur des enfants, notamment auprès des personnes reconnues coupables de délits de ce type. Il est important de sensibiliser le public au fait qu'il n'y a pas de crime sans victime: les enfants sont exploités pour produire du matériel qui est ensuite visionné, et celui qui consulte ou télécharge ce matériel participe directement à l'exploitation de l'enfant mis en scène et encourage de surcroît l'exploitation d'autres enfants pour produire davantage d'images.
- Sensibilisation au fait qu'un enfant ne peut pas consentir à être exploité sexuellement, que ce soit pour produire des contenus montrant des abus sexuels sur des enfants ou pour n'importe quelle autre activité. Encourager les utilisateurs de ce type de matériel à rechercher de l'aide et, dans le même temps, leur faire comprendre qu'ils sont pénalement responsables des activités illicites qu'ils ont entreprises ou qu'ils entreprennent.
- Autres stratégies pour lutter contre la demande de matériel montrant des abus sexuels sur des enfants. Certains pays, par exemple, tiennent un registre des agresseurs sexuels ayant fait l'objet d'une condamnation. Les tribunaux ont prononcé des décisions judiciaires interdisant à ces agresseurs d'utiliser l'Internet en général ou de consulter certains sites fréquentés par les enfants et les jeunes. Le problème rencontré jusqu'à présent est celui de leur application. Certains pays envisagent toutefois d'inclure la liste des agresseurs sexuels dans une liste de blocage empêchant tous ceux qui y figurent de se rendre ou de s'inscrire sur certains sites web, en particulier des sites dont on sait qu'ils sont très populaires auprès des enfants et des jeunes. L'agresseur a naturellement toujours la possibilité de se connecter en utilisant un autre nom ou un faux identifiant, ce qui compromet sérieusement l'efficacité de ces mesures, mais le fait d'ériger en délit ce type de comportement peut avoir un effet dissuasif.
- Fourniture d'une assistance à long terme aux victimes. Les enfants et les jeunes ayant été victimes d'abus en ligne, par exemple lorsque des images illicites les représentant ont été diffusées sur l'Internet, sont naturellement très préoccupés de savoir qui a pu visionner ces images et les répercussions que cela aura sur leur vie. Ils peuvent de fait se sentir très vulnérables au harcèlement ou particulièrement exposés à de nouveaux actes d'exploitation et d'abus sexuels. Dans ce contexte, il sera important de pouvoir fournir des services d'assistance professionnels aux enfants et aux jeunes qui se trouvent dans cette situation. Une telle assistance devra être fournie sur le long terme.
- Vérification de la mise en place et promotion à grande échelle d'un mécanisme permettant le signalement rapide et aisé des contenus illicites ainsi que de tout cybercomportement illégal ou inquiétant, autrement dit d'un système similaire à celui mis en place par la Virtual Global Taskforce et INHOPE. L'utilisation du système i24/7 d'INTERPOL devrait être encouragée.
- Formation adéquate d'un nombre suffisant de membres des forces de l'ordre à la réalisation d'enquêtes en matière de cybercriminalité et fourniture d'un accès aux installations judiciaires adéquates en vue d'extraire et d'interpréter les données numériques dont il est question.
- Investissement dans la formation pour familiariser les services de police, les autorités judiciaires et les autorités de poursuite aux méthodes utilisées par les criminels pour commettre leurs délits en ligne. Il faudra en outre des investissements pour acquérir

et entretenir les installations nécessaires à l'obtention et à l'interprétation des preuves judiciaires issues des équipements numériques. Enfin, il sera important d'instaurer une collaboration et des échanges d'information bilatéraux et multilatéraux avec les services de police et les organismes d'enquête des autres pays.

4.2.2 Éducation

Il convient d'éduquer les enfants au numérique dans le cadre d'une stratégie pour garantir qu'ils puissent tirer parti de la technologie, en étant à l'abri de tout danger. De cette manière, les enfants pourront développer un esprit critique qui leur permettra d'identifier et de comprendre les aspects positifs et négatifs de leur comportement dans le cyberespace. Il est important de montrer aux enfants les dangers auxquels ils sont exposés en ligne, mais cette stratégie sera efficace seulement si elle s'inscrit dans un programme plus vaste de formation au numérique, qui devrait être adapté à l'âge et axé sur les aptitudes et les compétences. Il importe d'inclure des concepts d'apprentissage social et émotionnel dans les programmes d'éducation en matière de sécurité en ligne, dans la mesure où les élèves seront ainsi aidés à comprendre et à gérer leurs émotions, pour nouer des relations saines et respectueuses, tant dans le monde virtuel que dans le monde réel.

Les enfants devraient disposer des outils appropriés. La maîtrise de l'utilisation de l'Internet est l'un des moyens les plus efficaces pour préserver leur sécurité. Une solution peut être d'introduire la maîtrise des outils numériques dans les programmes scolaires, tandis qu'une autre consiste à créer des ressources pédagogiques en dehors des programmes scolaires.

Ceux et celles qui travaillent avec les enfants devraient posséder les connaissances et les compétences adéquates pour aider avec assurance les enfants à faire face aux problèmes liés à la protection en ligne et à les résoudre, et pour leur transmettre les compétences numériques dont ils ont besoin pour tirer pleinement parti de la technologie.

4.2.3 Professionnels

Les professionnels du secteur, aux niveaux national et international, devraient s'employer à mieux faire connaître les problèmes ayant trait à la protection en ligne des enfants et à aider tous les adultes responsables du bien-être d'un enfant – notamment les parents et les personnes s'occupant d'enfants, le personnel des établissements scolaires, les membres d'organismes et de communautés au service des jeunes – à acquérir les connaissances et les compétences nécessaires pour préserver la sécurité des enfants. Les entreprises devraient intégrer des principes de sécurité dès la conception dans leurs produits, leurs services et leurs plates-formes, en faisant de la sécurité un objectif fondamental.

- Les entreprises devraient fournir des outils accessibles aux familles et adaptés à l'âge, pour aider les utilisateurs à mieux gérer la protection des membres de leur famille en ligne.
- Les entreprises devraient mettre à disposition des mécanismes de signalement appropriés pour que les utilisateurs puissent signaler des problèmes ou des éléments qui soulèvent des préoccupations. Les utilisateurs devraient s'attendre à une réponse rapide après un signalement avec la communication d'informations sur les mesures prises et, le cas échéant, sur les ressources auprès desquelles ils peuvent obtenir un soutien supplémentaire.
- De plus, il faudrait pouvoir signaler immédiatement les cas de maltraitance d'enfants pour détecter et éradiquer toute forme de maltraitance (classée comme activité criminelle) envers les enfants. L'expérience a montré que si toutes les parties prenantes contribuent à détecter, à bloquer et à signaler ces abus, il est possible d'envisager un cyberespace plus sain et plus sûr pour tous. Les entreprises devraient envisager d'utiliser tous les moyens

pertinents à disposition, comme les services de la Fondation IWF, pour éviter que leurs plates-formes ne soient utilisées à mauvais escient.

Il est essentiel de collaborer avec tous les acteurs compétents au sein de l'écosystème. Ceux-ci doivent être conscients des risques et des dangers en ligne pour être en mesure d'éviter que les enfants ne soient exposés à des risques qui pourraient être évités.

Il convient d'élaborer des instruments de mesure communs afin de mesurer tous les aspects pertinents de la question. Des normes et des mesures communes sont le seul moyen de suivre les progrès accomplis à l'échelle des pays et d'apprécier la réussite des projets et des activités mis en œuvre pour éradiquer toute forme de violence envers les enfants et évaluer la solidité de l'écosystème en matière de sécurité en ligne des enfants.

5 Élaboration d'une stratégie nationale de protection en ligne des enfants

5.1 Liste de vérification nationale

Les décideurs doivent examiner plusieurs stratégies en vue de développer une stratégie nationale pour assurer la sécurité des enfants dans le cyberespace. Le Tableau 1 présente les principaux paramètres à prendre en considération.

Tableau 1: Principaux paramètres à prendre en considération

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Cadre juridique	1	Analyser le cadre juridique existant pour déterminer s'il prévoit tous les mécanismes juridiques nécessaires pour permettre aux organismes d'application de la loi et aux autres organismes compétents de protéger les personnes de moins de 18 ans sur toutes les plates-formes connectées à l'Internet.	Il sera généralement nécessaire de mettre en place un ensemble de lois qui établissent clairement que tout crime commis contre un enfant dans le monde réel peut également, *mutatis mutandis*, être commis sur l'Internet ou par le truchement de tout autre réseau électronique. Il sera peut-être également nécessaire de promulguer de nouvelles lois ou d'adapter les lois existantes afin d'interdire certains types de comportement qui ne peuvent exister que sur l'Internet, par exemple le fait d'inciter les enfants à distance à participer ou à assister à des jeux sexuels ou encore de les manipuler psychologiquement (*grooming*) afin d'organiser une rencontre dans le monde réel à des fins sexuelles. Parallèlement, il sera en général nécessaire de disposer d'un cadre juridique qui proscrive l'utilisation abusive des ordinateurs à des fins criminelles, qui interdise le piratage informatique et toute autre utilisation malveillante ou non consentie du code informatique et qui établit que l'Internet est un lieu dans lequel des crimes peuvent être perpétrés.
	2	Établir, *mutatis mutandis*, que tout acte commis sur un enfant qui est illégal dans le monde réel est illégal dans le monde virtuel et que les règles sur la protection des données et de la vie privée dans le cyberespace s'appliquent également aux enfants.	

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Cadre réglementaire	3	Envisager d'élaborer des politiques de réglementation, par exemple des politiques d'autoréglementation ou de réglementation collective ou un cadre réglementaire complet. Le modèle d'autoréglementation ou de réglementation collective pourrait inclure l'élaboration et la publication de codes de bonnes pratiques ou d'exigences de base en matière de sécurité en ligne, tant pour contribuer à stimuler, à coordonner ou à organiser et à soutenir la participation de toutes les parties prenantes pertinentes, que pour formuler et appliquer plus rapidement les mesures idoines en réponse aux évolutions technologiques. Un modèle réglementaire pourrait définir les attentes et les obligations à l'échelle des parties prenantes et les consacrer dans un cadre juridique. Des sanctions en cas de violation des lois peuvent aussi être envisagées.	Certains pays ont mis en place un modèle autoréglementé ou coréglementé régissant l'élaboration des politiques dans ce domaine et ont à ce titre publié des codes de bonnes pratiques pour fournir des orientations au secteur de l'Internet sur les meilleures mesures à appliquer pour assurer la sécurité des enfants et des jeunes en ligne. À titre d'exemple, des codes européens ont été publiés au sein de l'Union européenne pour les sites des réseaux sociaux et les réseaux de téléphonie mobile en relation avec la fourniture de contenus et de services à destination des enfants et des jeunes via ces réseaux. Du fait de leur agilité accrue, l'autoréglementation et la réglementation collective peuvent permettre de formuler et d'appliquer plus rapidement les mesures idoines en réponse aux évolutions techniques. Plus récemment, plusieurs pays ont élaboré et/ou mis en œuvre un cadre réglementaire. Dans ces cas, le cadre réglementaire est issu de modèles de réglementation ou de réglementation commune et définit les exigences et les attentes vis-à-vis des parties prenantes, en particulier les fournisseurs de services, pour qu'ils protègent davantage leurs utilisateurs.

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Signalement – Contenus illicites	4	Veiller à l'établissement et à la promotion à grande échelle d'un mécanisme permettant de fournir des moyens simples et compréhensibles de signalement des contenus illicites trouvés sur l'Internet (par exemple, une ligne d'assistance téléphonique nationale capable de fournir une réponse rapide, d'obtenir le retrait des contenus illicites ou de les rendre inaccessibles). Les entreprises devraient disposer de mécanismes pour identifier, bloquer et retirer les contenus relatifs aux abus sexuels commis à l'encontre d'enfants en ligne, en mobilisant tous les services pertinents pour leurs organisations.	Il est nécessaire de faire connaître et de promouvoir, sur l'Internet ou via un autre média, les mécanismes permettant de signaler des abus liés à un service en ligne ou des comportements en ligne jugés répréhensibles ou illicites. Si une ligne d'assistance téléphonique nationale n'est pas disponible, la Fondation IWF propose de recourir aux Portails de signalement. Les liens vers les mécanismes de signalement des abus doivent être placés en évidence sur tout site web permettant l'affichage de contenu généré par l'utilisateur. Les personnes qui se sentent menacées de quelque manière que ce soit ou les personnes qui ont été témoins d'une activité inquiétante sur l'Internet doivent également pouvoir faire un signalement dans les plus brefs délais auprès des autorités policières, lesquelles doivent être formées et préparées pour apporter une réponse pertinente. Le Virtual Global Taskforce est un organisme d'application de la loi qui fournit une assistance, 24 heures sur 24 et 7 jours sur 7, permettant de recueillir les signalements de comportements ou de contenus illicites en provenance des États-Unis, du Canada, de l'Australie et de l'Italie. D'autres pays devraient prochainement adhérer à l'initiative. Pour de plus amples informations, veuillez consulter les sites web suivants: www.virtualglobaltaskforce.com et INHOPE.

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Signalement – Préoccupations des utilisateurs	5	Les entreprises devraient donner aux utilisateurs la possibilité de signaler des éléments préoccupants et des problèmes et y répondre en conséquence.	Les fournisseurs devraient avoir l'obligation de permettre à leurs utilisateurs de signaler des problèmes et des éléments préoccupants au sein de leurs services, et d'indiquer clairement cette possibilité. Ces moyens de signalement doivent être adaptés aux enfants et facilement accessibles.
Acteurs et parties prenantes	6	Mobiliser toutes les parties prenantes concernées par la protection en ligne des enfants, en particulier: • les organismes gouvernementaux; • les organismes d'application de la loi; • les organismes de services sociaux; • les fournisseurs de services Internet et d'autres fournisseurs de services électroniques; • les fournisseurs de réseau de téléphonie mobile; • les fournisseurs de réseaux WiFi publics; • d'autres sociétés de haute technologie pertinentes; • les organisations d'enseignement; • les organisations de parents; • les enfants et les jeunes; • les agences de protection de l'enfance et d'autres ONG compétentes; • le monde de l'enseignement et de la recherche; • les propriétaires de cybercafés et les autres fournisseurs d'accès public (bibliothèques, télécentres, PC Bangs[63], salles de jeux en réseau, etc.).	Plusieurs gouvernements nationaux ont jugé utile de rassembler tous les principaux acteurs et l'ensemble des parties prenantes afin d'élaborer et de mettre en œuvre une initiative nationale visant à faire de l'Internet un lieu plus sûr pour les enfants et les jeunes et afin d'accroître la sensibilisation du public aux problèmes rencontrés et à la manière de les aborder sous un angle pratique. Il sera important, dans le cadre de cette stratégie, de tenir compte du fait que beaucoup d'utilisateurs sont connectés en permanence à l'Internet, aux quatre coins du monde, via tout un éventail de dispositifs. Les opérateurs de réseaux large bande, mobiles et WiFi doivent être mobilisés. De plus, dans de nombreux pays, le réseau des bibliothèques publiques, les télécentres et les cafés Internet peuvent être d'importants lieux d'accès à l'Internet, en particulier pour les enfants et les jeunes.

[63] Un "PC Bang" est un terme couramment utilisé en Corée du Sud et dans d'autres pays pour désigner une grande salle équipée d'installations LAN permettant de jouer en réseau, avec d'autres internautes ou avec les joueurs présents dans la salle.

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Recherche	7	Entreprendre des travaux de recherche concernant les divers acteurs et les diverses parties prenantes au niveau national afin de connaître leurs points de vue, leurs données d'expérience, leurs préoccupations et leurs initiatives en matière de protection en ligne des enfants. Ces travaux devraient aussi permettre de connaître la portée des responsabilités et les activités existantes et celles qu'il est prévu de mener pour assurer la protection en ligne des enfants.	

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Éducation, maîtrise des outils numériques et compétences numériques	8	Développer des volets consacrés à la maîtrise des outils numériques dans le cadre des programmes scolaires nationaux adaptés à l'âge des enfants et destinés à tous les enfants.	Les établissements scolaires et le système éducatif serviront généralement de fondement au volet "éducation" et "maîtrise des outils numériques" d'une stratégie nationale en matière de protection en ligne des enfants. Tout programme scolaire national devrait inclure des aspects relatifs à la protection en ligne des enfants et viser à doter les enfants de tous âges de compétences adaptées à l'âge, afin qu'ils puissent, d'une part, tirer parti de la technologie et l'utiliser avec succès et, d'autre part, être attentifs aux risques et aux dangers à éviter. Un tel programme devrait permettre de reconnaître et de récompenser les comportements en ligne positifs et constructifs. Comme dans toute campagne d'éducation et de sensibilisation, il sera important de trouver le bon ton, d'éviter les messages suscitant la peur et de mettre en avant les nombreuses solutions positives et ludiques offertes par la nouvelle technologie. L'Internet offre aux enfants et aux jeunes des possibilités inouïes de découvrir de nouveaux univers, mais les programmes d'éducation et de sensibilisation doivent impérativement donner la priorité à l'apprentissage d'un comportement en ligne à la fois positif et responsable. Ceux et celles qui travaillent avec les enfants, en particulier les enseignants, devraient être suffisamment formés et équipés pour éduquer avec succès les enfants et leur transmettre ces compétences. Ils devraient comprendre les menaces et les dangers en ligne et être en mesure de reconnaître avec certitude les signes de maltraitance et de préjudice, de réagir comme il se doit et de les signaler, pour protéger les enfants dont ils ont la

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Ressources pédagogiques	9	Renforcer le savoir et l'expérience de toutes les parties prenantes et élaborer des messages et des contenus sur la sécurité sur Internet qui soient conformes aux lois et aux normes culturelles locales et qui présentent la garantie d'une distribution efficace et d'une diffusion appropriée auprès du public cible visé. Envisager de faire appel aux médias de masse pour promouvoir les messages de sensibilisation. Mettre au point une documentation qui met en avant les aspects positifs et stimulants de l'Internet pour les enfants et les jeunes et proscrit tout message alarmant. Encourager un comportement en ligne positif et responsable. Envisager d'élaborer des ressources pour aider les parents à évaluer la sécurité en ligne de leurs propres enfants et à apprendre comment réduire autant que possible les risques et optimiser les possibilités qui s'offrent à leur propre famille, grâce à une formation ciblée.	Lors de l'élaboration du matériel pédagogique, il faut garder à l'esprit que les nombreuses personnes pour lesquelles la technologie est une nouveauté auront des difficultés à l'utiliser. Aussi, les éléments relatifs à la sécurité devront-ils être communiqués par écrit ou par l'intermédiaire d'un autre média avec lequel les nouveaux venus seront plus familiers (par exemple, une vidéo). Les grandes sociétés Internet, pour la plupart, diffusent sur leurs sites web un grand nombre d'informations relatives à l'utilisation en ligne par les enfants et les jeunes. Toutefois, ce matériel n'est trop souvent disponible qu'en langue anglaise ou dans un nombre très restreint de langues. Ce matériel doit donc impérativement être produit localement, en conformité avec les lois nationales et avec les normes culturelles locales, pour toutes les campagnes liées à la sécurité sur Internet et pour tout le matériel de formation.
Protection de l'enfance	10	Veiller à la mise en place de mécanismes de protection des enfants universels et systématiques en vertu desquels tous ceux et toutes celles qui travaillent avec les enfants (protection sociale, santé, écoles, etc.) sont dans l'obligation d'identifier les cas d'abus et de préjudice qui se produisent en ligne, d'intervenir à cet égard, et de signaler ces cas.	Il convient de mettre en place un système universel de protection en ligne des enfants applicable à tous ceux et toutes celles qui travaillent avec les enfants, les obligeant à signaler les cas d'abus d'enfant ou de préjudice causé à un enfant, afin que ces cas fassent l'objet d'enquêtes et soit traités comme il se doit.

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Sensibilisation au niveau national	11	Organiser des campagnes de sensibilisation au niveau national afin de mettre en avant les questions liées à la protection en ligne des enfants auprès du plus grand nombre. Il peut être utile de s'inspirer de campagnes mondiales telles que la Journée pour un Internet plus sûr, en vue d'organiser une campagne.	Les parents, les tuteurs et les professionnels, comme les enseignants, ont un rôle crucial à jouer pour permettre aux enfants et aux jeunes de naviguer sur l'Internet en toute sécurité. Des programmes de soutien devraient être mis en place pour aider à mieux faire connaître ces questions et concevoir des stratégies pour les traiter. Il convient par ailleurs d'envisager de faire appel médias de masse pour promouvoir les campagnes et les messages de sensibilisation. Des initiatives telles que la Journée pour un Internet plus sûr peuvent contribuer à stimuler et à encourager un dialogue national sur le thème de la protection en ligne des enfants. De nombreux pays ont organisé avec succès des campagnes de sensibilisation nationale, dans le cadre de la Journée pour un Internet plus sûr, et mobilisent tous les acteurs et toutes les parties prenantes afin de donner un retentissement mondial aux messages, via les médias et les réseaux sociaux.

	#	Principaux paramètres à prendre en considération	Informations complémentaires
Outils, services et paramètres	12	Envisager le rôle que peuvent jouer les paramètres des dispositifs, les outils techniques (tels que les programmes de filtrage) et les applications et fonctionnalités de protection des enfants. Encourager les utilisateurs à être responsables lorsqu'ils utilisent leurs dispositifs, en les incitant à effectuer des mises à jour du système d'exploitation et à utiliser des logiciels et des applications de sécurité appropriés.	Plusieurs services mis à disposition permettent de supprimer les contenus non sollicités ou de bloquer les contacts non désirés. Certains de ces programmes de filtrage ou de contrôle parental sont gratuits, car ils font partie du système d'exploitation de l'ordinateur, ou sont inclus dans une offre d'un fournisseur de services Internet ou de services électroniques. Les fabricants de certaines consoles de jeux peuvent également proposer des outils de ce type à partir du moment où leurs consoles sont dotées d'une connexion Internet. Ces programmes de sécurité ne sont pas infaillibles, mais représentent une aide appréciée, en particulier dans les familles comptant de jeunes enfants. La plupart des dispositifs sont dotés de paramètres qui permettent de protéger les enfants et de promouvoir une utilisation saine et équilibrée. Il existe aussi des mécanismes qui permettent aux parents de gérer les dispositifs de leurs enfants (temps d'utilisation à disposition, applications et services qu'ils peuvent utiliser et gestion des achats). Plus récemment, des rapports et des paramètres ont été élaborés pour permettre aux utilisateurs et aux parents de mieux comprendre et de mieux gérer le temps d'écran et l'accès de leurs enfants. Ces outils techniques devraient être utilisés dans le cadre d'un dispositif plus large. La mobilisation des parents et/ou des tuteurs est essentielle. Au fur et à mesure qu'ils grandissent, les enfants réclament plus d'intimité et souhaitent de plus en plus ardemment explorer le monde par eux-mêmes. Par ailleurs, dans les cas où il existe une relation de facturation entre le fournisseur et le client, les procédures de vérification de l'âge peuvent jouer

5.2 Exemples de questions

Une fois que les parties prenantes et les acteurs nationaux ont été identifiés, il sera possible de leur transmettre les questions suivantes et de les inviter à y répondre et à y donner suite. Leurs réponses contribueront à déterminer la portée de la couverture de la stratégie, les points forts, ainsi que les domaines appelant une attention particulière dans une liste de vérification nationale.

- Dans quelle mesure la sécurité en ligne et les droits de l'enfant relèvent-ils de votre responsabilité?
- Comment la sécurité en ligne et les droits de l'enfant sont-ils intégrés dans vos politiques et vos processus existants?
- Dans quelle mesure la sécurité en ligne est-elle couverte dans la législation existante?
- Quelles sont vos priorités en matière de sécurité en ligne?
- Quelles sont les activités que vous organisez pour appuyer la sécurité en ligne?
- Comment collaborez-vous avec d'autres institutions ou organisations pour améliorer/faire progresser la sécurité en ligne?
- Les enfants/parents peuvent-ils vous signaler des préoccupations ou des problèmes concernant la sécurité en ligne?
- Quelles sont pour vous les trois principaux défis dans le monde virtuel?
- Quelles sont pour vous les trois principales opportunités dans le monde virtuel?

Par ailleurs, il pourrait être utile d'entreprendre des travaux de recherche et de comprendre ce que les enfants et les parents pensent de la protection en ligne des enfants, et leur expérience dans ce domaine.

6 Documents de référence

Protection en ligne des enfants: publications et documents essentiels

2020

- ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, 2020
- DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020

2019

- Internet Watch Foundation (IWF), Annual Report, 2019
- WePROTECT Global Alliance, Global Threat Assessment, 2019
- Commission sur le large bande UIT/UNESCO, Protection en ligne des enfants: Déclaration universelle, 2019
- Commission sur le large bande UIT/UNESCO, Protection en ligne des enfants: Online Security: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019
- Global Kids Online, Growing up in a connected world, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, dans Comptes rendus de la Conférence World Wide Web, 13-17 mai 2019, San Francisco, États-Unis d'Amérique, 2019
- UK Home Office, Online Harms White Paper (Royaume-Uni seulement), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (Royaume-Uni seulement), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019
- UNESCO, Au-delà des chiffres: en finir avec la violence et la harcèlement à l'école, 2019 (contient des données sur les comportements préjudiciables en ligne et le cyberharcèlement)
- Haut-Commissariat des Nations Unies aux droits de l'homme, Observation générale sur les droits de l'enfant en relation avec l'environnement numérique, 2019
- Australian eSafety Commissioner, Safety by Design Overview, 2019
- UNICEF, Why businesses should invest in digital child safety, 2019
- Département d'État des États-Unis, Trafficking in Persons report, 2019

2018

- WePROTECT Global Alliance, Global Threat Assessment, 2018
- La dignité de l'enfant dans le monde numérique, Rapport du groupe de travail technique, Conseil de l'Europe, Recommandation CM/Rec(2018)7 du Comité des Ministres aux États membres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WePROTECT Global Alliance, Working examples of Model of National Response capabilities and implementation, 2018
- INTERPOL et ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018

- EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018
- International Centre for Missing & Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation & Global Review, 9ème édition, 2018
- International Centre for Missing & Exploited Children (ICMEC), Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Internet Watch Foundation (IWF), Annual Report, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims, 2018
- UIT, Global Cybersecurity Index, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation – a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA – a rapid evidence assessment, 2018
- UNICEF, Policy guide on children and digital connectivity, 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- 5Rights Foundation, Digital Childhood, Addressing Childhood Development Milestones in the Digital Environment, 2017
- Childnet, DeShame Report, 2017
- Centre canadien de protection de l'enfance, Enquête internationale auprès des survivantes et des survivants, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017
- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Les enfants dans un monde numérique, 2017
- Western Sydney University, Young and Online: Children's Perspectives on Life in Digital Age, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017

2016

- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre de justice et de prévention du crime, Child Online Protection in the MENA Region, 2016
- ECPAT International, Groupe de travail interstitutionnel sur l'exploitation sexuelle des enfants, Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels (Lignes directrices d'ECPAT Luxembourg), 2016

2015

- WePROTECT Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015

- UIT et UNICEF, Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne, 2015

Défense des droits de l'homme dans un monde numérique

- Conseil de l'Europe, Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 2018
- UNESCO, Indicateurs sur l'universalité de l'Internet, 2019
- Ranking Digital Rights (RDR), 2019 RDR Corporate Accountability Index, 2019
- Commission "Le large bande au service du développement durable", La situation du large bande, 2019
- UIT, Mesurer le développement numérique, 2019
- UIT, Rapport Mesurer la société de l'information, 2018
- UNICEF, Children and Digital Marketing Industry Toolkit, 2018
- Commission "Le large bande au service du développement durable", Santé numérique, 2017
- Commission "Le large bande au service du développement durable", Des compétences numériques pour vivre et travailler, 2017
- Commission "Le large bande au service du développement durable", Fracture numérique entre les hommes et les femmes, 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- Convention des Nations Unies relative aux droits de l'enfant, Lignes directrices concernant l'application du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, 2019

Pour accéder à d'autres ressources, veuillez consulter la liste des ressources supplémentaires, à l'adresse www.itu-cop-guidelines.com.

Appendice 1: Terminologie

Les définitions ci-dessous sont principalement tirées de la terminologie existante, telle qu'élaborée dans la Convention relative aux droits de l'enfant de 1989, ainsi que par le Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants dans les Principes directeurs concernant la protection des enfants contre l'exploitation et l'abus sexuels, 2016[64] (Guide de terminologie du Luxembourg), par la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, 2012[65], ainsi que par le rapport Global Kids Online, 2019[66].

Adolescent

Les adolescents sont des personnes âgées de 10 à 19 ans. Il est important de noter que le terme *adolescent* n'est pas un terme contraignant en droit international, et que les personnes de moins de 18 ans sont considérées comme des enfants, tandis que les personnes de 19 ans sont considérées comme des adultes, sauf si la majorité est atteinte plus tôt en vertu du droit national[67].

Intelligence artificielle (IA)

Au sens large, le terme désigne indistinctement des systèmes qui sont du domaine de la pure science-fiction (les IA dites "fortes", dotées d'une forme de conscience d'elles-mêmes) et des systèmes qui sont déjà opérationnels et capables d'exécuter des tâches très complexes (reconnaissance faciale ou vocale, conduite d'un véhicule – ces systèmes sont qualifiés d'IA "faibles" ou "modérées")[68].

Systèmes d'IA

Un système d'IA est un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations ou de prendre des décisions influant sur des environnements réels ou virtuels, et qui est conçu pour fonctionner à des degrés d'autonomie divers[69].

---

64 *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels*, 2016, 114, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-FR.pdf.

65 Conseil de l'Europe, *Convention sur la protection des enfants contre l'exploitation et les abus sexuels*, (Strasbourg: Publications du Conseil de l'Europe, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_FR.pdf.

66 Globalkidsonline.net, *Done Right, Internet Use Can Increase Learning and Skills* (Une bonne utilisation de l'Internet peut améliorer l'apprentissage et les compétences), novembre 2019, http://globalkidsonline.net/synthesis-report-2019/.

67 UNICEF et UIT, *Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants* (itu.int/cop, 2015), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

68 Conseil de l'Europe, *L'IA, "c'est quoi?"*, coe.int, Intelligence artificielle, consulté le 16 janvier 2020, https://www.coe.int/fr/web/artificial-intelligence/what-is-ai.

69 OCDE, *Recommandation du Conseil sur l'intelligence artificielle*, (OCDE, 2019) https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

Intérêt supérieur de l'enfant

Décrit tous les éléments nécessaires pour prendre une décision dans une situation spécifique, pour un enfant ou un groupe d'enfants spécifique[70].

Enfant

Conformément à l'Article 1 de la Convention relative aux droits de l'enfant, on entend par enfant toute personne âgée de moins de 18 ans, sauf si la majorité est atteinte plus tôt en vertu du droit national[71].

Exploitation et abus sexuels à l'encontre des enfants

Décrit toutes les formes d'exploitation et d'abus sexuels (Convention des Nations Unies relative aux droits de l'enfant, 1989, art. 34), par exemple "a) que des enfants [soient] incités ou contraints à se livrer à une activité sexuelle illégale; b) que des enfants [soient] exploités à des fins de prostitution ou autres pratiques sexuelles illégales; c) que des enfants [soient] exploités aux fins de la production de spectacles ou de matériel de caractère pornographique", ainsi que tout "contact sexuel qui implique généralement l'usage de la force sur une personne sans son consentement". L'exploitation et les abus sexuels à l'encontre des enfants se produisent de plus en plus souvent sur l'Internet, ou en lien avec l'environnement en ligne[72].

Matériel montrant des abus sexuels sur des enfants

L'évolution rapide des TIC a créé de nouvelles formes d'exploitation et d'abus sexuels en ligne à l'encontre des enfants, qui peuvent avoir lieu virtuellement et n'impliquent pas nécessairement de rencontre physique en face à face avec l'enfant[73]. Bien que de nombreuses juridictions continuent de qualifier les images et les vidéos d'abus sexuels sur des enfants de "pédopornographie" ou d'"images indécentes d'enfants", les présentes lignes directrices désignent collectivement ces sujets sous le terme "matériel montrant des abus sexuels sur des enfants". Cette dénomination est conforme aux lignes directrices de la Commission sur le large bande et au modèle de réponse nationale de l'Alliance mondiale WePROTECT[74]. Ce terme décrit plus précisément le contenu.

La pornographie se réfère à une industrie légitime et commercialisée et, comme le précise le Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels, l'utilisation de ce terme:

"peut contribuer (volontairement ou non) à diminuer la gravité, à rendre trivial, voire à légitimer ce qui constitue en réalité un abus sexuel ou une exploitation sexuelle d'enfants […]; le terme

---

70 HCDH (Haut-Commissariat des Nations Unies aux droits de l'homme), *Convention relative aux droits de l'enfant,* consulté le 16 janvier 2020, https://www.ohchr.org/fr/professionalinterest/pages/crc.aspx.

71 HCDH; UNICEF et UIT, *Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants.*

72 *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels.*

73 *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels*; UNICEF, *Global Kids Online Comparative Report* (Rapport comparatif de Global Kids Online) (2019).

74 Alliance mondiale WePROTECT, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, 2016, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf; Commission sur le large bande (2019), *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online* (2019).

de "pédopornographie" risque d'insinuer qu'il s'agit d'une forme de pornographie comme une autre, et que les actes sont réalisés avec le consentement de l'enfant"[75].

Le terme "matériel montrant des abus sexuels sur des enfants" fait référence aux contenus qui représentent des actes d'abus et/ou d'exploitation sexuels d'un enfant. Cela comprend, sans s'y limiter, les enregistrements d'abus sexuels commis à l'encontre d'enfants par des adultes; les images d'enfants participant à un comportement sexuellement explicite; les images d'organes sexuels d'enfants lorsque les images sont produites ou utilisées à des fins principalement sexuelles.

Enfants et jeunes

Décrit toute personne âgée de moins de 18 ans: le terme *enfants*, ou *jeunes enfants* dans les lignes directrices, désigne toute personne âgée de moins de 15 ans, et le terme *jeunes* comprend les personnes âgées de 15 à 18 ans.

Jouets connectés

Les jouets connectés se connectent à l'Internet grâce à des technologies telles que la WiFi et le Bluetooth, et fonctionnent généralement en association avec des applications pour permettre aux enfants de jouer de manière interactive. Selon Juniper Research, le marché des jouets connectés a atteint 2,8 milliards USD en 2015 et devrait passer à 11 milliards USD d'ici 2020. Ces jouets collectent et stockent des informations personnelles sur les enfants, notamment leur nom, leur géolocalisation, leur adresse, des photographies, ainsi que des enregistrements audio et vidéo[76].

Cyberharcèlement, également appelé harcèlement en ligne

Le droit international ne définit pas le cyberharcèlement. Aux fins du présent document, le "cyberharcèlement" décrit un acte agressif intentionnel perpétré de manière répétée par un groupe ou une personne utilisant les technologies numériques et visant une victime qui ne peut pas se défendre facilement[77]. Il consiste généralement à "utiliser les technologies numériques et l'Internet pour publier des informations blessantes sur quelqu'un, à partager délibérément des informations privées, des photos ou des vidéos de manière blessante, à envoyer des messages menaçants ou insultants (par e-mail, messagerie instantanée, chat, SMS), à répandre des rumeurs et de fausses informations sur la victime ou à l'exclure délibérément des communications en ligne"[78]. Il peut s'agir de communications directes (par chat ou SMS), semi-publiques (comme l'envoi d'un message intimidant à une liste d'adresses e-mail) ou publiques (comme la création d'un site Web visant à se moquer de la victime).

Cyberhaine, discrimination et extrémisme violent

"La cyberhaine, la discrimination et l'extrémisme violent sont une forme distincte de cyberviolence car ils visent une identité collective, plutôt que des individus [...] et sont souvent

---

75 *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels.*

76 Jeremy Greenberg (2017), *Dangerous Games: Connected Toys, COPPA, and Bad Security*, Georgetown Law Technology Review, 4 décembre 2017, https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

77 Anna Costanza Baldry, Anna Sorrentino et David P. Farrington, *Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities*, Children and Youth Services Review 96 (janvier 2019): 302-7, https://doi.org/10.1016/j.childyouth.2018.11.058.

78 UNICEF, *Global Kids Online Comparative Report* (Rapport comparatif de Global Kids Online) (2019); *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels.*

liés à la race, l'orientation sexuelle, la religion, la nationalité ou le statut migratoire, le sexe/genre et la politique"[79].

Citoyenneté numérique

La citoyenneté numérique désigne la capacité à participer de manière positive, critique et compétente à l'environnement numérique, en s'appuyant sur des compétences efficaces en matière de communication et de création, à pratiquer des formes de participation sociale respectueuses des droits de l'Homme et de la dignité humaine grâce à une utilisation responsable des technologies[80].

Maîtrise du numérique

La maîtrise du numérique consiste à posséder les compétences nécessaires pour vivre, apprendre et travailler dans une société où la communication et l'accès à l'information se font de plus en plus par le biais de technologies numériques comme les plates-formes Internet, les réseaux sociaux et les appareils mobiles[81]. Elle comprend la capacité à communiquer clairement et le fait de posséder des compétences techniques et un esprit critique.

Résilience numérique

Ce terme décrit la capacité d'un enfant à faire face émotionnellement aux préjudices causés en ligne. La résilience numérique implique, pour l'enfant, de disposer des ressources émotionnelles nécessaires pour comprendre quand il est en danger en ligne, savoir comment demander de l'aide, mettre à profit son expérience et se remettre d'une mauvaise expérience[82].

Éducateurs

Un éducateur est une personne qui travaille systématiquement à améliorer la compréhension d'un sujet donné par une autre personne. Le rôle d'éducateur englobe à la fois les personnes chargées d'enseigner en classe et celles qui, de manière plus informelle, utilisent par exemple les plates-formes et services des réseaux sociaux pour fournir des informations concernant la sécurité en ligne, ou qui dispensent des cours à l'intention d'un groupe ou d'une école pour apprendre aux enfants et aux jeunes à se protéger en ligne.

La tâche des éducateurs varie selon le contexte dans lequel ils travaillent et la tranche d'âge des enfants et des jeunes (ou adultes) auxquels ils s'adressent.

Grooming (sollicitation d'enfants à des fins sexuelles) en ligne et hors ligne

Le terme *grooming* en ligne ou hors ligne, tel que défini par le Guide de terminologie du Luxembourg, désigne le processus consistant à établir ou à construire une relation avec un enfant, soit en personne, soit par le biais de l'Internet ou d'autres technologies numériques,

---

79 UNICEF, *Global Kids Online Comparative Report* (Rapport comparatif de Global Kids Online) (2019).

80 Conseil de l'Europe, *Citoyenneté numérique et éducation à la citoyenneté numérique,* Éducation à la citoyenneté numérique, consulté le 16 janvier 2020, https://www.coe.int/fr/web/digital-citizenship-education/home.

81 Western Sydney University-Claire Urbach, *What Is Digital Literacy? (*Qu'est-ce que la maîtrise du numérique?), consulté le 16 janvier 2020, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

82 Dr. Andrew K. Przybylski, et al., "A Shared Responsibility. Building Children's' Online Resilience Report" (ParentZone, University of Oxford and Virgin Media, 2014), https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.

afin de faciliter les contacts (sexuels) en ligne avec cette personne et de persuader l'enfant de s'engager dans une relation sexuelle[83]. Il s'agit d'un processus visant à inciter les enfants à avoir un comportement ou des conversations à caractère sexuel, à leur insu ou non, ou d'un processus qui implique une communication et une socialisation entre l'agresseur et l'enfant afin de le rendre plus vulnérable aux abus sexuels. Le terme "*grooming*" n'a pas été défini dans le droit international; certaines juridictions, dont le Canada, utilisent le terme "leurre d'enfants" (*luring*).

Technologies de l'information et de la communication (TIC)

Les technologies de l'information et de la communication décrivent toutes les technologies informatiques axées sur la communication. Elles comprennent tous les services et dispositifs de connexion à l'Internet tels que les ordinateurs, les ordinateurs portables, les tablettes, les smartphones, les consoles de jeu, les télévisions et les montres connectées[84]. Elles comprennent également des services tels que la radio et, entre autres, le haut débit, le matériel réseau et les systèmes par satellite.

Internet et technologies associées

Il est désormais possible de se connecter à l'Internet au moyen de différents dispositifs (smartphones, tablettes, consoles de jeux, télévisions et ordinateurs portables, et ordinateurs de bureau, par exemple). Par conséquent, sauf mention contraire, toute référence à l'Internet doit être entendue comme regroupant toutes ces méthodes différentes. Afin de tenir compte de la toile riche et complexe que constitue l'Internet, les termes "Internet et technologies associées", "TIC et entreprises en ligne" et "services fondés sur l'Internet" s'utiliseront de manière interchangeable.

Notification et retrait

Les opérateurs et les fournisseurs de services reçoivent parfois des notifications de clients, du public en général, de policiers ou d'organisations proposant un service d'assistance téléphonique pour signaler des contenus douteux en ligne. Par "procédures de notification et de retrait", on entend les processus qu'une entreprise applique en vue de supprimer rapidement ("retrait") un contenu illicite (le caractère illicite du contenu étant défini selon la juridiction) dès qu'elle a été mise au courant ("notification") de la présence de ce contenu dans ses services.

Jeux en ligne

Le terme "jeu en ligne" désigne tout type de jeu vidéo commercial à un ou plusieurs joueurs via un dispositif connecté à l'Internet, y compris les consoles, les ordinateurs de bureau, les ordinateurs portables, les tablettes et les téléphones portables.

La notion d'"écosystème des jeux vidéo" comprend le fait de regarder d'autres personnes jouer à des jeux vidéo sur des plates-formes de sport électronique, de streaming ou de partage de

[83] *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels.*
[84] UNICEF et UIT, *Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants.*

vidéos, qui permettent généralement aux spectateurs de commenter ou d'interagir avec les joueurs et d'autres personnes du public[85].

Outils de contrôle parental

Logiciel qui permet aux utilisateurs, le plus souvent un parent, de contrôler certaines ou toutes les fonctions d'un ordinateur ou d'un autre appareil pouvant se connecter à l'Internet. Généralement, ces programmes peuvent limiter l'accès à certains types ou catégories de sites web ou de services en ligne. Certains permettent également de gérer le temps d'écran, c'est-à-dire que l'appareil peut être réglé pour que l'accès à l'Internet ne soit possible qu'à certaines plages horaires. Des versions plus avancées peuvent enregistrer tous les SMS envoyés ou reçus par un appareil. Les programmes sont normalement protégés par un mot de passe[86].

Parents, tuteurs et personnes s'occupant d'enfants

Plusieurs sites Internet utilisent le terme "parents" de manière générique (par exemple sur une "page des parents" ou lorsqu'il est question de "contrôle parental"). Il pourrait donc être utile de définir les personnes qui, théoriquement, devraient permettre aux enfants et aux jeunes de tirer le meilleur parti des possibilités offertes en ligne, veiller à ce que ceux-ci utilisent les sites Internet en toute sécurité et de manière responsable, et donner leur accord pour leur permettre d'accéder à certains sites Internet. Dans le présent document, le terme "parents" désigne toute personne (à l'exclusion des éducateurs) ayant une responsabilité légale à l'égard d'un enfant. L'autorité parentale varie d'un pays à l'autre, tout comme les droits parentaux légaux.

Informations personnelles

Ce terme décrit les informations individuelles permettant d'identifier une personne, qui sont collectées en ligne. Il s'agit du nom complet, des coordonnées telles que l'adresse du domicile et l'adresse e-mail, les numéros de téléphone, les empreintes digitales ou les données de reconnaissance faciale, les numéros d'assurance ou tout autre facteur permettant de contacter ou de localiser une personne physiquement ou en ligne. Dans ce contexte, il s'agit également de toute information concernant un enfant et son entourage qui est collectée en ligne par des fournisseurs de services numériques, y compris les jouets connectés et l'Internet des objets ainsi que toute autre technologie connectée.

Vie privée

Le respect de la vie privée dépend souvent de facteurs tels que le partage d'informations personnelles en ligne, le fait d'avoir un profil public sur les réseaux sociaux, le partage d'informations avec des personnes qu'on a connues en ligne, le réglage des paramètres de confidentialité, le partage des mots de passe avec des amis et le souci du respect de la vie privée[87].

---

85 UNICEF, *Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry* (Droits de l'enfant et jeu en ligne: Opportunités et défis pour les enfants et l'industrie), DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

86 UNICEF et UIT, *Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants.*

87 "Children's Online Privacy Protection Act", Pub. L. No. 15 U.S.C. 6501-6505 (1998), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

Sexting

Le terme "sexting" désigne couramment le fait d'envoyer, de recevoir ou d'échanger des contenus à caractère sexuels et autoproduits, y compris des images, des messages ou des vidéos, par le biais de téléphones portables et/ou de l'Internet[88]. La création, la distribution et la possession d'images d'enfants à caractère sexuel sont illégales dans la plupart des pays. Si des images d'enfants à caractère sexuel sont divulguées, les adultes ne doivent pas les regarder. La diffusion d'images à caractère sexuel par un adulte auprès d'un enfant constitue toujours un acte criminel, et lorsque cela se produit entre des enfants, elle peut causer un préjudice aux enfants; il peut alors être nécessaire de procéder à un signalement et de prendre des mesures pour supprimer les images partagées.

Sextorsion ou chantage sexuel d'enfants

La "sextorsion" ou le "chantage sexuel" (ou encore "extorsion et coercition en ligne à des fins sexuelles")[89] est "une forme de chantage réalisée avec l'aide d'images autoproduites par une personne en vue de lui extorquer des faveurs sexuelles, de l'argent, ou tout autre avantage, en la menaçant de partager ce matériel sans son consentement (en publiant ces images sur les réseaux sociaux, par exemple)"[90].

L'Internet des objets (IoT)

L'Internet des objets représente la prochaine étape vers la numérisation de la société et de l'économie, au sein de laquelle les objets et les personnes sont interconnectés par des réseaux de communication et rendent compte de leur état et/ou de l'environnement qui les entoure[91].

URL

L'abréviation signifie "Uniform Resource Locator" (identificateur uniforme de ressources) et désigne l'adresse d'une page Internet[92].

Réalité virtuelle

La réalité virtuelle est l'utilisation de l'informatique pour créer l'effet d'un monde tridimensionnel interactif dans lequel les objets semblent présents dans l'espace[93].

WiFi

La WiFi (Wireless Fidelity) est l'ensemble des normes techniques qui permettent la transmission de données sur les réseaux sans fil[94].

---

88 *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels.*
89 Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (European Cybercrime Centre, mai 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.
90 *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels.*
91 Ntantko, *The Internet of Things,* 1er octobre 2013, *Digital Single Market*, Commission européenne, https://ec.europa.eu/digital-single-market/en/internet-of-things.
92 UNICEF et UIT, *Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants.*
93 NASA, "Virtual Reality," nas.nasa.gov, consulté le 16 janvier 2020, https://www.nas.nasa.gov/Software/VWT/vr.html.
94 *Children's Online Privacy Protection Act*

Appendice 2: Abus perpétrés contre les enfants et les jeunes

Dans le cyberespace, les enfants et les jeunes peuvent être exposés à toute une série de contacts non souhaités et inappropriés qui peuvent avoir des conséquences désastreuses sur leur existence. Certains de ces contacts peuvent être de nature sexuelle.

Des études ont montré que 22% des enfants et des jeunes déclarent avoir fait l'objet de manœuvres d'intimidation[95], de harcèlement ou de traque en ligne; 24% ont reçu des commentaires à caractère sexuel non sollicités[96]; 8% ont rencontré des individus dans la vie réelle qu'ils ne connaissaient jusque-là que dans le monde virtuel[97]. Bien qu'ils varient d'une région à l'autre, ces chiffres montrent que le risque est bel et bien réel[98]. Il ressort d'une étude sur l'Internet menée aux États-Unis d'Amérique[99] que 32% des adolescents ont été contactés en ligne par un parfait inconnu, 23% d'entre eux ont déclaré avoir pris peur et avoir ressenti un malaise durant la prise de contact, et 4% ont été sollicités à des fins sexuelles de manière agressive.

Les prédateurs sexuels recourent à l'Internet pour contacter des enfants et des jeunes à des fins sexuelles, souvent par la technique de la manipulation psychologique à des fins sexuelles, une manœuvre qui consiste à gagner la confiance des jeunes en ciblant le ou les sujets qui les touchent particulièrement. Ils parlent souvent de relations sexuelles, diffusent des photos et utilisent un langage explicite pour banaliser la chose, éveiller l'intérêt sexuel et briser la volonté de leurs victimes. Les prédateurs utilisent des cadeaux, de l'argent et même des titres de transport pour séduire et attirer leurs proies dans des lieux où ils pourront se livrer à des abus sexuels. Les rencontres sont parfois photographiées voire filmées. Bien souvent, les enfants et les jeunes n'ont pas la maturité émotionnelle et suffisamment d'estime de soi, ce qui les rend particulièrement vulnérables à toute tentative de manipulation et d'intimidation. Ils hésitent également à parler de leurs rencontres aux adultes de peur d'être dans l'embarras ou de se voir refuser l'accès à l'Internet. Dans certains cas, ils subissent les pressions des prédateurs qui les obligent à garder le silence sur leur relation. De plus, les prédateurs sexuels échangent des informations sur les forums Internet et les salons de discussion en ligne.

---

95 U-report (2019), http://www.ureport.in/v2/.

96 Project deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.

97 Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships (Les adolescents, la technologie, et les relations amoureuses), https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/.

98 Livingstone, S., Haddon, L., Görzig, A., et Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. (Risques et sécurité sur l'Internet: Les perspectives qui s'offrent aux enfants européens. Résultats complets.), LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.

99 Amanda Lenhart et al., "The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive Online Media." (L'utilisation des médias sociaux gagne en importance dans la vie des adolescents à mesure qu'ils prennent conscience de la nature conversationnelle des médias intéractifs en ligne), *Pew Internet and American Life Project*, 2007, 44, https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Appendice 3: Alliance mondiale WePROTECT

Modèle d'intervention nationale de l'Alliance mondiale WePROTECT

La stratégie de l'Alliance mondiale WePROTECT vise à aider les pays à élaborer des mesures multipartites et coordonnées pour lutter contre l'exploitation sexuelle d'enfants en ligne, conformément à son modèle d'intervention nationale. Ce modèle fait office de plan d'action au niveau national. Il fournit un cadre dont les pays peuvent s'inspirer pour lutter contre l'exploitation sexuelle d'enfants en ligne. Le modèle d'intervention nationale a pour vocation d'aider un pays:

- à évaluer les mesures déployées actuellement en réponse à l'exploitation sexuelle d'enfants en ligne et à recenser les lacunes;
- à donner la priorité aux actions visant à combler ces lacunes au niveau national;
- à améliorer la compréhension et la coopération au niveau international.

Le modèle n'a pas vocation à prescrire des activités ou à définir une approche unique. Il a pour objet de décrire les capacités nécessaires pour protéger efficacement les enfants et aider les pays à développer ou à renforcer les capacités dont ils disposent déjà. Il contient aussi une liste de catalyseurs qui, s'ils sont appliqués de manière efficace, permettront d'obtenir plus rapidement les résultats recherchés et d'en améliorer la qualité. Le modèle comprend 21 capacités, réparties en six domaines: politique et gouvernance, justice pénale, victime, éléments sociétaux, entreprises et médias et communications. L'Alliance mondiale WePROTECT est convaincue qu'en agissant dans les six domaines, il sera possible d'apporter une réponse nationale et exhaustive à cette criminalité.

Le modèle permettra à un pays – indépendamment de son niveau de départ – d'identifier les lacunes concernant les capacités et à commencer à planifier des mesures en vue de combler ces lacunes. Même si les pays élaboreront leurs propres approches de manière individuelle, en agissant dans le contexte d'un cadre convenu en commun et d'une compréhension commune des capacités, il est à espérer que la communication et la coopération entre les parties prenantes, tant au niveau national qu'au niveau international, n'en seront que renforcées.

Stratégie d'intervention mondiale de l'Alliance mondiale WePROTECT

La stratégie d'intervention mondiale de l'Alliance mondiale WePROTECT s'inscrit dans une approche coordonnée qui vise à lutter contre l'exploitation sexuelle d'enfants en ligne, en vue d'intégrer un aperçu plus vaste des connaissances mondiales, une harmonisation internationale des approches nationales, et des solutions mondiales qui vont au-delà des interventions déployées au niveau national. Cette stratégie est essentiellement le document d'accompagnement du modèle d'intervention nationale. Si le modèle est axé sur les capacités requises pour lutter contre l'exploitation sexuelle d'enfants en ligne, la stratégie porte quant à elle sur les domaines prioritaires de collaboration internationale et de renforcement des capacités.

La stratégie d'intervention mondiale s'articule autour de six domaines thématiques pour chacun desquels les capacités requises et les résultats escomptés ont été définis. Les

partenaires qui devraient œuvrer ensemble au-delà des frontières en vue d'obtenir ces résultats sont aussi mentionnés.

Politique et législation

En stimulant la volonté politique d'agir et en élaborant une législation permettant d'harmoniser de manière efficace l'approche adoptée en matière d'infractions pénales, il sera possible de donner un nouveau souffle à l'engagement des acteurs de haut rang, aux niveaux national et international, pour lutter contre l'exploitation sexuelle d'enfants en ligne.

Justice pénale

L'échange d'informations, y compris l'accès partagé aux bases de données internationales au moyen de cadres officiels de partage des données, associé au travail de juges et de procureurs dévoués et formés, dotés de compétences en matière d'exploitation sexuelle d'enfants en ligne, sont le moyen le plus efficace d'identifier les malfaiteurs, d'engager des poursuites à leur encontre et de les arrêter, notamment grâce à des enquêtes conjointes et des condamnations ayant abouti.

Conséquences pour les victimes et services fournis

En apportant un soutien efficace et opportun aux victimes, notamment en protégeant leur identité et en leur donnant la parole, on contribue à faire en sorte que celles-ci puissent accéder à l'aide dont elles ont besoin, lorsqu'elles en ont besoin.

Technologie

L'utilisation de solutions techniques, notamment l'intelligence artificielle, pour détecter, bloquer et empêcher la diffusion de matériel préjudiciable, le streaming en direct et la manipulation psychologique en ligne, permettra d'éviter que ces plates-formes ne soient utilisées comme outil pour l'exploitation sexuelle d'enfants en ligne. Pour autant, cette utilisation doit être répandue et homogène au sein du secteur des technologies.

Éléments sociétaux

Il existe un certain nombre de moyens qui, appliqués de concert dans la société au sens large, permettent de doter les enfants des capacités de se protéger contre l'exploitation sexuelle en ligne, indépendamment de l'endroit où ils vivent. En veillant à ce que le développement de la culture numérique soit par nature plus sûr (paramètres de sécurité intégrés dès la conception) et à ce qu'une approche éthique et homogène soit adoptée au regard de la couverture médiatique, il sera possible de réduire l'exposition aux contenus illicites en ligne. Dans le même temps, l'éducation et la sensibilisation des enfants et des parents, des personnes s'occupant d'enfants et des professionnels, ainsi que les interventions ciblées auprès des malfaiteurs, sont autant de facteurs qui contribuent à éviter ou à limiter les cas d'exploitation sexuelle d'enfants en ligne.

Recherche et éléments d'information

Enfin, les évaluations des menaces, telles que le rapport de 2019 sur l'évaluation des menaces dans le monde (*Global Threat Assessment 2019*), les études sur les malfaiteurs et les travaux visant à comprendre le traumatisme des victimes à long terme sont autant d'éléments qui permettront aux gouvernements, aux organismes d'application de la loi, à la société civile, aux établissements universitaires et aux entreprises de comprendre clairement les menaces les plus récentes.

Appendice 4: Exemples de mesures prises pour lutter contre les dangers en ligne

Les exemples donnés ci-dessous sont regroupés par les auteurs et les contributeurs des lignes directrices de l'UIT à l'intention des décideurs.

Éduquer les enfants à la lutte contre les dangers en ligne

Application BBC Own IT – Il s'agit d'une application de bien-être destinée aux enfants âgés de 8 à 13 ans qui reçoivent leur premier smartphone. Associant la technologie d'apprentissage automatique dernier cri pour suivre les activités des enfants sur leur smartphone et la possibilité pour les enfants de rendre compte de leur état émotionnel, cette application utilise ces informations pour proposer des contenus et des interventions adaptés aux enfants, afin de les aider à vivre une expérience saine et plaisante en ligne.

L'application, qui comprend des contenus commandés expressément auprès de la BBC, fournit des outils et des ressources utiles pour aider les jeunes à utiliser au mieux le temps passé devant leur écran et à adopter des attitudes et des habitudes saines en ligne, et permettre aux jeunes et aux parents d'avoir des conversations davantage constructives sur leur expérience en ligne. L'application ne recueille aucune donnée personnelle ou aucun contenu produit par l'utilisateur étant donné que le système d'apprentissage automatique tout entier fonctionne au sein de l'application/du dispositif de l'utilisateur.

Projet Evolve – Il s'agit d'un cadre pédagogique sur les compétences numériques entièrement équipé, qui permet d'identifier les compétences numériques pour chaque enfant, quel que soit l'âge, afin d'aider les parents et les enseignants à comprendre les compétences que leurs enfants devraient maîtriser. Il contient également les ressources et les activités qui leur permettront d'acquérir ces compétences particulières.

360 degree safe – Cet outil d'autoévaluation en ligne permet aux établissements scolaires d'évaluer et de noter la totalité des dispositions qu'ils appliquent en matière de sécurité en ligne et fournit des orientations et un appui en vue d'obtenir des normes définies.

Institut DQ – Des données ont été recueillies auprès de 145 426 enfants et adolescents dans 30 pays, de 2017 à 2019, dans le cadre de l'initiative #DQEveryChild, un mouvement mondial de citoyenneté numérique promu par l'Institut DQ, qui a vu le jour à Singapour, avec l'appui de Singtel, et a pris rapidement de l'ampleur en collaboration avec le Forum économique mondial pour inclure plus de 100 organisations partenaires. Ce mouvement visait à doter les enfants de compétences approfondies en matière de citoyenneté numérique, dès leurs premiers pas dans le monde numérique, en utilisant le programme de formation et d'évaluation en ligne DQ World. Les données recueillies dans le cadre de ce mouvement ont été utilisées pour élaborer l'Indice 2020 de sécurité en ligne des enfants (COSI). Le cadre de l'Indice COSI permet d'évaluer et d'établir un classement de la sécurité en ligne des enfants à l'échelle de 30 pays, compte tenu de 24 domaines qui s'articulent autour de six piliers ayant une incidence sur la sécurité en ligne des enfants.

Les systèmes "DQ Pro Family Readiness Package" et "DQ World" offrent la possibilité aux parents d'évaluer l'état de préparation de leur enfant au numérique et, grâce à des supports pédagogiques, d'améliorer leurs compétences numériques (citoyenneté numérique, gestion du temps d'écran, du cyberharcèlement, de la cybersécurité, de l'empreinte numérique et de la vie privée, esprit critique et empathie dans le monde numérique).

L'Australie a élaboré un kit pratique en matière de cybersécurité à l'intention des écoles, qui regroupe des ressources conçues pour aider les écoles à instaurer un environnement en ligne plus sûr. Ce kit pratique reflète une approche pluridimensionnelle à l'égard de la formation en matière de sécurité en ligne et s'articule autour de quatre catégories. Il contient des ressources qui visent à:

- préparer les écoles à évaluer leur état de préparation pour faire face aux problèmes de sécurité en ligne et formuler des suggestions pour améliorer leurs pratiques actuelles;
- mobiliser tous les membres de la communauté scolaire afin qu'ils s'engagent et contribuent à instaurer un environnement en ligne sûr;
- éduquer en mettant en avant les bonnes pratiques relatives à l'éducation en matière de sécurité en ligne et en aidant les écoles à développer les capacités des membres qui la composent en matière de sécurité en ligne;
- intervenir en cas d'incident de manière efficace, tout en agissant en faveur de la sécurité et du bien-être.

La campagne d'éducation "Je clique intelligemment" du Bureau des communications électroniques de la Pologne (UKE) vise à éduquer les enfants et les parents sur la manière de renforcer la sécurité en ligne et de reconnaître et de gérer les risques.

ChildFund Viet Nam a mis sur pied l'initiative Swipe Safe (Naviguer en toute sécurité). Ce programme vise à sensibiliser les enfants aux risques qu'ils peuvent rencontrer en ligne, tels que les cyberarnaques, le harcèlement ou les abus sexuels, et fournit des conseils sur les méthodes à appliquer pour naviguer en toute sécurité.

La Commission sur le large bande a publié en 2013 un rapport intitulé "Technologie, large bande et éducation: faire progresser l'éducation pour tous".

En 2019, l'UNICEF a publié un rapport intitulé "Children's Experience Online: Building Global Understanding and Action" (Favoriser une compréhension et une action à l'échelle mondiale: l'expérience des enfants en ligne).

Les travaux de recherche du réseau Global Kids Online sont une mine d'informations sur les bonnes pratiques appliquées pour lutter contre les dangers en ligne.

Exemples de professionnels engagés

Le Commissaire australien à la sécurité en ligne (*eSafety Commissioner*) noue des partenariats solides et collabore avec les entreprises afin de donner la possibilité à tous les Australiens d'utiliser l'Internet de façon plus sûre et plus constructive. Les travaux visant à intégrer des principes de sécurité dès la conception en sont un exemple. Dans le cadre de cette initiative, eSafety a organisé un processus de consultation détaillé avec des entreprises, des organes professionnels et des organisations ayant la responsabilité de protéger les utilisateurs, ainsi qu'avec des parents, des personnes s'occupant d'enfants et des jeunes. L'initiative visant à intégrer des principes de sécurité dès la conception a été imaginée pour encourager et aider les entreprises à s'assurer que la sécurité des utilisateurs fait partie intégrante de la

conception, de l'élaboration et du déploiement des services et des plates-formes en ligne. eSafety administre également trois dispositifs de signalement et de plainte, à savoir pour les cas de cyberharcèlement, d'abus fondés sur les images et de contenus en ligne. eSafety peut enjoindre officiellement à certains fournisseurs de services en ligne de retirer des contenus de leurs services. Si ces dispositifs sont largement utilisés dans le cadre d'une coopération entre le gouvernement et les entreprises, les pouvoirs dont dispose le Commissaire à la sécurité en ligne pour enjoindre au retrait de matériel constituent un filet de sécurité essentiel et incitent les entreprises à réagir en amont pour traiter les dangers en ligne.

La société Telia a la responsabilité de comprendre et de gérer les effets négatifs de la connectivité et d'agir en toute transparence et de manière responsable au niveau du Comité. La société s'occupe aussi des enfants et des jeunes puisqu'elle est consciente que ce sont des utilisateurs actifs de ses services.

Le Bureau des communications électroniques de la Pologne (UKE) associe actuellement les membres de la société civile et les enfants à ses campagnes de sensibilisation, afin qu'ils soient conscients des principes auxquels ils adhèrent en ligne.

La Fondation Internet Watch (IWF) est une organisation fondée sur les partenariats, qui rassemble des représentants d'entreprises, de gouvernements, d'organismes d'application de la loi et d'organisations non gouvernementales (ONG) pour mettre un terme aux abus sexuels à l'encontre d'enfants. En 2020, la Fondation IWF comptait 152 membres sur diverses plates-formes et diverses infrastructures en tant que service. Elle offre à ses membres un éventail de services pour empêcher la diffusion, sur leurs plates-formes, de photographies et d'images à caractère délictueux.

Champ d'application de la législation

Vous pouvez manifester votre volonté politique de prioriser la protection en ligne des enfants en signant la Déclaration universelle sur la sécurité en ligne des enfants (Commission sur le large bande).

Réglementation

Le rapport "Out of the Shadows: shining light on the response to child sexual abuse and exploitation" (De l'ombre à la lumière: coup de projecteur sur les mesures prises pour lutter contre les abus sexuels et l'exploitation sexuelle des enfants) présente l'indice 2019 élaboré par The Economist Intelligence Unit. C'est le seul outil de comparaison qui permet d'analyser les mesures appliquées par les pays en réponse aux abus sexuels et aux exploitations sexuelles des enfants, y compris celles des professionnels du cyberespace et du secteur des TIC.

Identification des abus commis en ligne à l'encontre d'enfants

On trouvera ci-dessous des exemples de bonnes pratiques appliquées pour identifier les abus commis en ligne à l'encontre d'enfants.

INHOPE: Le réseau INHOPE a été créé en 1999 pour lutter contre la diffusion de matériel montrant des abus sexuels sur des enfants et concrétiser la vision commune d'un cyberespace exempt de tout contenu montrant des abus sexuels sur des enfants. Au cours de ses deux décennies d'activités, le réseau INHOPE s'est renforcé en vue de lutter efficacement contre l'augmentation, la diffusion géographique et la gravité des contenus montrant des abus sexuels sur des enfants en ligne. À l'heure actuelle, les lignes d'assistance téléphonique du réseau

INHOPE sont actives sur chaque continent, reçoivent des rapports de signalement et procèdent sans délai au retrait de matériel montrant des abus sexuels sur des enfants de l'Internet, et échangent des données avec les forces de l'ordre.

La technologie **Microsoft PhotoDNA** permet de créer des hachages d'images et de les comparer à une base de données d'images qui ont déjà été identifiées et dont il a été confirmé qu'elles constituaient du matériel montrant des abus sexuels sur des enfants. Si une correspondance est trouvée, l'image est bloquée. Toutefois, cet outil n'emploie pas la technologie de reconnaissance faciale et n'est pas en mesure d'identifier une personne ou un objet dans l'image. Cependant, grâce à l'invention de la technologie PhotoDNA appliquée aux vidéos, la situation a considérablement évolué.

La technologie **PhotoDNA appliquée aux vidéos** permet de découper une vidéo en captures d'écran et de créer des hachages pour ces captures. De la même manière que la technologie PhotoDNA met en correspondance une image avec une autre image qui a été modifiée pour éviter d'être détectée, la technologie PhotoDNA appliquée aux vidéos permet de trouver des contenus montrant des abus sexuels sur des enfants qui ont été édités ou assemblés dans une vidéo qui, autrement, pourrait sembler inoffensive.

Microsoft a publié un nouvel outil pour identifier des prédateurs d'enfants qui les manipulent psychologiquement à des fins sexuelles lors de conversations en ligne. Le **Projet Artemis,** élaboré en collaboration avec le réseau The Meet Group, la plate-forme Roblox, l'application Kik et l'entreprise Thorn, s'appuie sur la technologie brevetée de Microsoft et sera accessible gratuitement, via l'entreprise Thorn, aux sociétés fournissant des services de conversation en ligne. Il s'agit d'un outil technique qui permet d'alerter les administrateurs quand une modération des contenus échangés dans les salles de conversation en ligne est nécessaire. Cette technique de détection des cas de manipulation à des fins sexuelles permettra de détecter, d'interpeller et de signaler les prédateurs qui tentent d'attirer les enfants à des fins sexuelles.

L'entreprise **Thorn** a élaboré des messages dissuasifs à l'intention des utilisateurs qui recherchent du matériel montrant des abus sexuels sur des enfants. Ces messages ont été diffusés des millions de fois sur quatre moteurs de recherche durant trois ans. De plus, ils ont enregistré un taux de clics de 3% correspondant à la part d'utilisateurs ayant demandé de l'aide après avoir recherché du matériel à des fins d'exploitation.

Thorn's Safer est un outil qui peut être utilisé directement sur la plate-forme d'une entreprise privée pour identifier, retirer et signaler un contenu montrant des abus sexuels sur des enfants.

Thorn Spotlight est un logiciel qui offre la possibilité aux forces de l'ordre dans les 50 États des États-Unis d'Amérique et au Canada d'accélérer l'identification des victimes et de réduire la durée des enquêtes de plus de 60%.

Geebo est un site de petites annonces engagé à se prémunir contre l'exploitation sexuelle sur sa plate-forme et qui n'a jamais enregistré de cas d'exploitation sexuelle d'enfant. Le site parvient à atteindre cet objectif notamment grâce à son processus de présélection.

L'outil de classification de Google fondé sur l'intelligence artificielle (Google IA) peut être utilisé pour détecter du matériel montrant des abus sexuels sur des enfants dans les réseaux et les services, et sur les plates-formes. Cet outil est mis à disposition gratuitement via **l'interface API de sécurité des contenus de Google**, qui est un kit pratique permettant d'accroître la capacité d'examen des contenus de manière qu'un nombre réduit de personnes y soient

exposées. Cet outil permettrait aux spécialistes d'examiner le matériel à plus grande échelle et de suivre à la trace les malfaiteurs, en ciblant les photographies et les images qui n'ont pas encore été classées comme illicites. Partager cette technologie permettrait d'accélérer l'identification des images.

En 2015, Google a élargi ses travaux en matière de hachage en introduisant la toute première technologie d'empreintes digitales et de mise en correspondance, toutes catégories confondues, pour les vidéos publiées sur **YouTube**. Cette technologie permet de scanner et d'identifier les vidéos téléchargées connues pour contenir du matériel montrant des abus sexuels sur des enfants.

Durant le Hackathon pour la sécurité de l'enfant organisé en 2019, **Facebook** a annoncé la mise à disposition en libre accès de deux technologies permettant de détecter des photos et des vidéos identiques et quasi identiques. Ces deux algorithmes sont disponibles sur l'interface GitHub, qui permet aux systèmes de partage des hachages de communiquer entre eux, ce qui renforce leurs capacités.

La **ligne d'assistance téléphonique de la Fondation IWF** reste constamment en alerte, non seulement pour donner suite aux milliers de cas signalés par des individus qui ont pu découvrir malencontreusement des images en ligne d'abus sexuels sur des enfants, mais aussi pour assumer un rôle unique dans la recherche proactive de ce type de contenu illicite sur le web. En donnant les moyens aux lignes d'assistance téléphonique d'utiliser les informations obtenues et de mobiliser des ressources, il sera possible d'identifier et de retirer davantage de contenus. De plus, la Fondation IWF poursuit sa collaboration avec Google, Microsoft, Facebook et d'autres sociétés en vue de repousser sans cesse les limites de la technologie. La Fondation IWF met à disposition un Portail de signalement, une solution qui permet aux internautes des pays qui ne disposent pas d'une ligne d'assistance téléphonique de signaler des images et des vidéos dont ils soupçonnent le caractère pédopornographique directement à la Fondation IWF, via un portail en ligne créé à cet effet.

La **Fondation IWF, en collaboration avec la Fondation Marie Collins, une organisation caritative d'aide aux victimes**, vise à organiser une nouvelle campagne pour inciter les jeunes hommes à signaler toute image ou toute vidéo à caractère sexuel autoproduite et mettant en scène des enfants de moins de 18 ans, sur lesquels ils pourraient tomber en naviguant en ligne.

INTERPOL a créé une base de données internationale sur l'exploitation sexuelle des enfants (ICSE) contenant des images et des vidéos, qui est un outil de renseignement et d'enquête permettant aux enquêteurs spécialisés issus de plus de 50 pays d'échanger des informations sur des cas d'abus sexuels sur des enfants. Moyennant l'analyse des contenus numériques, visuels et audio, les spécialistes chargés de l'identification des victimes peuvent récupérer des indices, recenser les affaires qui se recoupent et associer leurs efforts afin de retracer les victimes d'abus sexuel sur des enfants. À l'heure actuelle, la base de données ICSE contient plus de 1,5 million d'images et de vidéos et a contribué à identifier 19 400 victimes dans le monde.

NetClean ProActive est un logiciel basé sur la technique de concordance de signature et d'autres algorithmes de détection pour détecter automatiquement des images et des vidéos d'abus sexuels sur des enfants qui circulent dans les entreprises.

La technologie **Griffeye Brain** utilise l'intelligence artificielle pour scanner des contenus qui ne sont pas encore classés, effectue une comparaison compte tenu des caractéristiques des

contenus montrant des abus sexuels sur des enfants identifiés au préalable, et signale les articles suspects en vue d'un examen par un agent.

Aux États-Unis, le réseau RAINN a créé et gère la ligne d'assistance téléphonique nationale pour les agressions sexuelles, en partenariat avec plus d'un millier de prestataires locaux de services permettant de signaler des cas d'agressions sexuelles à l'échelle du pays, et gère la ligne d'urgence "DoD Safe" pour le Département de la défense. Le réseau RAINN organise aussi des programmes pour empêcher les violences sexuelles, aider les victimes et s'assurer que les responsables sont traduits en justice.

Safehorizon est une organisation à but non lucratif qui vise à fournir une assistance aux victimes. Elle soutient les victimes de violence et d'abus dans la ville de New York depuis 1978. Safehorizon offre des services d'assistance téléphonique aux victimes de violence.

Le projet Arachnid est un outil innovant utilisé par le Centre canadien en vue de lutter contre la prolifération croissante de matériel montrant des abus sexuels sur enfants sur l'Internet.

[i] http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf.

Avec le soutien de:

Union internationale des télécommunications
Bureau de développement des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse

ISBN: 978-92-61-30452-2
9 789261 304522

Publié en Suisse
Genève, 2020
Crédits photo: Shutterstock