ITU Publications

Union Internationale des Télécommunications
Bureau de Développement des Télécommunications

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

2020

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

Remerciements

Ces lignes directrices ont été élaborées par l'Union internationale des télécommunications (UIT) en collaboration avec un groupe de travail d'auteurs travaillant pour des institutions majeures du secteur des technologies de l'information et de la communication et de la protection des enfants, telles que l'Union européenne de radio-télévision (UER), le Partenariat mondial pour l'élimination de la violence envers les enfants, la GSM Association (GSMA), l'International Disability Alliance, l'Internet Watch Foundation (IWF), Privately SA et le Fonds des Nations Unies pour l'enfance (UNICEF). Le groupe de travail était présidé par Anjan Bose (UNICEF) et coordonné par Fanny Rotino (UIT).

La rédaction de ces lignes directrices n'aurait pas été possible sans les efforts, l'enthousiasme et le dévouement de ces auteurs. Une participation inestimable a également été apportée par e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter et The Walt Disney Company, ainsi que par d'autres acteurs du secteur. Tous partagent un objectif commun qui consiste à faire de l'Internet un endroit meilleur et plus sûr pour les enfants et les jeunes. L'UIT tient à remercier les partenaires suivants pour leur précieuse contribution et pour le temps qu'ils ont consacré à la préparation de ce document (par ordre alphabétique des organisations):

- Giacomo Mazzone (UER)
- Salma Abbasi (e-WWG)
- David Miles et Caroline Hurst (Facebook)
- Amy Crocker et Serena Tommasino (Partenariat mondial pour l'élimination de la violence envers les enfants)
- Jenny Jones (GSMA)
- Lucy Richardson (International Disability Alliance)
- Fanny Rotino (UIT)
- Tess Leyland (IWF)
- Deepak Tewari (Privately SA)
- Adam Liu (Tencent Games)
- Katy Minshall (Twitter)
- Anjan Bose, Daniel Kardefelt Winther, Emma Day, Josianne Galea Baron, Sarah Jacobstein et Steven Edwin Vosloo (UNICEF)
- Amy E. Cunningham (The Walt Disney Company)

ISBN

978-92-61-30082-1 (version papier)

978-92-61-30412-6 (version électronique)

978-92-61-30072-2 (version EPUB)

978-92-61-30422-5 (version Mobi)

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

Avant-propos

Compte tenu de l'explosion des technologies numériques, les enfants et les jeunes bénéficient de possibilités sans précédent de communiquer, d'entrer en relation, de partager, d'apprendre, d'accéder à des informations et d'exprimer leurs opinions sur des questions qui touchent leur vie et leur communauté.

Cependant, cet accès élargi et facilité aux services sur Internet pose aussi des enjeux majeurs concernant la sécurité des enfants, que ce soit en ligne ou hors ligne. Les jeunes d'aujourd'hui sont confrontés à de nombreux risques graves: confidentialité, violence entre enfants, contenus violents et/ou inappropriés pour leur âge, ou encore escroqueries sur Internet et crimes contre les enfants (manipulation psychologique sur Internet à des fins sexuelles, exploitation et abus sexuels, etc.). Tandis que les menaces se multiplient, leurs auteurs se jouent de plus en plus des frontières, rendant leur traçage difficile et leur sanction d'autant plus complexe.

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 leurs études et de conserver des interactions sociales. En raison des contraintes imposées par le virus, de nombreux jeunes enfants ont non seulement dû interagir en ligne beaucoup plus tôt que leurs parents ne l'avaient prévu, mais la nécessité pour les parents de gérer leurs engagements professionnels empêche bon nombre d'entre eux de surveiller leurs enfants. Ceux-ci risquent ainsi d'accéder à des contenus inappropriés ou d'être pris pour cibles par des criminels produisant du matériel montrant des abus sexuels sur des enfants.

Les criminels tirent parti des progrès technologiques, tels les applications et les jeux interconnectés, le partage rapide de fichiers, la diffusion en direct, les cryptomonnaies, le dark web et les logiciels de chiffrement puissant. Ils profitent également de la mauvaise coordination et de l'indécision du secteur des technologies dans la mise en place de mesures visant à lutter efficacement contre ce fléau.

Les technologies émergentes peuvent apporter un début de solution, comme la base de données d'Interpol sur l'exploitation sexuelle des enfants basée sur l'intelligence artificielle, qui emploie un logiciel de comparaison d'images et de vidéos pour faire le lien rapidement entre des victimes, des agresseurs et des lieux. Malgré tout, la technologie seule ne suffit pas pour résoudre le problème.

Pour limiter les risques induits par la révolution numérique tout en permettant à un nombre toujours croissant de jeunes d'en bénéficier, une réponse multipartite collaborative et coordonnée est plus indispensable que jamais. Gouvernements, société civile, communautés locales, organisations internationales et parties prenantes du secteur doivent tous se rassembler autour d'un but commun.

Compte tenu de cette nécessité, en 2018, les États membres de l'UIT ont demandé une mise à jour complète de nos lignes directrices sur la protection en ligne des enfants. Ces nouvelles lignes directrices de l'UIT ont été repensées, réécrites et refaçonnées afin de refléter les changements majeurs survenus dans le paysage numérique dans lequel évoluent les enfants de la génération actuelle. En plus de prendre en compte les récentes évolutions des technologies et plates-formes numériques, cette nouvelle édition vise à pallier une lacune majeure, à savoir la situation des enfants handicapés, pour lesquels l'Internet constitue une ligne de vie particulièrement importante qui leur permet de participer pleinement à la société.

L'industrie des technologies a un rôle essentiel et proactif à jouer dans l'établissement des bases aux fins d'une utilisation plus sûre et plus sécurisée des services Internet et des autres technologies, pour les enfants aujourd'hui et les générations à venir.

Les entreprises doivent de plus en plus placer les intérêts des enfants au cœur de leurs activités et veiller particulièrement à la protection de la confidentialité des données des jeunes utilisateurs, ainsi que de leur droit à la liberté d'expression. Ces entreprises sont également tenues de lutter contre le fléau grandissant du matériel montrant des abus sexuels sur des enfants et de s'assurer que des systèmes sont en place pour lutter efficacement contre les éventuelles violations des droits de l'enfant.

Dans les cas où la législation nationale ne traduit pas encore le droit international, chaque entreprise se voit offrir l'occasion et confier la responsabilité d'aligner ses propres cadres opérationnels aux normes et bonnes pratiques les plus strictes.

Nous espérons que les présentes lignes directrices serviront de base solide sur laquelle les professionnels s'appuieront pour élaborer des politiques d'entreprise et des solutions innovantes. Conformément au rôle de mobilisateur mondial de l'UIT, je suis fière que ces lignes directrices soient le fruit d'un effort de collaboration mondiale et qu'elles aient été corédigées par des experts issus d'une grande communauté internationale.

J'ai également l'immense plaisir de vous présenter notre nouvelle mascotte de la protection en ligne des enfants, Sango: un personnage amical, courageux et intrépide, entièrement créé par un groupe d'enfants dans le cadre du nouveau programme international de sensibilisation de la jeunesse de l'UIT.

À une époque où les jeunes sont de plus en plus nombreux en ligne, les lignes directrices sur la protection en ligne des enfants sont plus importantes que jamais. Professionnels, gouvernements, parents et éducateurs, ainsi que les enfants eux-mêmes… Tous ont un rôle essentiel à jouer. Comme toujours, je vous remercie de votre soutien et je me réjouis à la perspective de poursuivre notre étroite collaboration sur cette question cruciale.

Doreen Bogdan-Martin
Directrice
Bureau de développement des télécommunications de l'UIT

Table des matières

Table

1 Présentation

L'objet du présent document consiste à fournir une orientation aux parties prenantes du secteur des technologies de l'information et de la communication (TIC) afin de leur donner les moyens de créer leurs propres ressources en matière de protection en ligne des enfants. Ces lignes directrices sur la protection en ligne des enfants à l'intention des professionnels visent à apporter un cadre utile, flexible et convivial en soutien aux visions d'entreprise et à leur responsabilité de protéger les utilisateurs. Elles contribuent également à l'établissement des bases aux fins d'une utilisation plus sûre et plus sécurisée des services Internet et des technologies associées, pour les enfants aujourd'hui et les générations à venir.

Véritable boîte à outils, ces lignes directrices ont également pour but de dynamiser la réussite des entreprises en aidant les structures et parties prenantes, quelle que soit leur envergure, à créer et à conserver un modèle économique attrayant et durable, tout en saisissant les responsabilités juridiques et morales qui leur incombent en ce qui concerne les enfants et la société.

En réponse aux progrès considérables réalisés dans les technologies et la convergence, l'Union internationale des télécommunications (UIT), le Fonds des Nations Unies pour l'enfance (UNICEF) et leurs partenaires de la protection en ligne des enfants ont élaboré et mis à jour les lignes directrices pour les nombreuses entreprises qui conçoivent, fournissent ou utilisent des moyens de télécommunication ou bien qui exercent des activités connexes pour fournir leurs produits et services.

Ces nouvelles lignes directrices sur la protection en ligne des enfants à l'intention des professionnels sont le résultat de consultations avec les membres de l'initiative pour la protection des enfants en ligne, ainsi que de consultations élargies avec des membres de la société civile, des entreprises, des institutions universitaires, des gouvernements, des médias, des organisations internationales et des jeunes.

Les objectifs du présent document sont les suivants:

- Établir un point de référence commun et des orientations pour les professionnels des TIC et du numérique, ainsi que pour les parties prenantes concernées.
- Fournir des orientations aux entreprises leur permettant de repérer, de prévenir et de réduire toutes les conséquences négatives de leurs produits et services sur les droits des enfants.
- Fournir des orientations aux entreprises leur permettant de déterminer des moyens de promouvoir les droits des enfants et la citoyenneté numérique chez ces derniers.
- Proposer des principes communs afin de constituer la base des engagements nationaux ou régionaux dans l'ensemble des secteurs associés, tout en tenant compte du fait que les modèles de mise en œuvre varieront en fonction des types d'entreprises.

Champ d'application

La protection des enfants en ligne est un défi complexe impliquant différents aspects sur les plans politique, opérationnel, technique, juridique et en matière de gouvernance. Ces lignes directrices visent à prendre en compte, organiser et hiérarchiser la plupart de ces domaines à partir de références existantes et reconnues telles que des modèles et des cadres.

Les lignes directrices sont axées sur la protection des enfants dans tous les domaines et contre tous les risques que comporte le monde numérique. Elles mettent en avant en tant que telles les bonnes pratiques des acteurs du secteur qui peuvent être prises en considération dans les processus de rédaction, d'élaboration et de gestion des politiques des entreprises relatives à la protection en ligne des enfants. Non seulement elles fournissent des orientations aux

acteurs du secteur sur la façon de gérer et d'enrayer les activités illégales en ligne contre lesquelles il leur incombe de lutter (le matériel montrant des abus sexuels sur des enfants en ligne, par exemple) sur l'ensemble de leurs services, mais elles mettent aussi l'accent sur d'autres problématiques qui peuvent ne pas être définies comme des crimes dans toutes les juridictions. Il s'agit par exemple de la violence entre enfants, de la cyberintimidation ou du harcèlement en ligne, ainsi que des problèmes liés à la confidentialité des données ou au bien-être général, à la fraude ou à d'autres menaces, qui peuvent ne s'avérer préjudiciables aux enfants que dans certains contextes.

Dans cette optique, ces lignes directrices incluent des recommandations en matière de bonnes pratiques visant à atténuer les risques auxquels sont exposés les enfants dans le monde du numérique. Elles orientent aussi sur la manière d'agir en vue de créer un environnement en ligne sûr pour eux. Ces lignes directrices donnent des conseils sur les mesures que peuvent mettre en place les professionnels pour veiller à la sécurité des enfants lorsqu'ils utilisent des TIC, l'Internet ou autres appareils ou technologies associés pouvant s'y connecter. Cela inclut les téléphones mobiles, les consoles de jeux vidéo, les jouets et montres connectés, l'Internet des objets et les systèmes reposant sur l'intelligence artificielle (IA). Ainsi est fournie une vue d'ensemble des principales difficultés et problématiques relatives à la protection en ligne des enfants. Des mesures sont également proposées aux entreprises et parties prenantes pour l'élaboration de politiques locales et internes en matière de protection des enfants en ligne. Ces lignes directrices n'abordent pas les aspects tels que le processus d'élaboration concret ou le contenu éventuel des politiques des professionnels en matière de protection des enfants en ligne.

Structure

Section 1 – Présentation: cette section met en avant l'objet, le champ d'application et l'audience cible de ces lignes directrices.

Section 2 – Introduction à la protection des enfants en ligne: cette section donne un aperçu de la question de la protection des enfants en ligne. Elle présente des informations de contexte, comme la situation particulière des enfants handicapés. Sont également fournis des exemples de modèles internationaux et nationaux existants visant à garantir la sécurité des enfants en ligne en tant que domaines d'intervention possibles pour les acteurs du secteur.

Section 3 – Principaux domaines de protection et de promotion des droits des enfants: cette section présente cinq domaines clés dans lesquels les entreprises peuvent agir pour garantir une utilisation sûre et positive des TIC par les enfants.

Section 4 – Directives générales: cette section formule des recommandations destinées à l'ensemble des acteurs du secteur sur la protection des enfants utilisant des TIC et sur la promotion d'une utilisation positive de ces dernières, y compris sur la citoyenneté numérique chez les enfants.

Section 5 – Listes de contrôle spécifiques par fonctionnalité: cette section émet des recommandations spécifiques à l'intention des parties prenantes concernées sur des actions concrètes permettant de respecter et de soutenir les droits des enfants, à l'aide des fonctionnalités suivantes:

- Fonctionnalité A: fournir des services de connectivité, de stockage de données et d'hébergement
- Fonctionnalité B: proposer du contenu numérique soigneusement sélectionné

- Fonctionnalité C: héberger du contenu produit par les utilisateurs et établir un lien entre ces derniers
- Fonctionnalité D: systèmes reposant sur l'IA

Audience cible

S'appuyant sur les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme[1], les Principes régissant les entreprises dans le domaine des droits de l'enfant invitent les entreprises à honorer la responsabilité qui leur incombe de respecter les droits des enfants en veillant à ce qu'aucun effet néfaste ne découle de leurs opérations, leurs produits ou leurs services. Ces principes font également la distinction entre le respect (le minimum requis auprès des entreprises pour éviter tout préjudice aux enfants) et le soutien (par exemple, la prise de mesures volontaires visant à faire progresser la réalisation des droits des enfants). Les entreprises sont tenues de garantir le droit des enfants à la protection en ligne, mais aussi à l'accès à l'information et à la liberté d'expression, tout en favorisant une utilisation positive des TIC par les enfants.

Les distinctions faites traditionnellement entre l'industrie des télécommunications et l'industrie de la téléphonie mobile, ou entre les compagnies Internet et les diffuseurs sont de moins en moins pertinentes. La convergence médiatique rassemble ces courants jusqu'ici distincts en un flot unique, qui touche des milliards d'individus à travers le monde. Coopération et partenariat sont les clés pour établir des bases en faveur d'une utilisation plus sûre et plus sécurisée de l'Internet et des technologies qui y sont associées. Gouvernements, secteur privé, décideurs publics, éducateurs, société civile, parents et personnes s'occupant d'enfants: tous ont un rôle essentiel à jouer dans l'accomplissement de cet objectif. Les professionnels du secteur peuvent prendre des mesures dans cinq domaines clés, décrits dans la Section 3.

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

Au cours des dix dernières années, l'utilisation de l'Internet et son rôle dans la vie des individus ont considérablement évolué. Avec la prévalence des smartphones et des tablettes, l'accessibilité des technologies WiFi et 4G, mais aussi le développement des plates-formes et applications de réseaux sociaux, de plus en plus de personnes accèdent à l'Internet pour des raisons toujours plus diverses.

En 2019, plus de la moitié de la population mondiale utilisait l'Internet. La plus grande proportion des utilisateurs sont âgés de moins de 44 ans, et on observe un niveau d'utilisation similaire chez les 16 à 24 ans et les 35 à 44 ans. Au niveau mondial, un utilisateur de l'Internet sur trois est un enfant (entre 0 et 18 ans) et l'UNICEF estime à 71% le taux de jeunes déjà en ligne[2]. La prolifération des points d'accès Internet, la technologie mobile et le nombre croissant d'appareils dotés d'un accès Internet, combinés à l'infinité des ressources disponibles dans le cyberespace, les occasions d'apprendre, de partager et de communiquer sont sans précédent.

Les TIC offrent de nombreux avantages: un accès plus large à l'information relative aux services sociaux, aux ressources éducatives et aux recommandations sanitaires. Lorsque les

[1] Nations Unies, Principes directeurs relatifs aux entreprises et aux droits de l'homme.
[2] Organisation de coopération et de développement économiques (OCDE), "New Technologies and 21st Century Children: Recent Trends and Outcomes", document de travail sur l'éducation N 179.

enfants, les jeunes et les familles utilisent l'Internet et les téléphones mobiles pour rechercher des renseignements et demander de l'aide, ou pour signaler des cas de maltraitance, ces technologies peuvent contribuer à la protection des enfants et des jeunes contre la violence et l'exploitation. Les fournisseurs de services de protection des enfants s'appuient également sur les TIC pour rassembler et transmettre des données, facilitant ainsi l'enregistrement des naissances, la gestion des dossiers, la recherche des familles, la collecte de données, la cartographie des cas de violence, etc.

En outre, l'Internet a amélioré l'accès à l'information aux quatre coins du monde, permettant ainsi aux enfants et aux jeunes d'effectuer des recherches sur sensiblement tous les sujets qui les intéressent, d'accéder aux médias du monde entier, de réaliser leurs objectifs professionnels et d'exploiter des idées pour l'avenir. L'utilisation des TIC permet aux enfants et aux jeunes de faire valoir leurs droits et d'exprimer leurs opinions, et leur permet également d'entrer en contact et de communiquer avec leur famille et leurs amis. Les TIC constituent également un mode d'échange culturel primordial ainsi qu'une source de divertissement.

Néanmoins, malgré les avantages considérables de l'Internet, les enfants et les jeunes peuvent rencontrer un certain nombre de risques lorsqu'ils utilisent les TIC. Ils peuvent être exposés à des contenus inadaptés à leur âge ou à des contacts inappropriés, y compris de la part d'auteurs potentiels d'abus sexuels. Ils peuvent porter atteinte à leur propre réputation en publiant des informations personnelles sensibles soit en ligne, soit par "sexto", souvent dans l'ignorance des conséquences de leurs actes sur leur propre personne et sur les autres, ainsi que sur leur "empreinte numérique" à long terme. Ils sont également confrontés à des risques liés à la confidentialité en ligne résultant de la collecte de données, ainsi que de la collecte et de l'utilisation des informations de localisation.

La Convention relative aux droits de l'enfant, qui est le traité international relatif aux droits de l'homme le plus largement ratifié[3], énonce les droits civils, politiques, économiques, sociaux et culturels des enfants. Elle établit que tous les enfants et les jeunes ont droit à l'éducation, aux loisirs, au jeu et à la culture, à la liberté de pensée et d'expression, ainsi qu'au respect de la vie privée. La Convention entérine également le droit des enfants d'accéder à des informations appropriées et d'exprimer leur point de vue sur les questions qui les concernent en fonction de leurs capacités évolutives. La Convention protège également les enfants et les jeunes contre toutes les formes de violence, d'exploitation, de maltraitance et de discrimination d'une quelconque nature, et stipule que l'intérêt supérieur de l'enfant doit être le principal élément à prendre en compte pour toute question qui le concerne. Les parents, les personnes s'occupant d'enfants, les éducateurs et les membres de la communauté, y compris les dirigeants communautaires et les acteurs de la société civile, ont la responsabilité de prendre soin des enfants et des jeunes et de les soutenir dans leur passage à l'âge adulte. Les gouvernements ont un rôle important à jouer pour garantir que tous ces acteurs remplissent ce rôle.

En ce qui concerne la protection des droits des enfants en ligne, les industries doivent travailler ensemble pour trouver un juste équilibre entre le droit des enfants à la protection et leur droit d'accès à l'information et à la liberté d'expression. Les entreprises devraient donc accorder la priorité à l'adoption de mesures de protection des enfants et des jeunes en ligne qui sont ciblées et qui ne sont pas indûment restrictives, ni pour l'enfant ni pour les autres utilisateurs. En outre, de plus en plus d'acteurs s'accordent sur le fait que la promotion de la citoyenneté

[3] Nations Unies, Convention relative aux droits de l'enfant. Tous les pays sauf trois (la Somalie, le Soudan du Sud et les États-Unis) ont ratifié la Convention relative aux droits de l'enfant.

numérique chez les enfants et les jeunes ainsi que la création de produits et de plates-formes qui facilitent l'utilisation positive des TIC par les enfants devraient constituer des priorités pour le secteur privé.

Bien que les technologies en ligne offrent de nombreuses possibilités aux enfants et aux jeunes de communiquer, d'acquérir de nouvelles compétences, d'être créatifs et de contribuer à l'amélioration de la société pour tous, elles peuvent également poser de nouveaux risques pour leur sécurité. Elles peuvent les exposer à des risques et préjudices potentiels liés à la confidentialité, à des contenus illégaux, au harcèlement, à la cyberintimidation, à l'utilisation abusive de données personnelles ou à de la manipulation psychologique à des fins sexuelles, voire même à de l'exploitation et à des abus sexuels. Les enfants et les jeunes peuvent également être exposés à des atteintes à leur réputation, notamment à la pornodivulgation ("revenge porn") à la suite de la publication d'informations personnelles sensibles en ligne ou par le biais de "sextos", qui consistent à envoyer des messages, des photographies ou des images sexuellement explicites d'un téléphone mobile à un autre. Ils sont aussi confrontés à des risques liés à la confidentialité en ligne lorsqu'ils utilisent l'Internet. Les enfants, en raison de leur âge et du développement encore inachevé de leur maturité, sont souvent incapables de saisir pleinement les risques associés au monde en ligne et les éventuelles répercussions négatives de leur comportement inapproprié sur les autres et sur eux-mêmes.

Malgré les avantages qu'elle offre, l'utilisation de technologies émergentes et plus avancées présente également des inconvénients. Les progrès de l'IA, de l'apprentissage automatique, de la réalité virtuelle et augmentée, des mégadonnées, de la robotique et de l'Internet des objets devraient transformer encore plus les pratiques des enfants et des jeunes dans le domaine des médias. Bien que ces technologies soient principalement développées pour élargir la portée de la prestation de services et améliorer la commodité (via, par exemple, l'assistance vocale, l'accessibilité et les nouvelles formes d'immersion numérique), certaines pourraient avoir des incidences involontaires, voire être utilisées à mauvais escient par des pédophiles pour répondre à leurs besoins. La création d'un environnement en ligne sûr et sécurisé pour les enfants et les jeunes nécessite la participation effective des gouvernements, du secteur privé et de toutes les parties prenantes. Mettre l'accent sur les compétences et la culture numériques des parents et des éducateurs doit également être l'un des premiers objectifs, et l'industrie peut jouer un rôle vital et durable à cette fin.

Certains enfants peuvent avoir une bonne compréhension des risques en ligne et de la manière d'y réagir. Cependant, il est impossible de considérer que c'est le cas de tous, partout, en particulier au sein des groupes vulnérables. Au titre de la cible 16.2 des Objectifs de développement durable des Nations Unies, qui vise à mettre un terme à la maltraitance, à l'exploitation, à la traite et à toutes les formes de violence et de torture dont sont victimes les enfants, la protection en ligne de ces derniers est vitale.

Depuis 2009, l'Initiative pour la protection des enfants en ligne, un effort international multipartite mis en place par l'UIT, vise à sensibiliser aux risques auxquels sont exposés les enfants en ligne et aux actions à entreprendre face à ceux-ci. L'Initiative rassemble des partenaires internationaux issus de tous secteurs afin d'assurer une expérience en ligne sûre et sécurisée pour les enfants du monde entier. Dans le cadre de l'Initiative, l'UIT a publié en 2009 un ensemble de directives relatives à la protection des enfants en ligne pour quatre groupes: les enfants, les parents, tuteurs et éducateurs, l'industrie et les décideurs publics. Dans ces directives, la protection des enfants en ligne est considérée comme une approche globale destinée à répondre à toutes les menaces et tous les préjudices que les enfants et les

jeunes sont susceptibles de rencontrer en ligne, ou qui sont facilités par les technologies en ligne. Dans ce document, le principe de protection des enfants en ligne couvre également les préjudices causés aux enfants hors ligne, mais qui sont liés à des preuves de violence et d'abus en ligne. Outre la prise en compte du comportement et des activités des enfants en ligne, le principe de protection des enfants en ligne fait également référence à l'utilisation abusive de la technologie par des personnes autres que les enfants eux-mêmes pour exploiter ces derniers.

Toutes les parties prenantes concernées ont un rôle à jouer pour aider les enfants et les jeunes à bénéficier des possibilités que l'Internet peut offrir, tout en acquérant des connaissances et une résilience numériques en ce qui concerne leur bien-être et leur protection en ligne.

La protection des enfants et des jeunes est une responsabilité partagée par toutes les parties prenantes. Pour qu'elle soit assurée, les décideurs publics, l'industrie, les parents, les personnes s'occupant d'enfants et les éducateurs, entre autres, doivent veiller à ce que les enfants et les jeunes puissent réaliser leur potentiel, aussi bien en ligne que hors ligne.

Bien qu'il n'existe pas de définition universelle, la protection des enfants en ligne consiste en une approche holistique visant la création d'espaces numériques sûrs, adaptés à l'âge des internautes, inclusifs et participatifs pour les enfants et les jeunes, caractérisés par les éléments suivants:

- Réaction, soutien et entraide face aux menaces.
- Prévention des préjudices.
- Équilibre dynamique entre le fait d'assurer la protection des enfants et celui de leur offrir la possibilité de devenir des citoyens numériques.
- Défense des droits et des responsabilités des enfants et de la société.

De plus, en raison des progrès rapides de la technologie et de la société, ainsi que de la nature sans frontières de l'Internet, la protection des enfants en ligne doit être flexible et adaptable pour être efficace. À mesure que les innovations technologiques se développent, de nouveaux défis verront le jour et varieront d'une région à l'autre. Il sera préférable de traiter ces problèmes en travaillant main dans la main en tant que communauté mondiale, car de nouvelles solutions à ces défis doivent être trouvées.

2.1 Contexte

L'Internet étant pleinement intégré dans la vie des enfants et des jeunes, il est impossible d'appréhender les mondes numérique et physique séparément.

Cette connectivité est extrêmement stimulante. Le monde en ligne permet aux enfants et aux jeunes de surmonter leurs désavantages et handicaps. Il a également mis à leur disposition de nouveaux espaces favorables au divertissement, à l'éducation, à la participation et à l'établissement de relations. Les plates-formes numériques actuelles sont utilisées pour une multitude d'activités et proposent souvent des expériences multimédias.

Avoir accès à cette technologie, apprendre à l'utiliser et à y naviguer est considéré comme essentiel au développement des jeunes, d'autant que la première utilisation des TIC survient à un âge très précoce. C'est pourquoi il est absolument crucial que tous les acteurs soient conscients que les enfants et les jeunes commencent souvent à utiliser des plates-formes et des services avant d'atteindre l'âge minimum imposé à l'industrie des technologies. Par conséquent, l'éducation doit être intégrée dans tous les services en ligne utilisés par les enfants, parallèlement aux mesures de protection.

2.1.1 Les enfants dans le monde numérique

Accès à l'Internet

En 2019, plus de la moitié de la population mondiale utilisait l'Internet, soit environ 4,1 milliards d'utilisateurs (53,6%). Au niveau mondial, un internaute sur trois est un enfant de moins de 18 ans[1]. Selon l'UNICEF, 71% des jeunes dans le monde sont déjà en ligne[2]. Malgré l'âge minimum requis, l'Ofcom (organisme de régulation des communications du Royaume-Uni) estime que près de 50% des enfants entre 10 et 12 ans ont déjà un compte sur les réseaux sociaux[3]. Les enfants et les jeunes constituent désormais une présence importante, permanente et continue sur l'Internet. Ce dernier sert d'autres fins sociales, économiques et politiques et est devenu un produit ou un service familial ou de consommation, faisant partie intégrante de la vie des familles, des enfants et des jeunes.

En 2017, au niveau régional, l'accès des enfants et des jeunes à l'Internet était fortement lié au niveau du revenu national. Les pays à faible revenu comptent généralement moins d'enfants parmi les internautes 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 âgés de 15 à 17 ans passant les plus longues périodes en ligne, entre 2,5 et 5,3 heures, selon le pays.

---

1 Livingstone, S., Carr, J. et Byrne, J., "One in three: The task for global internet governance". Global Commission on Internet Governance: Paper Series. CIGI et Chatham House, Londres, 2015. Disponible à l'adresse suivante: https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 adband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)", *Broadband Commission for Sustainable Development,* October 2019, 84,

3 Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)", *Broadband Commission for Sustainable Development,* October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

Utilisation de l'Internet

Chez les enfants et les jeunes, l'appareil le plus populaire pour accéder à Internet est le téléphone portable, suivi des ordinateurs de bureau et des ordinateurs portables. Les enfants et les jeunes passent en moyenne deux heures par jour en ligne en semaine, et quatre heures par jour le week-end. Alors que certains se sentent connectés en permanence, de nombreux autres n'ont toujours pas accès à l'Internet à leur domicile. Dans la pratique, la plupart des enfants et des jeunes qui utilisent le web y ont accès depuis plusieurs appareils. Ceux qui se connectent au moins une fois par semaine utilisent parfois jusqu'à trois appareils différents. Les enfants plus âgés et ceux des pays riches utilisent généralement plus d'appareils, les garçons en employant légèrement plus que les filles dans tous les pays étudiés.

L'activité la plus populaire chez les filles et les garçons consiste à regarder des clips vidéo. Plus des trois quarts des enfants et des jeunes qui utilisent Internet déclarent regarder des vidéos en ligne au moins une fois par semaine, seuls ou avec d'autres membres de leur famille. De nombreux enfants et jeunes peuvent être considérés comme des "socialiseurs actifs", utilisant plusieurs plates-formes de réseaux sociaux telles que Facebook, Twitter, TikTok ou Instagram. Les enfants et les jeunes s'engagent également dans la politique en ligne et font entendre leur voix via leurs blogs.

Le niveau global de participation aux jeux en ligne varie selon les pays, mais coïncide à peu près avec la facilité d'accès à l'Internet des enfants et des jeunes. Cependant, la disponibilité et l'accessibilité des jeux en ligne évoluent rapidement, et l'âge des enfants et des jeunes y accédant pour la première fois diminue.

Chaque semaine, 10 à 30% des enfants et des jeunes utilisant Internet, interrogés dans certains pays précis, se livrent à des activités créatives en ligne[11]. De nombreux enfants et jeunes de tous âges utilisent aussi l'Internet à des fins éducatives de manière hebdomadaire: pour faire leurs devoirs, rattraper leur retard après avoir manqué des cours ou pour chercher en ligne des renseignements sur la santé. Les enfants plus âgés semblent faire preuve d'une plus grande soif d'information que les plus jeunes.

---

[1] Livingstone, S., Kardefelt Winther, D. et Hussein, M., *Global Kids Online Comparative Report, Innocenti Research Report*. Centre de recherche de l'UNICEF – Innocenti, Florence, 2019. Disponible à l'adresse suivante: https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html.

Exploitation et abus sexuels à l'encontre des enfants en ligne

L'exploitation et les abus sexuels à l'encontre des enfants en ligne augmentent à un rythme effarant. Il y a dix ans, moins d'un million de cas de maltraitance d'enfants ont été signalés. En 2019, ce nombre est passé à 70 millions, soit une augmentation de près de 50% par rapport aux chiffres de 2018. En outre, pour la première fois, les vidéos témoignant de ces maltraitances ont été plus nombreuses que les photos dans les rapports aux autorités, montrant la nécessité de nouveaux outils pour lutter contre cette tendance. Les enfants victimes d'exploitation et d'abus sexuels en ligne appartiennent à toutes les tranches d'âge, mais sont de plus en plus jeunes. En 2018, le réseau INHOPE, qui fournit des plates-formes de signalement, a noté un changement dans le profil des victimes, passant de l'âge pubère à l'âge prépubère. Par ailleurs, des recherches menées par ECPAT International et INTERPOL en 2018 ont révélé que les jeunes enfants étaient plus susceptibles de subir des sévices graves, notamment la torture, le viol avec violence ou le sadisme. Sont également concernés les nourrissons âgés de seulement quelques jours, semaines ou mois. Alors que les filles sont plus touchées, la maltraitance des garçons peut être plus grave. Le même rapport dévoile que 80% des victimes mentionnées dans les rapports sont des filles et 17% des garçons. Les 3% restants concernaient les enfants des deux genres[1].

Quelques données[2]

- Un internaute sur trois dans le monde est un enfant.
- Toutes les demi-secondes, un enfant se connecte pour la première fois.
- 800 millions d'enfants utilisent les réseaux sociaux.
- À tout moment, on estime que 750 000 personnes en ligne cherchent à entrer en contact avec des enfants à des fins sexuelles.
- Le référentiel EUROPOL recense plus de 46 millions d'images ou de vidéos uniques montrant des abus sexuels sur des enfants.
- Plus de 89% des victimes sont âgées de 3 à 13 ans.

Pour plus d'informations sur l'ampleur de l'exploitation et des abus sexuels à l'encontre des enfants en ligne ainsi que sur les mesures destinées à les contrer, consultez le site de WePROTECT Global Alliance.

[1] Livingstone, S., Kardefelt Winther, D. et Hussein, M., *Global Kids Online Comparative Report, Innocenti Research Report*. Centre de recherche de l'UNICEF – Innocenti, Florence, 2019. Disponible à l'adresse suivante: https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html

[2] End Violence Against Children, "Safe Online".

2.1.2 L'impact des différentes plates-formes sur l'expérience numérique des enfants

L'Internet et la technologie numérique présentent des possibilités comme des risques pour les enfants et les jeunes. En voici quelques exemples.

Lorsque les enfants utilisent les **réseaux sociaux**, ils bénéficient de nombreuses occasions d'explorer, d'apprendre, de communiquer et de développer des compétences clés. Les réseaux sociaux sont considérés par les enfants comme des plates-formes leur permettant

d'explorer leur identité personnelle dans un environnement sûr. Il est important pour les jeunes d'avoir les compétences nécessaires et de savoir comment aborder les questions liées à confidentialité et à la réputation.

"Je sais que tout ce qu'on publie sur Internet y reste pour toujours, et cela peut affecter notre vie à l'avenir", garçon de 14 ans, Chili.

Cependant, compte tenu des enquêtes montrant que la plupart des enfants utilisent les réseaux sociaux avant l'âge minimum de 13 ans, et du fait que les services de vérification de l'âge sont généralement inefficaces ou insuffisants, les risques auxquels les enfants sont confrontés peuvent être graves. De plus, bien que les enfants cherchent acquérir des compétences numériques, devenir des citoyens numériques et contrôler les paramètres de confidentialité, ils ont tendance à axer leur perception de la confidentialité sur leurs amis et connaissances ("que peuvent voir mes amis?") plutôt que sur les étrangers et les tiers. Cette vision de la confidentialité, combinée à la curiosité naturelle des enfants et à un seuil de perception du risque généralement plus bas, peut les rendre vulnérables au pédopiégeage, à l'exploitation, à l'intimidation ou à d'autres types de contenus ou de contacts nuisibles.

La grande popularité du partage d'images et de vidéos via des applications mobiles, et en particulier l'utilisation de plates-formes de diffusion en direct par les enfants, présente d'autres problèmes et risques en matière de confidentialité. Certains enfants produisent des images sexuelles d'eux-mêmes, d'amis et de frères et sœurs, puis les partagent en ligne. En 2019, près d'un tiers (29%) de l'ensemble des pages web passées en revue par l'Internet Watch Foundation (IWF) contenait des images autoproduites. Parmi celles-ci, 76% présentaient des filles âgées de 11 à 13 ans, la plupart dans leur chambre ou une autre pièce du domicile. Pour certains cas, en particulier les enfants plus âgés, cela peut être considéré comme l'exploration naturelle de la sexualité et de l'identité sexuelle, tandis que pour d'autres, en particulier les jeunes enfants, il s'agit souvent d'une coercition de la part d'un adulte ou d'un autre enfant. Quoi qu'il en soit, le contenu qui en résulte est dans de nombreux pays illégal et peut exposer les enfants à des risques de poursuite. Par ailleurs, ce contenu peut également être utilisé en vue d'exploiter, de manipuler psychologiquement les enfants à des fins sexuelles ou de les extorquer.

De même, les **jeux en ligne** permettent aux enfants de réaliser leur droit fondamental de jouer, ainsi que de créer des réseaux, de passer du temps avec des amis, d'en rencontrer de nouveaux, et de renforcer des compétences clés. Bien qu'elles puissent s'avérer extrêmement positives, dans certains cas, les plates-formes de jeu peuvent également présenter des risques pour les enfants si elles sont utilisées sans surveillance et sans soutien de la part d'un adulte responsable. Parmi ces risques figurent le jeu excessif, les risques financiers liés aux achats déraisonnables dans le jeu, la collecte et la monétisation des données personnelles des enfants par les acteurs de l'industrie, la cyberintimidation, les discours de haine, la violence et l'exposition à des comportements ou des contenus inappropriés, la manipulation psychologique à des fins sexuelles, l'utilisation d'images et de vidéos réelles, générées par ordinateur, voire de réalité virtuelle illustrant et normalisant l'exploitation et les abus sexuels à l'encontre des enfants. Ces risques s'appliquent à d'autres environnements numériques où les enfants passent du temps et ne sont pas exclusifs aux environnements ludiques.

En outre, les progrès technologiques ont conduit à l'émergence de "l'**Internet des objets**", où un nombre et une variété grandissants d'appareils connectés à Internet sont capables de communiquer et d'établir un réseau via Internet. Sont concernés les jouets, les moniteurs

pour bébés et les appareils dotés d'IA, lesquels peuvent présenter des risques en matière de confidentialité et de contacts indésirables.

Bonne pratique: la recherche

Microsoft a mené des recherches sur la sécurité numérique et l'intimidation en ligne, aussi appelée cyberintimidation. En 2012, l'entreprise a interrogé des enfants âgés de 8 à 17 ans dans 25 pays sur les comportements négatifs en ligne. D'après les résultats, en moyenne, 54% des participants craignaient d'être intimidés en ligne, 37% ont indiqué avoir été victimes de cyberintimidation; et 24% ont révélé avoir déjà intimidé quelqu'un. La même enquête a démontré que moins de trois parents sur dix avaient discuté de l'intimidation en ligne avec leurs enfants. Depuis 2016, Microsoft **mène régulièrement des recherches** sur les risques en ligne en fournissant des rapports annuels sur l'indice de civilité numérique.

FACES, un programme multimédia produit par NHK Japan et par un consortium de divers diffuseurs du service public, présente les témoignages de victimes d'intimidation en ligne et hors ligne à travers le monde. Il s'agit d'une série de portraits d'adolescents dans lesquels les protagonistes expliquent, face à la caméra, comment ils ont réagi aux attaques sur le net. Cette série, produite également sous forme de clips de deux minutes, a été adoptée par Facebook, l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) et le Conseil de l'Europe. Elle est disponible en plusieurs langues.

En 2019, l'UNICEF a publié un document de travail intitulé "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry afin d'aborder les possibilités et les difficultés qui se présentent aux enfants dans l'une des industries du divertissement à la croissance la plus rapide. Ce document explore les thèmes suivants:

- Droit de jouer et liberté d'expression des enfants (temps de jeu et incidence sur la santé).
- Non-discrimination, participation et protection contre les abus (interaction et inclusion sociales, environnements toxiques, limites d'âge et vérification, protection contre le pédopiégeage et les abus sexuels).
- Droit au respect de la confidentialité et à l'absence d'exploitation économique (modèles commerciaux basés sur l'octroi d'un accès en échange de données, jeux gratuits et monétisation, manque de transparence des contenus commerciaux).

Bonne pratique: la technologie

Le Virtual Reality Action Lab de Google examine la façon dont la réalité virtuelle peut contribuer à encourager les jeunes à devenir des opposants à l'intimidation, hors ligne comme en ligne[1].

En septembre 2019, la BBC a quant à elle lancé une application mobile appelée Own IT, une application de bien-être destinée aux enfants de 8 à 13 ans recevant leur premier smartphone. Cette application s'inscrit dans le cadre de l'engagement de la BBC à soutenir les jeunes dans l'environnement médiatique en mutation d'aujourd'hui, et fait suite au lancement réussi du site Web Own IT en 2018. Dotée d'une technologie d'apprentissage automatique de pointe, l'application peut suivre l'activité des enfants sur leur smartphone et comporte une option leur permettant d'indiquer eux-mêmes leur état émotionnel. Elle s'appuie sur ces informations pour fournir un contenu et des interventions sur mesure, aidant ainsi les enfants à bénéficier d'une expérience en ligne positive et saine. Pour ce faire, elle leur adresse des coups de pouce amicaux et encourageants lorsque leur comportement semble inhabituel. Si les utilisateurs peuvent accéder à l'application lorsqu'ils recherchent de l'aide, celle-ci peut également leur fournir des conseils et une assistance instantanés à l'écran lorsqu'ils en expriment le besoin, via un clavier conçu spécialement à ces fins. Voici quelques fonctionnalités de l'application:

- Rappel à l'utilisateur de réfléchir à deux fois avant de partager des informations personnelles comme son numéro de mobile sur les réseaux sociaux.
- Aide à la compréhension sur la manière dont les messages peuvent être perçus par les autres avant que l'utilisateur n'appuie sur "Envoyer".
- Suivi de l'humeur au fil du temps et envoi de conseils sur la façon d'améliorer la situation si nécessaire.
- Apport d'informations sur des sujets tels que l'utilisation du téléphone tard le soir et l'impact sur le bien-être de l'utilisateur.

L'application propose du contenu spécialement produit à la demande de la BBC. Elle fournit des supports et des ressources utiles pour aider les jeunes à tirer le meilleur parti de leur temps en ligne et à adopter des comportements et des habitudes en ligne sains. Elle aide les jeunes et les parents à avoir des conversations plus constructives sur leurs expériences en ligne, mais ne fournit pas de rapports ou de commentaires aux parents. En outre, aucune donnée n'est transmise à partir des appareils des utilisateurs. L'application ne recueille aucune donnée personnelle ni aucun contenu produit par l'utilisateur, car l'intégralité de l'apprentissage automatique s'exécute dans l'application et dans l'appareil de l'utilisateur. Les machines sont entraînées séparément à l'aide de données d'apprentissage afin de garantir un respect total de la confidentialité des données.

[1] Pour plus d'informations, voir Alexa Hasse *et al.*, "Youth and Cyberbullying: Another Look". Berkman Klein Center for Internet & Society, 2019.

2.1.3 La situation particulière des enfants handicapés[4]

Si les enfants et les jeunes handicapés courent des risques en ligne au même titre que les autres, ils peuvent également faire face à des risques spécifiques liés à leur handicap. Les enfants et les jeunes handicapés sont souvent confrontés à l'exclusion, à la stigmatisation et à divers obstacles (physiques, économiques, sociétaux et comportementaux) entravant leur participation au sein de leur communauté. Ces expériences peuvent avoir un impact négatif sur un enfant handicapé et le conduire à rechercher des interactions sociales et des amitiés dans des espaces en ligne. Bien que de telles interactions puissent s'avérer positives en contribuant au renforcement de l'estime de soi et à la création de réseaux de soutien, elles peuvent également exposer ces enfants à un risque accru d'incidents de pédopiégeage, de sollicitation en ligne et/ou de harcèlement sexuel. Des recherches montrent que les enfants et les jeunes qui éprouvent des difficultés dans la vie réelle et ceux qui sont touchés par des difficultés psychosociales sont encore plus exposés à de tels incidents[5].

En règle générale, les enfants qui sont victimisés dans la vie réelle sont susceptibles de l'être en ligne. Ce phénomène expose les enfants handicapés à un risque plus élevé en ligne, bien qu'ils aient davantage besoin de se connecter à Internet. D'autres recherches indiquent que les enfants handicapés sont plus susceptibles de subir des mauvais traitements de toute nature[6], en particulier la victimisation sexuelle[7]. La victimisation peut comprendre l'intimidation, le harcèlement, l'exclusion et la discrimination fondés sur le handicap réel ou perçu d'un enfant ou sur des aspects liés à son handicap, tels que la façon dont il se comporte ou s'exprime, ou bien l'équipement ou les services qu'il utilise.

Les auteurs de pédopiégeage, de sollicitation en ligne et/ou de harcèlement sexuel envers les enfants et les jeunes handicapés peuvent inclure aussi bien les agresseurs préférentiels qui ciblent les enfants et les jeunes, mais aussi ceux qui ciblent les enfants et les jeunes handicapés. Parmi ces délinquants figurent notamment les "dévots", à savoir des personnes non handicapées attirées sexuellement par des personnes handicapées (le plus souvent des personnes amputées et utilisant des aides à la mobilité). Certains d'entre eux vont jusqu'à prétendre être eux-mêmes handicapés[8]. Ces personnes peuvent, par exemple, télécharger des photos et des vidéos d'enfants et de jeunes handicapés (qui sont de nature inoffensive) et/ou les partager sur des forums ou des comptes de réseaux sociaux spécialisés. Les outils de signalement sur les forums et les réseaux sociaux n'ont souvent pas de mécanismes appropriés en place pour faire face à de telles actions.

Il est à craindre que le partage en ligne par les parents d'informations et de photos de leurs enfants puisse porter atteinte à la vie privée d'un enfant, entraîner l'intimidation et l'embarras, ou avoir des conséquences négatives plus tard dans sa vie[9]. Certains parents d'enfants handicapés peuvent partager des informations ou des contenus multimédias de leur enfant

4 Conseil de l'Europe, "Deux clics en avant et un clic en arrière: Rapport sur les enfants en situation de handicap dans l'environnement numérique", 2019.
5 Andrew Schrock *et al.*, "Solicitation, Harassment, and Problematic Content". Berkman Center for Internet & Society, 2008.
6 UNICEF, "La Situation des enfants dans le monde 2013: les enfants handicapés".
7 Katrin Mueller Johnson *et al.*, "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors". *Journal of Interpersonal Violence*, 2014.
8 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", *Sexuality and Disability*, 1997.
9 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy". Document de travail Innocenti 2017-03.

à la recherche de soutien ou de conseils, ce qui expose leur enfant à des risques de violation de la vie privée, dans l'immédiat et à l'avenir. Ces parents risquent également d'être ciblés par des personnes non informées ou sans scrupules qui proposent des traitements, des thérapies ou des "remèdes" pour le handicap de leur enfant. De même, certains parents d'enfants et de jeunes handicapés peuvent se montrer surprotecteurs en raison de leur manque de connaissances sur la meilleure façon de guider leurs enfants sur l'utilisation de l'Internet ou de les protéger contre l'intimidation ou le harcèlement[10].

Certains enfants et jeunes handicapés peuvent éprouver des difficultés à utiliser des environnements en ligne, voire en être exclus. Cela peut s'expliquer par des conceptions inaccessibles (par exemple, des applications qui ne permettent pas d'augmenter la taille du texte), le refus de demandes d'adaptation (par exemple, l'intégration d'un logiciel de lecteur d'écran ou de commandes informatiques adaptables) ou un besoin en soutien approprié (par exemple, des explications sur l'utilisation de l'équipement, un soutien individuel pour créer des interactions sociales)[11].

2.2 Modèles nationaux et transnationaux existants pour la protection des enfants en ligne

Au niveau mondial, plusieurs modèles sont adoptés pour assurer la sécurité des enfants et des jeunes en ligne. Il est recommandé aux parties prenantes de l'industrie de les considérer comme des orientations aux fins de la mise en œuvre d'initiatives internationales et comme un cadre visant à garantir qu'elles ne ménagent aucun effort pour protéger les enfants et les jeunes en ligne. Le secteur de l'Internet est une arène diversifiée et complexe, composée d'entreprises aux tailles et aux fonctions diverses. Il est essentiel que la protection de l'enfance soit abordée non seulement par les plates-formes et services de contenus, mais aussi par ceux qui soutiennent l'infrastructure de l'Internet.

Il convient de noter que la capacité d'un secteur à mettre en place une politique globale de protection de l'enfance est limitée à ses ressources disponibles. Ces lignes directrices recommandent donc aux différents secteurs de collaborer en vue de déployer ensemble des services visant à protéger les utilisateurs. En partageant leurs ressources et leur expertise technique, ils pourraient créer plus efficacement des "espaces sûrs" pour prévenir les abus.

Coopération intrasectorielle

La Technology Coalition est un exemple de coopération fructueuse entre les parties prenantes du secteur pour lutter contre l'exploitation et les abus sexuels à l'encontre des enfants.

Modèles transnationaux

Les professionnels devraient inclure des directives internationales pertinentes dans leur programme structurel, et se conformer à toute législation nationale ou transnationale pertinente applicable dans les pays où ils opèrent. Ils devraient non seulement prendre en compte les actions à entreprendre au niveau juridique, mais aussi les activités qu'ils peuvent mener et,

[10] UNICEF, "Is there a ladder of children's online participation?". Document de recherche Innocenti, 2019.
[11] Pour connaître les directives concernant ces droits, consulter la Convention des Nations Unies relative aux droits des personnes handicapées son Protocole facultatif, en particulier l'Article 9 relatif à l'accessibilité et l'Article 21 relatif à la liberté d'expression et d'opinion, et l'accès à l'information.

si possible, chercher à mettre en œuvre des initiatives à l'échelle mondiale. Voici quelques modèles fournissant des principes à l'appui de telles initiatives:

- Five Country Ministerial, Voluntary principles to counter online CSEA (Principes volontaires pour lutter contre l'exploitation et les abus sexuels à l'encontre des enfants en ligne), 2020
- Commission "Le large bande au service du développement durable", 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), 2019
- WePROTECT Global Alliance, Une réponse stratégique mondiale à l'exploitation sexuelle et à l'abus des enfants en ligne, 2019
- Partenariat mondial pour l'élimination de la violence envers les enfants, Safe to Learn: Call to Action (Apprendre en toute sécurité: appel à l'action)
- Child Dignity in the Digital World, Child Dignity Alliance: Technology Working Group Report (Alliance pour la dignité de l'enfant: rapport du groupe de travail sur les technologies), 2018
- Directive (UE) 2018/1808 du Parlement européen et du Conseil: directive "Services de médias audiovisuels"
- Règlement général sur la protection des données de la Commission européenne, 2018
- Recommandation du Conseil de l'OCDE sur la protection des enfants sur Internet, 2012

Modèles nationaux

Un certain nombre de modèles nationaux et internationaux définissent clairement les rôles et les responsabilités de l'industrie des technologies dans la protection des enfants en ligne. Certains d'entre eux ne sont pas spécifiques aux enfants en soi, mais peuvent s'appliquer à eux en tant qu'utilisateurs de l'Internet. Ils fournissent des directives générales au secteur concernant les politiques réglementaires, les normes et la collaboration intersectorielle. Aux fins du présent document, les principes clés de ces modèles sont mis en évidence, tels qu'ils s'appliquent à l'industrie des TIC.

Le code Age Appropriate Design, Royaume-Uni

Début 2019, le Bureau du Commissaire à l'information a publié des propositions pour son code de conception adapté à l'âge en faveur de la protection des données des enfants. Le code proposé est fondé sur l'intérêt supérieur de l'enfant, tel que défini dans la Convention des Nations Unies relative aux droits de l'enfant, et définit plusieurs attentes vis-à-vis du secteur. Le code est constitué de quinze normes, dont l'obligation de désactivation par défaut des services de localisation pour les enfants. Ainsi, le secteur ne collecte et ne conserve que le minimum de données personnelles des mineurs, les produits sont par défaut privés et les explications sont adaptées à l'âge et accessibles.

Le Harmful Digital Communications Act, Nouvelle-Zélande

Cette Loi de 2015 a fait des abus en ligne un crime spécifique et porte sur un large éventail de préjudices, de la cyberintimidation à la pornodivulgation. Elle vise à dissuader, prévenir et réduire les communications numériques nuisibles, rendant illégale la publication des communications numériques ayant l'intention de causer une détresse émotionnelle grave à autrui. En outre, elle énonce une série de 10 principes de communication. Elle permet aux utilisateurs de porter plainte auprès d'une organisation indépendante si ces principes ne sont pas respectés, ou de demander des décisions judiciaires contre l'auteur ou l'hôte de la communication si le problème n'est pas résolu.

Le Commissaire à la sécurité en ligne, Australie

Créé en 2015, le Bureau du Commissaire australien à la sécurité en ligne (eSafety Commissionner) est la première agence publique au monde vouée à la lutte contre les abus et à la sécurité de ses citoyens en ligne. En tant que régulateur national indépendant pour la sécurité en ligne, l'organisme eSafety rassemble une puissante combinaison de fonctions. On compte parmi celles-ci la prévention par la sensibilisation, l'éducation, la fourniture de conseils en matière de recherche et de bonnes pratiques, l'intervention précoce et la réparation des dommages par le biais de divers régimes réglementaires légaux qui donnent à eSafety le pouvoir d'éliminer rapidement la cyberintimidation, les abus liés à la pornodivulgation et les contenus en ligne illégaux. Cette multitude de capacités permet à eSafety d'assurer la sécurité en ligne de manière multiforme, globale et proactive.

En 2018, eSafety a développé l'initiative Safety by Design (SbD), qui place la sécurité et les droits des utilisateurs au cœur de la conception, du développement et du déploiement de produits et services en ligne. Cette initiative est fondée sur l'application d'un ensemble de principes de sécurité dès la conception. Elle définit des mesures sérieuses, concrètes et réalisables à mettre en place par l'industrie en vue de mieux protéger les citoyens en ligne. En voici les trois principes généraux:

1) **Responsabilités du fournisseur de services**: le devoir relatif à la sécurité ne doit jamais incomber seulement à l'utilisateur final. Des mesures préventives peuvent être prises pour garantir que les préjudices connus et prévus ont été évalués dans le cadre de la conception et de la fourniture d'un service en ligne, au même titre que les mesures visant à rendre les services moins susceptibles de faciliter, d'attiser ou d'encourager les comportements illégaux et inappropriés.
2) **Autonomisation et responsabilisation des utilisateurs**: la dignité des utilisateurs et leur intérêt supérieur sont d'une importance capitale. La capacité d'action et l'autonomie humaines doivent être encouragées, amplifiées et renforcées dans la conception des services, afin de conférer aux utilisateurs un contrôle, une gouvernance et une réglementation accrus de leurs propres expériences.
3) **Transparence et responsabilité**: ce sont les caractéristiques d'une approche solide de la sécurité. Elles garantissent que les services fonctionnent conformément aux objectifs de sécurité définis, et qu'ils éduquent et responsabilisent le public sur les mesures qui peuvent être prises pour résoudre les problèmes de sécurité.

La WePROTECT Global Alliance

La stratégie de la WePROTECT Global Alliance consiste essentiellement à aider les pays à établir des interventions coordonnées et multipartites contre l'exploitation sexuelle des enfants en ligne. L'élaboration de ces interventions est guidée par le modèle de réponse nationale de l'Alliance, qui sert de plan pour toute action au niveau national. Cette stratégie fournit aux pays un cadre sur lequel s'appuyer pour lutter contre l'exploitation sexuelle des enfants en ligne. Dans le modèle de réponse nationale de WePROTECT, il existe un ensemble clair d'engagements des sociétés de TIC concernant:

- les procédures de notification et de retrait;
- le signalement des cas d'exploitation et d'abus sexuels à l'encontre des enfants en ligne;
- l'élaboration de solutions technologiques; et
- l'investissement dans des programmes de prévention et dans des services d'intervention efficaces en matière de protection des enfants en ligne.

Le Partenariat et le fonds mondiaux pour l'élimination de la violence envers les enfants

Le Partenariat et le Fonds mondiaux pour l'élimination de la violence envers les enfants ont été lancés par le Secrétaire général des Nations Unies en 2016 avec un seul objectif: catalyser et soutenir l'action visant à mettre fin à toutes les formes de violence contre les enfants d'ici à 2030 grâce à une collaboration unique de plus de 400 partenaires de tous les secteurs.

Cette initiative est axée sur le secours des victimes et le soutien qui peut leur être apporté, les solutions technologiques permettant de détecter et de prévenir les infractions, l'appui aux autorités répressives, les réformes législatives et politiques, la génération de données et d'éléments de preuve sur l'ampleur et la nature de l'exploitation et des abus sexuels dont sont victime les enfants en ligne, ainsi que sur la compréhension du point de vue des enfants[12].

3 Points essentiels liés à la protection et à la promotion des droits de l'enfant

Cette section décrit **cinq domaines clés** dans lesquels les entreprises peuvent prendre des mesures pour protéger la sécurité des enfants et des jeunes lors de l'utilisation des TIC et promouvoir une utilisation positive de ces dernières.

3.1 Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés

Pour intégrer les considérations liées aux droits de l'enfant, les entreprises doivent prendre des mesures adéquates pour repérer, prévenir, atténuer et, le cas échéant, remédier aux répercussions négatives potentielles et réelles sur les droits des enfants. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme invitent toutes les entreprises et industries à mettre en place des politiques et des processus appropriés pour s'acquitter de leur responsabilité de respecter les droits de l'homme.

Les industries doivent accorder une attention particulière à la protection des données du groupe vulnérable que constituent les enfants et les jeunes, mais aussi à leur liberté d'expression. La Résolution 68/167 de l'Assemblée générale des Nations Unies sur le droit à la vie privée à l'ère du numérique réaffirme le droit à la vie privée et à la liberté d'expression sans subir d'immixtions illégales. En outre, la Résolution 32/13 du Conseil des droits de l'homme des Nations Unies sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, reconnaît la nature mondiale et ouverte de l'Internet en tant que moteur de l'accélération des progrès vers le développement, et affirme que les droits dont disposent les personnes dans la vie réelle doivent également être protégés en ligne. Dans les États où il n'existe pas de cadres juridiques adéquats pour la protection des droits des enfants et des jeunes à la vie privée et à la liberté d'expression, les entreprises doivent faire preuve d'une diligence raisonnable renforcée pour garantir que les politiques et les pratiques sont conformes au droit international. Alors que l'engagement citoyen des jeunes continue de croître grâce aux communications en ligne, les entreprises ont une plus grande responsabilité en matière de respect des droits des enfants et des jeunes, même lorsque les lois nationales ne sont pas encore conformes aux normes internationales.

[12] Pour plus d'informations, consulter la page du Partenariat consacrée aux bénéficiaires du Fonds.

Les entreprises doivent avoir mis en place un mécanisme de réclamation au niveau opérationnel afin de permettre aux personnes concernées de faire remonter leurs préoccupations à propos de potentielles violations. De tels mécanismes doivent être accessibles aux enfants, à leur famille et à ceux qui représentent leurs intérêts. Le principe 31 des Principes directeurs relatifs aux entreprises et aux droits de l'homme précise que ces mécanismes doivent être légitimes, accessibles, prévisibles, équitables, transparents, compatibles avec les droits, une source d'apprentissage permanent et fondés sur la participation et le dialogue. Parallèlement aux processus internes de lutte contre les impacts négatifs, les mécanismes de réclamation doivent garantir que les entreprises disposent de cadres pour assurer aux enfants et aux jeunes la possibilité d'un recours approprié lorsque leurs droits sont menacés.

Lorsque les entreprises adoptent une approche de la sécurité des TIC fondée sur la conformité et axée sur le respect de la législation nationale, en suivant les directives internationales en l'absence de législation nationale et en évitant les impacts négatifs sur les droits des enfants et des jeunes, elles promeuvent de manière proactive le développement et le bien-être des enfants et des jeunes à travers des actions volontaires qui font progresser les droits de ceux-ci à accéder à l'information, à la liberté d'expression, à la participation, à l'éducation et à la culture.

Bonne pratique: cadre normatif et conception adaptée à l'âge

Le développeur d'applications Toca Boca conçoit des jouets numériques en se basant sur le point de vue de l'enfant. La politique de confidentialité de l'entreprise vise à renseigner les utilisateurs sur les informations que l'entreprise collecte et sur la façon dont elles sont utilisées. Toca Boca, Inc. est membre du programme de certification COPPA Safe Harbor de PRIVO Kids.

LEGO® Life est un exemple de plate-forme de réseaux sociaux sécurisée permettant aux enfants de moins de 13 ans de partager leurs créations LEGO, de trouver de l'inspiration et d'interagir en toute sécurité. Dans cet espace, les enfants ne sont pas invités à fournir des informations personnelles pour créer un compte, car la procédure requiert seulement l'adresse e-mail d'un parent ou d'une personne s'occupant de l'enfant. L'application permet aux enfants et aux familles de discuter de la sécurité et de la confidentialité en ligne dans un environnement favorable.

Parmi les conceptions adaptées à l'âge, on trouve des offres spécifiques de radiodiffuseurs de droit public majeurs à l'attention de certaines tranches d'âge: par exemple, le groupe de radiodiffuseurs allemands ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland – Das Erste) et la chaîne ZDF (Zweites Deutsches Fernsehen) ciblent leur public à partir de 14 ans, proposant un contenu personnalisé via la chaîne en ligne funk.net. La BBC (British Broadcasting Corporation) a lancé CBeebies, qui s'adresse aux enfants de moins de 6 ans. Le contenu du site web est spécialement conçu pour des tranches d'âge particulières.

Bonne pratique: cadre normatif et technologie

Twitter investit continuellement dans une technologie propriétaire qui contribue à réduire régulièrement la charge qui incombe aux utilisateurs d'effectuer des signalements[1]. Plus précisément, plus de 50% des tweets (contre 20% en 2018) que Twitter suit en raison de leur nature abusive sont actuellement détectés de manière proactive grâce à cette technologie, plutôt qu'à partir des signalements à l'entreprise. Cette nouvelle technologie est utilisée pour traiter les domaines normatifs relatifs à l'information privée, aux médias sensibles, aux comportements haineux, aux abus et à l'usurpation d'identité.

[1] Twitter, "15th Transparency Report: Increase in proactive enforcement on accounts".

3.2 Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants

En 2019, l'IWF a analysé 132 676 pages web confirmées comme contenant du matériel montrant des abus sexuels sur des enfants[13]. Toute URL peut contenir des centaines, voire des milliers, d'images et de vidéos. Parmi les images examinées par l'IWF, 45% montraient des enfants âgés de 10 ans ou moins, et 1 609 pages web représentaient des enfants âgés de 0 à 2 ans, dont 71% contenaient les cas d'abus sexuels les plus graves, tels que le viol et la torture sexuelle. Ces faits troublants soulignent l'importance d'une action concertée de la part de l'industrie, des gouvernements, des services de police et de la société civile pour lutter contre le matériel montrant des abus sexuels sur des enfants.

Alors que de nombreux gouvernements luttent contre la diffusion de matériel montrant des abus sexuels sur des enfants en promulguant des lois, en poursuivant et en traduisant en justice les agresseurs, en sensibilisant la population et en aidant les enfants et les jeunes à se rétablir après avoir été maltraités ou exploités, beaucoup d'entre eux ne disposent pas encore de systèmes adéquats. Des mécanismes sont nécessaires dans chaque pays pour permettre au grand public de signaler les contenus de cette nature à caractère abusif et exploitant. L'industrie, les forces de police, les gouvernements et la société civile doivent travailler de concert pour garantir la mise en place de cadres juridiques appropriés et conformes aux normes internationales. De tels cadres devraient incriminer toutes les formes d'exploitation et d'abus sexuels à l'encontre des enfants, y compris le matériel montrant des abus sexuels sur des enfants, et protéger les enfants victimes. Ces cadres doivent garantir que les processus de signalement, d'enquête et de suppression de contenu fonctionnent aussi efficacement que possible.

Les professionnels doivent assurer les liens vers des services de signalement nationaux ou locaux, comme les portails IWF dans certains pays. En l'absence de canaux de signalement locaux, ils doivent fournir des liens vers d'autres services internationaux, le cas échéant, comme le National Center for Missing and Exploited Children (centre national pour les enfants disparus et exploités) aux États-Unis ou l'International Association of Internet Hotline (Association

[13] IWF, "The why. The how. The who. And the results. Annual Report 2019".

internationale de services de signalement en ligne, INHOPE), n'importe laquelle des plates-formes internationales de signalement pouvant être utilisée à cette fin.

Les entreprises responsables prennent un certain nombre de mesures pour empêcher que leurs réseaux et services ne soient utilisés pour diffuser du matériel montrant des abus sexuels sur des enfants. Il s'agit notamment d'introduire des formulations dans les conditions générales ou les codes de conduite qui interdisent explicitement de tels contenus ou comportements[14], de mettre en place de solides processus de notification et de retrait, de collaborer avec les plates-formes de signalement nationales et de les soutenir.

De plus, certaines entreprises déploient des mesures techniques pour empêcher l'utilisation abusive de leurs services ou réseaux en vue de partager du matériel connu montrant des abus sexuels sur des enfants. Par exemple, certains fournisseurs de services Internet bloquent l'accès aux URL confirmées par une autorité compétente comme contenant du matériel montrant des abus sexuels sur des enfants si le site web est hébergé dans un pays où aucun processus n'est en place pour garantir qu'il sera rapidement supprimé. D'autres déploient des technologies de hachage afin de détecter et de supprimer automatiquement les images représentant des abus sexuels sur des enfants qui sont déjà connues des forces de l'ordre ou des plates-formes de signalement. Les professionnels doivent envisager et intégrer tous les services pertinents pour leurs opérations afin de prévenir la diffusion de telles images.

Les acteurs du secteur doivent s'engager à consacrer des ressources proportionnées et continuer à développer et à privilégier le partage de solutions technologiques open source pour détecter et supprimer le matériel montrant des abus sexuels sur des enfants.

Bonne pratique: la technologie

Microsoft utilise une approche en quatre volets pour favoriser une utilisation responsable et sûre de la technologie, en mettant l'accent sur la technologie elle-même, l'autogouvernance, les partenariats, ainsi que l'éducation et la sensibilisation des consommateurs. Microsoft a également intégré des fonctionnalités qui permettent aux individus de gérer plus efficacement leur sécurité en ligne. L'une de ces fonctionnalités, intitulée "Sécurité familiale", permet aux parents et aux personnes s'occupant d'enfants de surveiller la façon dont leurs enfants utilisent l'Internet.

Microsoft applique des politiques contre le harcèlement sur ses plates-formes, et les utilisateurs qui enfreignent ces réglementations sont soumis à la résiliation de leur compte ou, en cas de violations plus graves, à des mesures répressives.

[14] Il convient de noter que la conduite inappropriée d'un utilisateur ne se limite pas au matériel montrant des abus sexuels sur des enfants et que tout type de comportement ou de contenu inapproprié doit être géré de manière appropriée par l'entreprise.

La technologie PhotoDNA de Microsoft est un outil qui crée des hachages d'images et les compare à une base de données de hachages déjà identifiés et confirmés comme matériel montrant des abus sexuels sur des enfants. Si l'outil trouve une correspondance, l'image est bloquée. Cet instrument a permis aux fournisseurs de contenu de supprimer des millions de photographies illégales de l'Internet, aidé à condamner les prédateurs sexuels d'enfants et, dans certains cas, aidé les forces de l'ordre à sauver des victimes potentielles avant que leur intégrité physique ne soit atteinte. La société Microsoft étant engagée depuis longtemps à protéger ses clients contre les contenus illégaux sur ses produits et services, l'application de cette technologie déjà créée par l'entreprise pour lutter contre la multiplication des vidéos illégales était une suite logique dans son implication. Cependant, cet outil n'est pas doté de technologie de reconnaissance faciale et ne peut pas identifier une personne ou reconnaître un objet sur l'image. C'est avec l'invention de PhotoDNA for Video que les choses ont pris un nouveau tournant. PhotoDNA for Video décompose les vidéos en trames de référence et crée essentiellement des hachages pour ces captures d'écran. De la même manière que PhotoDNA recherche des correspondances pour une image qui a été modifiée en vue d'éviter toute détection, PhotoDNA for Video peut trouver des contenus d'exploitation sexuelle d'enfants qui ont été modifiés ou rassemblés en une vidéo qui pourrait sembler inoffensive.

En outre, Microsoft a récemment lancé un nouvel outil permettant d'identifier les prédateurs d'enfants qui les mettent en confiance en vue d'en abuser dans les chats en ligne. Project Artemis, élaboré en collaboration avec The Meet Group, Roblox, Kik et Thorn, s'appuie sur la technologie brevetée de Microsoft et sera mis gratuitement à disposition via Thorn aux sociétés de services en ligne qualifiées qui offrent une fonction de chat. Project Artemis est un outil technologique qui aide à avertir les administrateurs lorsqu'une modération est nécessaire dans les salles de chat. Grâce à cette technique de détection du pédopiégeage, il sera possible d'identifier, d'approcher et de signaler les prédateurs qui tentent d'attirer des enfants à des fins sexuelles.

L'**IWF** fournit une gamme de services aux professionnels du secteur afin de protéger leurs utilisateurs du matériel montrant des abus sexuels sur des enfants. Ces services sont notamment:

- Une liste de blocage d'URL dynamique et de qualité garantie, mise à jour en temps réel.
- Une liste de hachage du matériel criminel connu montrant des abus sexuels sur des enfants.
- Une liste unique de mots clés cryptés connus pour être associés à du matériel montrant des abus sexuels sur des enfants.
- Une liste détaillée des noms de domaine connus pour héberger des contenus montrant des abus sexuels sur des enfants, permettant la suppression rapide des domaines hébergeant des contenus illégaux.

3.3 Créer un environnement numérique plus sûr et adapté à l'âge

Très peu de choses dans la vie peuvent être considérées comme absolument sûres et sans risque en permanence. Même dans les villes où la circulation est hautement réglementée et

étroitement contrôlée, des accidents se produisent encore. De même, le cyberespace n'est pas sans risques, notamment pour les enfants et les jeunes. Ceux-ci peuvent être considérés comme des récepteurs, des participants et des acteurs dans leur environnement en ligne. Les risques auxquels ils sont confrontés peuvent être classés en quatre catégories[15]:

- *Contenu inapproprié* – Les enfants et les jeunes peuvent tomber sur du contenu inapproprié et illégal lorsqu'ils recherchent autre chose en cliquant sur un lien semblant inoffensif dans un message instantané, sur un blog ou lors d'un partage de fichiers. Ils peuvent également rechercher et partager des contenus inappropriés ou réservés à un certain public. Les contenus considérés comme préjudiciables varient d'un pays à l'autre. Il s'agit entre autres des contenus qui favorisent l'abus de substances psychoactives, la haine raciale, les comportements à risque, le suicide, l'anorexie ou la violence.
- *Comportement inapproprié* – Certains enfants et adultes peuvent utiliser l'Internet pour harceler, voire exploiter d'autres personnes. Les enfants peuvent parfois diffuser des commentaires blessants ou des images embarrassantes, ou bien voler du contenu ou porter atteinte à des droits d'auteur.
- *Contact inapproprié* – Certains adultes et jeunes peuvent utiliser l'Internet pour rechercher des enfants ou d'autres jeunes vulnérables. Souvent, ils cherchent à convaincre leur cible qu'ils ont développé une relation significative, à des fins sous-jacentes de manipulation. Ils peuvent tenter de persuader l'enfant de commettre des actes sexuels ou d'autres actes de violence en ligne, en utilisant une webcam ou un autre appareil d'enregistrement. Ils peuvent aussi essayer d'organiser une rencontre en personne et d'initier un contact physique. Ce processus est souvent appelé "pédopiégeage" ou "grooming".
- *Risques commerciaux* – Cette catégorie fait référence aux risques de confidentialité liés à la collecte et à l'utilisation des données des enfants, ainsi qu'au marketing numérique. La sécurité en ligne est un défi communautaire et une occasion pour le secteur, les gouvernements et la société civile de travailler ensemble à l'établissement de principes et de pratiques de sécurité. Le secteur de l'Internet peut offrir une multitude d'approches techniques, d'outils et de services aux parents, aux enfants et aux jeunes, et devrait avant tout créer des produits faciles à utiliser, sûrs de par leur conception et adaptés selon l'âge des nombreux utilisateurs. D'autres approches incluent la mise à disposition d'outils permettant de créer des systèmes de vérification de l'âge approprié qui respectent les droits des enfants en matière de confidentialité et d'accès, qui limitent l'accès des enfants et des jeunes à des contenus inappropriés pour leur âge, ou encore qui restreignent les personnes avec lesquelles les enfants peuvent entrer en contact ou limitent les moments auxquels ils peuvent se connecter à l'Internet. Plus important encore, les cadres de "sécurité dès la conception[16]", y compris la confidentialité, doivent être intégrés dans les processus d'innovation et de conception des produits. La sécurité des enfants et l'utilisation responsable de la technologie doivent être soigneusement prises en compte et ne doivent pas être considérées *a posteriori*.

Certains programmes permettent aux parents de surveiller les textos et autres communications que leurs enfants et jeunes envoient et reçoivent. Si des programmes de ce type doivent être utilisés, il est important d'en discuter ouvertement avec l'enfant. En l'absence de conversation, une telle conduite peut être perçue comme de l'"espionnage" et affecter la confiance au sein de la famille.

L'élaboration de politiques d'utilisation acceptable est un moyen pour les entreprises d'établir quel type de comportement est encouragé chez les adultes et les enfants, quels types d'activités ne sont pas acceptables et les conséquences de toute violation de ces politiques. Des mécanismes de signalement clairs et transparents doivent être mis à la disposition des

[15] Sonia Livingstone et al., "EU Kids Online: Final Report". London School of Economics and Political Science, 2009.
[16] eSafety Commissioner, Safety by Design Overview, 2019.

utilisateurs ayant des doutes concernant un contenu ou un comportement. En outre, les signalements doivent faire l'objet d'un suivi approprié, et leur état doit être mis à jour en temps opportun. Bien que la mise en œuvre des mécanismes de suivi des entreprises puisse varier selon le cas, il est essentiel d'établir un calendrier clair pour les réponses, de communiquer les décisions prises concernant le signalement et de proposer une méthode de suivi si l'utilisateur n'est pas satisfait de la réponse.

Bonne pratique: signalements

Afin de lutter contre le harcèlement sexuel sur les plates-formes numériques, Facebook a cofinancé le projet deSHAME avec l'Union européenne, une collaboration entre Childnet, Save the Children, Kek Vonal et UCLan. Ce projet vise à accroître les signalements de harcèlement sexuel en ligne parmi les mineurs et à améliorer la coopération multisectorielle pour prévenir ce comportement et le contrer.

Étant donné que l'un des principaux objectifs du projet est d'encourager les utilisateurs à signaler tout contenu dérangeant ou inapproprié, les Standards de la communauté de Facebook constituent également des lignes directrices pertinentes sur ce qui est autorisé ou non sur la plate-forme. Ces standards décrivent également les types d'utilisateurs qui ne sont pas autorisés à publier. Facebook a par ailleurs créé des fonctionnalités de sécurité telles que "Connaissez-vous cette personne?", une "seconde" boîte de réception rassemblant les nouveaux messages de personnes que l'utilisateur ne connaît pas, et une fenêtre contextuelle qui apparaît sur le fil d'actualité s'il semble qu'un mineur est contacté par un adulte qu'il ne connaît pas.

Les fournisseurs de contenus et de services en ligne peuvent également décrire la nature des contenus ou des services qu'ils fournissent et la tranche d'âge cible. Ces descriptions doivent être conformes aux normes nationales et internationales préexistantes, aux réglementations en vigueur et aux conseils sur le marketing et la publicité destinés aux enfants mis à disposition par les organismes de classification appropriés. Ce processus devient cependant plus difficile avec la croissance des services interactifs qui permettent la publication de contenu produit par les utilisateurs, par exemple via des panneaux de messages, des forums de discussion et des services de réseaux sociaux. Lorsque les entreprises ciblent spécifiquement les enfants et les jeunes et que les services s'adressent massivement à un public plus jeune, les exigences seront beaucoup plus élevées **sur les plans de la sécurité ainsi que de la convivialité des contenus, de leur compréhensibilité et de leur accessibilité**.

Les entreprises sont également encouragées à adopter les normes de confidentialité les plus strictes en matière de collecte, de traitement et de stockage de données fournies par des enfants et des jeunes ou à leur sujet. En effet, ces derniers peuvent manquer de maturité pour évaluer les conséquences sociales et personnelles étendues qu'impliquent la divulgation de leurs informations personnelles en ligne, l'acceptation de partager celles-ci ou l'utilisation de ces informations à des fins commerciales. Les services destinés à un public principalement constitué d'enfants et de jeunes ou susceptibles d'attirer ce type d'audience doivent tenir compte des risques que présente pour eux l'accès par des tiers à leurs informations personnelles, la collecte et l'utilisation de ces informations (y compris les informations de localisation). Il incombe aux prestataires de services de garantir que ces risques sont correctement pris en compte et que les utilisateurs en sont informés. En particulier, les entreprises doivent s'assurer de la justesse

du langage et du style des supports et des communications employés pour promouvoir leurs services, y fournir un accès ou pour accéder aux informations personnelles, les recueillir et les utiliser. Elles sont également tenues d'aider les utilisateurs à comprendre le principe de confidentialité et à gérer leurs préférences en la matière de manière claire et simple. Enfin, elles doivent expliquer ce à quoi les utilisateurs consentent dans un langage clair et accessible.

Bonne pratique: innovation

En 2018-2019, le Bureau régional de l'UNICEF pour l'Asie de l'Est et le Pacifique a organisé cinq tables rondes multipartites afin de partager les pratiques prometteuses du secteur pour lutter contre l'exploitation et les abus sexuels à l'encontre des enfants en ligne. Les participants aux tables rondes comptaient des entreprises du secteur privé de premier plan, telles que Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongolie) Mobifone+ (Viet Nam), Globe Telecom (Philippines), True (Thaïlande), la GSMA, ainsi que des partenaires de la société civile, notamment INHOPE, ECPAT International et Child Helpline International.

Dans le cadre du même projet, en février 2020, l'UNICEF a lancé un groupe de réflexion pour accélérer le leadership du secteur dans la région de l'Asie de l'Est et du Pacifique en vue de prévenir la violence contre les enfants dans le monde en ligne. Ce groupe de réflexion est un incubateur d'idées et d'innovation s'appuyant sur la perspective unique des acteurs du secteur (création de produits, marketing, etc.) aux fins du développement de supports pédagogiques percutants et de la détermination des plates-formes d'exécution les plus efficaces. Il vise également la création d'un cadre d'évaluation capable de mesurer l'impact de ces supports et messages éducatifs destinés aux enfants. Le groupe de réflexion est composé de Facebook, Telenor, d'experts universitaires, d'entités des Nations Unies, notamment l'UIT, l'UNESCO et l'Office des Nations Unies contre la drogue et le crime, mais aussi eSafety Commissioner, ECPAT International, le Centre international pour enfants disparus et sexuellement exploités, INTERPOL et le Fonds mondial pour l'élimination de la violence envers les enfants. La réunion inaugurale du groupe de réflexion, qui s'est tenue parallèlement à la Conférence régionale de l'Association des nations de l'Asie du Sud-Est sur la protection en ligne des enfants, a réuni des experts, dont Microsoft, afin d'explorer les possibilités technologiques et de recherche qui permettraient de mieux suivre les changements de comportement en ligne, sur la base de l'adoption de documents et de messages de sécurité en ligne.

3.4 Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC

Si des mesures techniques peuvent être cruciales pour garantir que les enfants et les jeunes sont protégés contre les risques potentiels en ligne, il ne s'agit là que d'une partie de l'équation. **Les outils de contrôle parental, la sensibilisation** et l'éducation sont également des éléments clés qui aideront à autonomiser et à informer les enfants et les jeunes de tous âges, ainsi que les parents, les personnes s'occupant d'enfants et les éducateurs. Bien que les entreprises aient un rôle important à jouer pour encourager les enfants et les jeunes à utiliser les TIC de

manière responsable et sûre, cette responsabilité est partagée avec les parents, les écoles, les enfants et les jeunes.

De nombreuses entreprises investissent dans des programmes éducatifs conçus pour permettre aux utilisateurs de prendre des décisions éclairées sur les contenus et les services. Elles aident les parents, les personnes s'occupant d'enfants et les éducateurs à guider les enfants et les jeunes vers des expériences en ligne et mobiles plus sûres, plus responsables et appropriées. Cela se traduit notamment par l'affichage de contenu approprié à l'âge de l'utilisateur, et par la garantie que les informations sur des éléments tels que le prix des contenus, les conditions d'abonnement et les procédures d'annulation des abonnements sont clairement communiquées. La promotion du respect de l'âge minimum requis par les réseaux sociaux dans tous les pays où la vérification de l'âge est possible contribuerait également à protéger les enfants, en leur permettant d'accéder à des services adaptés à leur âge. Il est néanmoins important de bien tenir compte de la collecte de données personnelles supplémentaires que cela peut impliquer, ainsi que de la nécessité de limiter cette collecte, mais aussi le stockage et le traitement de ces informations.

Il est également important de fournir directement aux enfants et aux jeunes des informations en faveur d'une utilisation plus sûre des TIC, et de communiquer sur les comportements positifs et responsables en la matière. Au-delà de la sensibilisation à la sécurité, les entreprises peuvent favoriser les expériences positives en créant du contenu pour les enfants et les jeunes sur le respect, la gentillesse et l'ouverture d'esprit lors de l'utilisation des TIC et lorsqu'ils prennent soin d'amis. Elles peuvent fournir des informations sur les mesures à prendre en cas d'expériences négatives, telles que l'intimidation ou la manipulation psychologique à des fins sexuelles, en facilitant le signalement de tels incidents et en créant une fonction permettant de refuser les messages anonymes.

Les parents ont parfois une compréhension et une connaissance de l'Internet et des appareils mobiles moins avancées que les enfants et les jeunes. De plus, la convergence des appareils mobiles et des services Internet rend la surveillance parentale plus difficile. Les professionnels peuvent travailler en collaboration avec le gouvernement et les éducateurs pour améliorer la capacité des parents à aider leurs enfants à renforcer leur résilience numérique et à agir en citoyens numériques responsables. L'objectif n'est pas de transférer la responsabilité de l'utilisation des TIC chez les jeunes aux seuls parents, mais plutôt de reconnaître que ces derniers sont mieux placés pour décider de ce qui convient à leurs enfants, et qu'ils devraient être informés de tous les risques afin de mieux protéger leurs enfants et leur donner les moyens d'agir.

Les informations peuvent être transmises en ligne et hors ligne via plusieurs canaux multimédias, en tenant compte du fait que certains parents n'utilisent pas de services Internet. Il est important de collaborer avec les académies pour fournir aux enfants et aux jeunes des programmes scolaires sur la sécurité en ligne et l'utilisation responsable des TIC, ainsi que du matériel éducatif aux parents. Citons par exemple l'explication des types de services et d'options disponibles pour surveiller les activités, les mesures à prendre si un enfant est victime d'intimidation ou de pédopiégeage, les méthodes pour éviter les spams et gérer les paramètres de confidentialité, et les conseils pour parler de sujets sensibles avec des garçons et des filles de différentes tranches d'âge. La communication est un processus bidirectionnel. Aussi, de nombreuses entreprises offrent aux clients la possibilité de les contacter afin de signaler tout problème ou de discuter de leurs préoccupations.

Parce que l'offre de contenus et de services est toujours plus abondante, les utilisateurs gagneront toujours à recevoir de nouveaux conseils et de nouveaux rappels sur la nature des services, et sur la meilleure manière d'en profiter sans danger. S'il est important d'enseigner aux enfants l'utilisation responsable de l'Internet, nous savons que ceux-ci aiment expérimenter, prendre des risques, qu'ils sont intrinsèquement curieux et ne prennent pas toujours les meilleures décisions. Leur donner la possibilité de se forger leurs propres expériences contribue à leur croissance et constitue un moyen sain de les aider à développer leur autonomie et leur résilience, tant que le retour de flamme n'est pas trop brutal. Bien que les enfants doivent être autorisés à prendre des risques en ligne, il est essentiel que les parents et les entreprises puissent les soutenir lorsque les choses tournent mal, compensant ainsi l'impact négatif d'une expérience inconfortable en vue d'en tirer une leçon utile pour l'avenir.

Bonne pratique: sensibilisation

NHK Japan mène une campagne de prévention du suicide chez les jeunes sur Twitter: au Japon, le nombre de suicides chez les adolescents explose lorsqu'ils retournent à l'école après des vacances d'été. Le retour à la réalité serait la raison de ce pic. L'équipe de production NHK Heart Net TV (NHK Japan) produit une émission multimédia intitulée #On the Night of August 31st. Reliant la télévision, la diffusion en direct et les réseaux sociaux, NKH a réussi à créer un "espace" où les adolescents peuvent partager leurs sentiments sans crainte.

Twitter a également publié un guide destiné aux éducateurs sur l'éducation aux médias. Élaboré en partenariat avec l'UNESCO, ce manuel vise principalement à aider les éducateurs à doter les jeunes générations d'une éducation aux médias. Un autre aspect du travail de Twitter en faveur de la sécurité concerne la divulgation de ses opérations d'information. Il s'agit d'une archive des activités d'information soutenues par l'État, que Twitter partage publiquement. L'initiative a été lancée pour permettre aux universitaires et au public de comprendre les campagnes liées à cette question dans le monde et pour permettre l'examen indépendant par des tiers de ces tactiques sur la plate-forme Twitter.

Project deSHAME, cofinancé par Facebook et l'Union européenne, facilite également la création de ressources pour un large éventail de tranches d'âge, en mettant un accent particulier sur les enfants âgés de 9 à 13 ans. Dans le cadre du projet, une boîte à outils intitulée "Step Up, Speak Up!" (Avance-toi, élève la voix!) a été mise en place, fournissant divers supports d'éducation, de formation et de sensibilisation, ainsi que des outils pratiques pour les stratégies de prévention et d'intervention multisectorielles. Le projet transférera ce matériel pédagogique à d'autres pays européens et partenaires du monde entier afin de promouvoir les droits numériques des jeunes.

Google a élaboré une gamme d'initiatives, de ressources et d'outils éducatifs pour aider à promouvoir la sécurité en ligne pour les jeunes. L'entreprise a notamment créé la campagne Be Internet Awesome (Sois fantastique sur Internet), autour de la citoyenneté numérique, en collaboration avec des organisations telles que ConnectSafely, le Family Online Safety Institute et l'Internet Keep Safe Coalition. Adressée aux jeunes de 8 à 11 ans, cette campagne propose un jeu en ligne (Interland) qui enseigne les principes fondamentaux de la sécurité numérique et des ressources pour les éducateurs, tels que le Digital Citizenship and Safety Curriculum (programme pour la citoyenneté et la sécurité numériques). Ce document propose des plans de cours pour les cinq domaines thématiques clés de la campagne, dont l'un porte sur la cyberintimidation. En plus de cela, Google a créé une formation en ligne sur la citoyenneté et la sécurité numériques pour les éducateurs d'élèves de tous âges. Cette formation fournit un soutien supplémentaire pour l'intégration de la citoyenneté numérique et des activités portant sur la sécurité en classe. Google propose également plusieurs programmes pour aider à impliquer directement les jeunes dans les efforts de sécurité en ligne et de citoyenneté numérique. L'initiative mondiale Web Rangers en fait partie. Ce programme encourage aussi les jeunes à concevoir leurs propres campagnes autour d'une utilisation positive et sûre de l'Internet. Il existe également des programmes spécifiques par pays, tels que les programmes Internet Citizens et Internet Legends au Royaume-Uni, eux aussi lancés par Google.

Lors de l'**Échange d'actualités pour les jeunes de l'Eurovision**, l'Union européenne de radio-télévision rassemble 15 télédiffuseurs européens afin de partager des programmes, des formats et des solutions en ligne comme hors ligne. Au cours des dernières années, l'enseignement de la culture numérique et la sensibilisation des enfants aux risques sur Internet sont devenus des éléments fondamentaux de leurs programmes. Parmi les initiatives les plus réussies de ces dernières années figurent les publicités sur les réseaux sociaux et les programmes d'information adaptés aux enfants, produits par Super et Ultra nytt sous NRK, le diffuseur public norvégien.

Bonne pratique: partenariats stratégiques

Dans le cadre d'un projet soutenu par le Fonds pour l'élimination de la violence envers les enfants, Capital Humano y Social Alternativo a conclu en 2018 un partenariat avec Telefónica, le premier fournisseur de services Internet, de transmission de données par câble et de téléphonie au Pérou (14,4 millions de clients, dont plus de 8 millions d'utilisateurs mobiles Movistar).

Plusieurs activités ont été menées dans le cadre de ce partenariat fructueux:

- **Un cours virtuel sur la protection des enfants en ligne** a été mis au point par Telefónica avec le soutien technique de Capital Humano y Social Alternativo. Ce cours est désormais librement accessible sur le site web de Telefónica et l'entreprise suit le nombre de personnes qui s'inscrivent et réussissent le cours. Le Ministère péruvien de l'éducation a accepté de fournir un accès à ce cours virtuel sur son site officiel.
- **Une brochure sur la sécurité sur Internet** a été créée par Capital Humano y Social Alternativo et distribuée par Telefónica dans ses plus de 300 centres de vente mobile. L'objectif est de sensibiliser les clients de Telefónica à la sécurité en ligne et aux risques associés à l'exploitation et aux abus sexuels à l'encontre des enfants en ligne.
- **Un jeu interactif sur l'exploitation et les abus sexuels à l'encontre des enfants en ligne** a été créé par Telefónica avec le soutien technique de Capital Humano y Social Alternativo. Les clients de l'opérateur peuvent y jouer en attendant leur tour dans les magasins Telefónica.

Capitalisant sur le succès de sa collaboration avec Telefónica, Capital Humano y Social Alternativo s'est associé à **Econocable**, un fournisseur de services Internet et câblés qui travaille dans les zones reculées et à faible revenu du Pérou.

3.5 Promouvoir les technologies numériques en tant que moyen de renforcer l'engagement civique

Selon l'Article 13 de la Convention des Nations Unies relative aux droits de l'enfant, "L'enfant a droit à la liberté d'expression. Ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen du choix de l'enfant". Pour s'acquitter de leur devoir de respect des droits civils et politiques des enfants et des jeunes, les entreprises peuvent veiller à ce que la technologie ainsi que l'application de la législation et des politiques conçues pour protéger les enfants et les jeunes contre tout préjudice en ligne n'entraînent pas de conséquences inattendues, telles que la suppression de leur droit à la participation et à l'expression, ou l'interdiction d'accéder à des informations importantes pour leur bien-être. Il est essentiel de veiller à ce que les systèmes de vérification de l'âge ne compromettent pas le besoin réel d'accéder à un contenu pertinent pour le développement de tranches d'âge spécifiques.

Dans le même temps, les entreprises et les secteurs pertinents peuvent également soutenir les droits des enfants et des jeunes en fournissant des systèmes et des outils facilitant leur participation. Ces acteurs peuvent mettre l'accent sur la capacité de l'Internet à favoriser une participation positive à une vie civique plus large, à stimuler le progrès social et à influer sur

la durabilité et la résilience des communautés, par exemple à travers des campagnes sociales et environnementales et en faisant en sorte que les responsables soient tenus de rendre des comptes. Avec les outils et les informations appropriés, les enfants et les jeunes sont mieux à même d'accéder aux soins de santé, à l'éducation et à l'emploi. Ils sont également capables d'exprimer leurs opinions et leurs besoins dans le cadre scolaire, communautaire et national. Ils ont la possibilité d'accéder à des informations sur leurs droits et de se renseigner sur des questions qui les concernent personnellement, telles que leur santé sexuelle, ainsi que sur la responsabilité politique et gouvernementale.

Les entreprises peuvent également investir dans la création d'interfaces en ligne adaptées aux enfants, aux jeunes et aux familles. Elles peuvent soutenir la création de technologies et de contenus qui encouragent les enfants et les jeunes à apprendre, à innover et à créer des solutions, et qui leur permettent d'y parvenir. Les entreprises doivent toujours tenir compte de la sécurité dès la conception de leurs produits.

Par ailleurs, elles peuvent soutenir de manière proactive les droits des enfants et des jeunes en s'efforçant de réduire la fracture numérique. La participation des enfants et des jeunes nécessite une certaine culture numérique, c'est-à-dire la capacité de comprendre et d'interagir dans le monde virtuel. Les citoyens dénués de cette aptitude sont tenus à l'écart de nombreuses fonctions sociales qui ont été numérisées, comme la déclaration d'impôts, le soutien aux candidats politiques, la signature de pétitions en ligne, l'enregistrement d'une naissance ou tout simplement l'accès à des informations commerciales, sanitaires, éducatives ou culturelles. Sans action, le fossé entre les citoyens qui ont accès à ces forums et ceux qui ne l'ont pas, en raison d'un manque d'accès à l'Internet ou de culture numérique, continuera de se creuser, au grand détriment de ces derniers. Les entreprises peuvent soutenir des initiatives multimédias pour contribuer au développement des compétences numériques dont les enfants et les jeunes ont besoin pour être des citoyens confiants, connectés et activement impliqués[17]. Dans de nombreux pays, les services publics s'investissent depuis quelques années d'une mission d'éducation au numérique et aux médias, en vue de réduire la fracture numérique. Le Parlement italien, par exemple, a proposé que le diffuseur national cible en priorité la réduction de la fracture numérique et la protection des enfants hors ligne et en ligne, un exemple qui pourrait être suivi par d'autres pays.

[17] Pour découvrir des exemples de participation des jeunes de la communauté mobile, cliquez ici.

Bonne pratique: collaboration interorganisations

Récemment, Microsoft a rejoint la campagne mondiale Power of ZERO, dirigée par l'organisation No Bully. Cette campagne vise à enseigner aux jeunes enfants et aux adultes qui s'en occupent à bien utiliser la technologie numérique et à encourager la prise de parole, la compassion et l'inclusivité, des valeurs qui sont au cœur de la citoyenneté numérique. L'initiative offre aux éducateurs de la petite enfance (la campagne cible les enfants de 8 ans et moins) et aux familles des supports pédagogiques gratuits pour poser des bases solides dès la petite enfance et aider les jeunes enfants à cultiver les "12 pouvoirs pour le bien", à savoir les 12 compétences de vie ou "pouvoirs" définis par Power of Zero comme permettant aux enfants de naviguer en toute quiétude dans le monde virtuel aussi bien que dans le monde réel. On y retrouve, entre autres, la résilience, le respect, l'inclusivité et la créativité.

4 Directives générales à l'intention des professionnels

Le Tableau 1 présente les grandes lignes à suivre par les professionnels pour repérer, prévenir et atténuer tout impact négatif de leurs produits et services sur les droits des enfants et des jeunes, et pour promouvoir une utilisation positive des TIC par ces derniers.

Il convient de noter que toutes les étapes répertoriées dans le Tableau 1 ne conviendront pas à toutes les sociétés et services; de même, toutes les étapes nécessaires pour chaque service ne figurent pas dans ce tableau. Les directives générales à l'intention des professionnels sont complétées par les listes de contrôle spécifiques par fonctionnalité (voir Section 5) et vice versa. Les listes de contrôle spécifiques par fonctionnalité des Tableaux 2 à 5 mettent en évidence les étapes supplémentaires les plus pertinentes pour des services particuliers. Notez que ces listes de contrôle peuvent se chevaucher et que plusieurs listes de contrôle peuvent être pertinentes pour le même service.

Tableau 1: Directives générales à l'intention des professionnels

Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés	Les professionnels du secteur peuvent repérer, prévenir et atténuer les effets néfastes des TIC sur les droits des enfants et des jeunes, et explorer les voies possibles en matière de promotion de ces droits en prenant les mesures suivantes:
	Veiller à ce qu'une personne et/ou une équipe spécifique soient désignées comme responsables de ce processus et puissent entrer en contact avec les parties prenantes internes et externes nécessaires. Autoriser cette personne ou cette équipe à prendre l'initiative de faire de la protection des enfants en ligne une priorité dans l'ensemble de l'entreprise.
	Élaborer une politique de protection et de défense des enfants et/ou intégrer les risques et opportunités spécifiques aux droits des enfants et des jeunes dans les engagements stratégiques globaux de l'entreprise (par exemple, en matière de droits de l'homme, de confidentialité, de marketing ou dans les codes de conduite pertinents).
	Intégrer le principe de diligence raisonnable concernant les questions de protection des enfants en ligne dans les cadres existants relatifs aux droits de l'homme ou à l'évaluation des risques (au niveau de l'entreprise, du produit, de la technologie et/ou du pays), afin de déterminer si l'entreprise ou le secteur peut avoir des effets néfastes ou y contribuer par le biais de ses activités. Cela permet aussi de savoir si des effets néfastes peuvent être directement associés aux opérations de l'entreprise, à ses produits, services, ou à ses relations commerciales.
	Mettre en évidence les répercussions possibles sur les droits de l'enfant selon les tranches d'âge découlant des opérations de l'entreprise et de la conception, du développement et de l'introduction de ses produits et services; rechercher des voies possibles de soutien des droits des enfants et des jeunes.

Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés *(suite)*	Adopter une approche de la protection de l'enfance fondée sur l'autonomisation et l'éducation. Tenir compte des droits des enfants en matière de protection des données, de leur droit à la vie privée et à la liberté d'expression, tout en prodiguant une éducation et des conseils par le biais des services de l'entreprise. S'appuyer sur une expertise interne et externe et consulter les principales parties prenantes, y compris les enfants et les jeunes, concernant les mécanismes de protection des enfants en ligne en vue de recevoir des commentaires et des conseils continus sur les méthodes de l'entreprise.
	Dans les États où il n'existe pas de cadres juridiques adéquats pour la protection des droits des enfants et des jeunes à la vie privée et à la liberté d'expression, les entreprises doivent garantir que leurs politiques et pratiques sont conformes aux normes internationales. Voir la Résolution 68/167 de l'Assemblée générale des Nations Unies sur le droit à la vie privée à l'ère du numérique.
	Garantir l'accès à des recours en établissant des systèmes de réclamation et de signalement au niveau opérationnel pour toute violation des droits de l'enfant (comme le matériel montrant des abus sexuels sur des enfants, les contenus ou contacts inappropriés ou les atteintes à la vie privée).
	Nommer un responsable de la politique de protection de l'enfance ou une autre personne désignée qui peut être contactée pour des problèmes liés à la protection des enfants en ligne. Si un enfant est exposé à des risques de préjudice, le responsable de la politique de protection de l'enfance doit immédiatement alerter les autorités compétentes. Les directives éditoriales de la BBC (2019), par exemple, prévoient la nomination d'une personne responsable de la politique de protection de l'enfance, ce qui est considéré comme obligatoire dans les médias de service public.
Élaborer des normes sectorielles afin de protéger les enfants en ligne	Définir et mettre en œuvre des normes pour les entreprises et les secteurs afin de protéger les enfants et les jeunes en fonction du secteur concerné et des caractéristiques spécifiques en jeu.

Établir des processus standard concernant le matériel montrant des abus sexuels sur des enfants	En collaboration avec le gouvernement, les forces de l'ordre, la société civile et les organisations de signalement, le secteur a un rôle clé à jouer dans la lutte contre le matériel montrant des abus sexuels sur des enfants en prenant les mesures suivantes:
	Interdire la mise en ligne, la publication, la transmission, le partage ou la mise à disposition de contenu qui viole les droits d'une partie quelconque ou enfreint toute loi locale, étatique, nationale ou internationale.
	Communiquer avec les autorités répressives ou les plates-formes de signalement nationales afin de dénoncer tout matériel montrant des abus sexuels sur des enfants dès qu'un quelconque matériel de ce type est porté à la connaissance du fournisseur. Veiller à ce que des procédures internes soient en place pour assumer les responsabilités en matière de signalement qui leur incombent en vertu des lois locales et internationales. Lorsqu'une entreprise opère sur des marchés où la bonne application de la réglementation et des lois est moins surveillée, elle peut rediriger ceux qui souhaitent effectuer un signalement vers le réseau INHOPE, où les dépositions peuvent être transmises auprès de n'importe quelle ligne d'assistance internationale. Établir des procédures internes pour garantir le respect des lois locales et internationales sur la lutte contre le matériel montrant des abus sexuels sur des enfants. Mettre en place un poste ou une équipe senior consacré(e) à l'intégration de ces procédures au sein de l'organisation. Les professionnels du secteur doivent ensuite rendre compte des mesures prises et des résultats atteints par cette équipe dans leur rapport annuel d'activité sur le développement durable. Lorsque les réglementations nationales n'offrent pas de protection suffisante, les entreprises doivent assurer une protection supérieure à celle garantie par la législation nationale et utiliser leur influence pour faire pression en faveur de modifications législatives et ainsi permettre au secteur de lutter contre le matériel montrant des abus sexuels sur des enfants. Un poste ou une équipe senior doit être créé(e) au sein de l'organisation aux fins de l'intégration de ces procédures et du suivi des opérations. Ces dernières doivent être consignées de manière transparente dans les rapports annuels d'activité sur le développement durable, et mises à la disposition du public.

Établir des processus standard concernant le matériel montrant des abus sexuels sur des enfants *(suite)*	Préciser qu'en cas de signalement ou de découverte de contenu illégal, l'entreprise coopérera pleinement dans le cadre des enquêtes des forces de l'ordre; spécifier les détails concernant les sanctions prévues le cas échéant (amendes ou annulation des privilèges de facturation).
	Indiquer explicitement aux clients la position de l'entreprise sur l'utilisation abusive de ses services en vue de stocker ou de partager du matériel montrant des abus sexuels sur des enfants dans les conditions générales et/ou les politiques d'utilisation pertinentes, et préciser les conséquences de tout abus.
	Élaborer des processus de notification, de retrait et de signalement permettant aux utilisateurs de signaler tout matériel montrant des abus sexuels sur des enfants ou tout contact inapproprié, ainsi que le profil/l'emplacement spécifique où ledit matériel ou contact a été détecté. Établir des processus de suivi des signalements, convenir de procédures pour recueillir les preuves et supprimer ou bloquer immédiatement l'accès au matériel montrant des abus sexuels sur des enfants. S'assurer que, le cas échéant, les fournisseurs de services demandent l'avis d'experts (par exemple, des organes nationaux de protection des enfants en ligne) avant de détruire les contenus illégaux. Veiller à ce que les tiers concernés avec lesquels l'entreprise entretient une relation contractuelle mettent en place des processus de notification et de retrait tout aussi solides.
	Se tenir prêt à gérer le matériel montrant des abus sexuels sur des enfants et à signaler les cas aux autorités compétentes. Si une relation avec les forces de l'ordre et la plate-forme de signalement nationale n'est pas déjà établie, entrer en contact avec elles pour élaborer ensemble des processus.
	Travailler avec des services internes, tels que le service client, la prévention des fraudes et la sécurité pour garantir que l'entreprise peut effectuer des signalements de contenu illégal suspecté directement aux forces de l'ordre et aux plates-formes spécialisées. Idéalement, cela devrait être fait d'une manière qui n'expose pas le personnel de première ligne à un contenu nuisible et qui ne revictimise pas les enfants et les jeunes touchés. Pour faire face aux situations où le personnel peut être exposé à du matériel abusif, mettre en œuvre une politique ou un programme favorisant la résilience, la sécurité et le bien-être du personnel.

Établir des processus standard concernant le matériel montrant des abus sexuels sur des enfants *(suite)*	Mettre en place des politiques de conservation et de préservation des données pour aider les services de police en cas d'enquête criminelle par le biais d'activités telles que le recueil de preuves. Documenter les pratiques de l'entreprise en matière de gestion du matériel montrant des abus sexuels sur des enfants, en commençant par la surveillance jusqu'au transfert final et à la destruction du matériel. Consigner une liste de tout le personnel responsable de la manipulation du matériel.
	Promouvoir des systèmes de signalement du matériel montrant des abus sexuels sur des enfants et s'assurer que les clients savent comment envoyer un rapport s'ils découvrent un matériel de ce type. Si une plate-forme de signalement nationale existe, fournir des liens vers celle-ci sur le site web de l'entreprise et sur tout service de contenu pertinent mis en avant par cette dernière.
	Recourir à tous les ensembles de services/données pertinents pour empêcher la diffusion de contenus connus montrant des abus sexuels sur des enfants sur les services ou plates-formes de l'entreprise.
	Évaluer régulièrement et activement tous les contenus hébergés sur les serveurs de l'entreprise, y compris les contenus commerciaux (de marque ou contractés auprès de fournisseurs de contenu tiers). Envisager d'utiliser des outils tels que le hachage des images connues montrant des abus sexuels sur des enfants, un logiciel de reconnaissance d'image ou un système de blocage d'URL pour gérer le matériel montrant des abus sexuels sur des enfants.
Créer un environnement en ligne plus sûr et adapté à l'âge	Les professionnels du secteur peuvent contribuer à la création d'un environnement numérique plus sûr et plus agréable pour les enfants et les jeunes de tous âges, en prenant les mesures suivantes:
	Appliquer des principes de sécurité et de confidentialité dès la conception dans les technologies et services de l'entreprise, et accorder la priorité aux solutions qui réduisent au maximum le volume de données relatives aux enfants.
	Proposer des services dont la conception est adaptée à l'âge. Présenter aux enfants des informations concernant les règles du site d'une manière accessible et adaptée à l'âge, en fournissant une quantité appropriée de détails. En plus des conditions générales d'utilisation adaptées à l'âge et accessibles, les professionnels doivent également communiquer clairement des informations telles que les principales règles et politiques. Ces informations doivent mettre l'accent sur les comportements acceptables et inacceptables sur le service, sur les conséquences de toute violation des règles, sur les spécificités du service et sur ce à quoi l'utilisateur consent en s'inscrivant. Ces informations doivent être particulièrement destinées aux jeunes utilisateurs et à leurs parents et tuteurs.
	Rédiger des conditions d'utilisation ou des conditions générales pour attirer l'attention des utilisateurs sur le contenu des services en ligne de l'entreprise susceptible de ne pas convenir à tous les âges. Les conditions d'utilisation doivent également inclure des mécanismes clairs permettant de signaler et de traiter les infractions à ces règles.

Créer un environnement en ligne plus sûr et adapté à l'âge ***(suite)***	Envisager de fournir des systèmes tels qu'un logiciel de contrôle parental et d'autres outils permettant aux parents et aux personnes s'occupant d'enfants de gérer l'accès de leurs enfants aux ressources Internet, tout en leur fournissant des conseils sur leur utilisation appropriée afin que les droits des enfants ne soient pas violés. Il s'agit notamment de listes de blocage/d'autorisation, de filtres de contenu, de surveillance de l'utilisation, de gestion des contacts et de limites de temps/programmes.
	Proposer des options de contrôle parental faciles à utiliser qui permettent aux parents et aux personnes s'occupant d'enfants de restreindre certains services et contenus auxquels les enfants peuvent accéder lorsqu'ils utilisent des appareils électroniques. Ces restrictions peuvent prendre la forme de contrôles au niveau du réseau et du périphérique ou de contrôles d'application. Étant donné que ces contrôles ont une incidence considérable sur la capacité de l'enfant à faire progresser ses compétences numériques et qu'ils affectent ses possibilités en ligne, ils devraient être conçus pour les très jeunes enfants en fonction de leur contexte de développement et être accompagnés d'orientations pertinentes pour les parents.
	Dans la mesure du possible, promouvoir les services d'assistance au niveau national afin de permettre aux parents et aux personnes s'occupant d'enfants de signaler toute infraction et d'obtenir de l'aide pour signaler les cas d'abus sur mineurs ou d'exploitation.
	Éviter les contenus publicitaires nuisibles ou inappropriés en ligne et établir des obligations en matière de communication de l'information à la clientèle pour les fournisseurs de services dont le contenu est destiné à un public adulte et pourrait être nuisible pour les enfants et les jeunes. La publicité nuisible peut également inclure les annonces pour des aliments et des boissons riches en matières grasses, en sucre ou en sel. Aligner les pratiques commerciales avec les réglementations et les conseils en matière de marketing et de publicité destinés aux enfants et aux jeunes. Surveiller où, quand et comment les enfants et les jeunes peuvent être confrontés à des messages publicitaires potentiellement nuisibles destinés à un autre segment du marché.
	Veiller à ce que les politiques de collecte de données soient conformes aux lois applicables concernant la vie privée des enfants et des jeunes, notamment en examinant si le consentement des parents est requis avant que les entreprises commerciales ne puissent collecter des informations personnelles à propos d'un enfant.
	Adapter et appliquer des paramètres de confidentialité par défaut renforcés pour la collecte, le traitement, le stockage, la vente et la publication de données personnelles, notamment les informations liées à la localisation et les habitudes de navigation recueillies auprès de personnes de moins de 18 ans. Les paramètres de confidentialité par défaut et les informations sur l'importance de la confidentialité doivent être adaptés à l'âge des utilisateurs et à la nature du service.

Créer un environnement en ligne plus sûr et adapté à l'âge *(suite)*	Empêcher l'accès et l'exposition des mineurs à des contenus ou services inappropriés à l'aide de moyens techniques, tels que des outils de contrôle parental appropriés, la sécurité dès la conception, les expériences différenciées selon l'âge, le contenu protégé par mot de passe, les listes de blocage/d'autorisation, le contrôle des achats/du temps d'utilisation, les fonctions de désabonnement, le filtrage et la modération. Mettre en œuvre une technologie permettant de connaître l'âge des utilisateurs et de leur présenter une version de l'application adaptée en conséquence. En ce qui concerne les contenus ou services réservés à un public d'un certain âge, les parties prenantes du secteur doivent prendre des mesures pour vérifier l'âge des utilisateurs. Dans la mesure du possible, vérifier l'âge pour limiter l'accès aux contenus ou aux matériels qui, selon la loi ou le cadre réglementaire, sont destinés uniquement aux personnes au-dessus d'un certain âge. Les entreprises doivent également reconnaître le risque d'utilisation à mauvais escient de ces technologies en vue de restreindre le droit des enfants et des jeunes à la liberté d'expression et à l'accès à l'information, ou en vue de menacer leur vie privée. Garantir que tout contenu ou service qui ne conviennent pas aux utilisateurs de tous âges sont: • classés conformément aux normes nationales et culturelles; • conformes aux normes existantes dans les médias équivalents; • mis en évidence par des options d'affichage évidentes afin d'en contrôler l'accès; • proposés avec une fonctionnalité de vérification de l'âge dans la mesure du possible (le cas échéant), et accompagnés de conditions claires concernant l'effacement de toutes les données personnelles identifiables obtenues via le processus de vérification. Par exemple, en ce qui concerne les normes relatives aux médias, toutes les autorités de réglementation des médias fournissent un ensemble d'exigences pour le contenu réservé à un certain âge, et les fournisseurs Internet sont tenus d'adapter les référentiels et d'appliquer ces lignes directrices à leur offre de contenu. Voir l'Ofcom au Royaume-Uni, le CSA en France et l'AGCOM en Italie
	Offrir des outils de signalement clairs, élaborer un processus de suivi des signalements de contenus ou de contacts inappropriés et d'abus, et fournir des commentaires détaillés aux utilisateurs du service sur le processus de signalement.
	Assurer la modération préalable des espaces interactifs conçus pour les enfants et les jeunes en respectant les capacités évolutives des enfants ainsi que leur droit à la vie privée. Une modération active peut favoriser une atmosphère où l'intimidation et le harcèlement ne sont pas acceptables. Exemples de comportements inacceptables: • publication de commentaires désagréables ou menaçants sur le profil d'autrui; • création de faux profils ou de sites haineux en vue d'humilier une victime; • envoi de messages en chaîne et de pièces jointes avec l'intention de nuire; • piratage du compte d'un utilisateur pour envoyer des messages offensants à d'autres personnes.

Créer un environnement en ligne plus sûr et adapté à l'âge ***(suite)***	Prendre des précautions particulières avec les membres du personnel ou les collaborateurs qui travaillent avec des enfants et des jeunes, pour lesquels une vérification préliminaire du casier judiciaire auprès des autorités de police peut être requise.
	Signaler rapidement tout incident de pédopiégeage soupçonné à l'équipe de direction en ligne ou interactive chargée de le signaler aux autorités compétentes en: • signalant tout cas à la haute direction et à un responsable de la politique de protection de l'enfance désigné, dans la mesure du possible; • permettant aux utilisateurs de signaler les incidents soupçonnés directement aux autorités; • rendant possible un contact direct via des adresses e-mail à des fins de signalement et d'élaboration de rapports.
	Accorder la priorité à la sécurité et au bien-être de l'enfant à tout moment. Toujours faire preuve de professionnalisme et s'assurer que tout contact avec les enfants est essentiel au service, au programme, à l'événement, à l'activité ou au projet. Ne prendre en aucun cas l'entière responsabilité d'un enfant. Si un enfant a besoin de soins, prévenir le parent, le tuteur ou l'accompagnateur. Écouter et respecter les enfants en tout temps. Si une personne se comporte de manière inappropriée vis-à-vis des enfants, signaler le comportement au contact local chargé de la protection de l'enfance.
	Établir un ensemble clair de règles bien mises en évidence et faire écho aux points clés mentionnés dans les conditions de service et les directives d'utilisation pertinentes. Ces règles doivent définir les éléments suivants, dans un langage convivial: • la nature du service et les attentes vis-à-vis de ses utilisateurs; • les contenus, comportements et le langage acceptables ou non, ainsi que l'interdiction de toute utilisation illégale; • les conséquences proportionnelles à toute violation, par exemple, le signalement aux forces de l'ordre ou la suspension du compte de l'utilisateur.
	Donner la possibilité aux clients de signaler facilement au service clientèle leurs préoccupations relatives à une utilisation abusive, grâce à des processus standard et accessibles permettant de faire face à différentes préoccupations, telles que la réception de communications indésirables (par exemple, les spams SMS).
	Être transparent et fournir aux clients des informations claires sur la nature des services proposés, par exemple: • le type de contenu/service et les tarifs; • l'âge minimum requis pour accéder au service; • la disponibilité de contrôles parentaux, ce qu'ils couvrent (par exemple, le réseau) ou ne couvrent pas (par exemple, le WiFi) et une formation sur leur utilisation; • le type d'informations collectées sur les utilisateurs et comment ces informations sont utilisées.
	Promouvoir des services de soutien nationaux qui permettent aux enfants et aux jeunes de signaler et de demander de l'aide en cas de maltraitance ou d'exploitation (par exemple, Child Helpline International).

Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC	L'industrie peut compléter les moyens techniques par des activités d'éducation et d'autonomisation en prenant les mesures suivantes:
	Décrire clairement le contenu disponible et les contrôles parentaux ou les paramètres de sécurité familiale correspondants. Rendre le langage et la terminologie accessibles, visibles, clairs et pertinents pour tous les utilisateurs, y compris les enfants, les parents et les personnes s'occupant d'enfants, en particulier en ce qui concerne les conditions générales d'utilisation, les coûts liés à l'utilisation d'un contenu ou de services, les politiques de confidentialité, les informations de sécurité et les mécanismes de signalement.
	Éduquer les clients sur la façon de gérer les préoccupations liées à l'utilisation de l'Internet, comme les spams, le vol de données et les contacts inappropriés tels que l'intimidation et le pédopiégeage; décrire les mesures que les clients peuvent prendre et la marche à suivre pour exprimer leurs préoccupations concernant une utilisation inappropriée.
	Mettre en place des mécanismes et éduquer les parents à s'impliquer dans les activités liées aux TIC de leurs enfants et adolescents, en particulier s'agissant de jeunes enfants, en permettant aux parents d'examiner les paramètres de confidentialité des enfants et des jeunes, par exemple.
	Collaborer avec le gouvernement et les éducateurs pour renforcer les capacités des parents à aider et à inviter leurs enfants et jeunes à être des citoyens numériques et des utilisateurs des TIC responsables.
	En fonction du contexte local, fournir du matériel pédagogique à utiliser dans les écoles et les foyers pour améliorer l'utilisation des TIC par les enfants et les jeunes et les encourager à développer une pensée critique pour leur permettre de se comporter de manière sûre et responsable lorsqu'ils utilisent des services TIC.
	Soutenir les clients en diffusant des directives sur la sécurité de la famille en ligne qui encouragent les parents et les personnes s'occupant d'enfants à: • se familiariser avec les produits et services utilisés par les enfants et les jeunes; • s'assurer d'une utilisation modérée des appareils électroniques par les enfants et les jeunes dans le cadre d'un mode de vie sain et équilibré; • porter une attention particulière au comportement des enfants et des jeunes afin de pouvoir déceler tout changement qui pourrait indiquer un cas de cyberintimidation ou de harcèlement.
	Fournir aux parents les informations nécessaires pour leur permettre de comprendre comment leurs enfants et jeunes utilisent les services TIC, de gérer les problèmes liés aux contenus et comportements préjudiciables et d'avoir toutes les clés en main pour guider les enfants et les jeunes dans une utilisation responsable. Pour faciliter cette tâche, les professionnels peuvent employer des outils et collaborer avec les académies scolaires en vue de créer des programmes sur la sécurité en ligne pour les enfants et du matériel pédagogique pour les parents.

Protéger et éduquer les enfants grâce aux avancées technologiques	Les technologies d'IA (qui comprennent les textes, les images, les conversations et les contextes) qui préservent la confidentialité sont capables de détecter et de s'attaquer à divers dangers et menaces en ligne, et d'utiliser ces informations pour responsabiliser et éduquer les enfants lorsqu'ils y sont confrontés. Lorsqu'elles sont utilisées avec des appareils intelligents, elles peuvent protéger les données et la confidentialité des jeunes tout en leur apportant une certaine aide.
	Les médias nationaux et de service public peuvent jouer un rôle essentiel à travers leurs offres de programmes (hors et en ligne) pour éduquer les parents et les enfants et les sensibiliser aux risques et aux possibilités que présente le monde en ligne.
Promouvoir la technologie numérique en tant que moyen de favoriser l'engagement civique	Le secteur peut encourager et autonomiser les enfants et les jeunes en soutenant leur droit à la participation grâce aux actions suivantes:
	Fournir des informations sur un service pour mettre en évidence les avantages que les enfants obtiennent en se comportant convenablement et de manière responsable, comme l'utilisation du service à des fins créatives.
	Établir des procédures écrites qui garantissent une mise en œuvre cohérente des politiques et des processus protégeant la liberté d'expression pour tous les utilisateurs, y compris les enfants et les jeunes, ainsi que la documentation relative au respect de ces politiques.
	Éviter le blocage excessif de contenus légitimes et adaptés au développement. Afin de garantir que les demandes et les outils de filtrage ne sont pas utilisés à mauvais escient pour restreindre l'accès des enfants et des jeunes aux informations, garantir la transparence concernant les contenus bloqués et établir un processus permettant aux utilisateurs de signaler tout blocage par inadvertance. Ce processus doit être accessible à tous les clients, y compris les administrateurs web. Tout processus de signalement doit fournir des conditions de service claires, responsables et tranchées.
	Créer des plates-formes en ligne qui promeuvent le droit des enfants et des jeunes à s'exprimer; faciliter leur participation à la vie publique et encourager leur collaboration, leur esprit d'entreprise et leur participation civique.
	Soutenir l'élaboration de contenus pédagogiques pour les enfants et les jeunes qui encouragent l'apprentissage, la pensée créative et la résolution de problèmes.
	Promouvoir la culture numérique, le renforcement des capacités et les compétences en TIC pour donner les moyens aux enfants et aux jeunes, en particulier ceux des zones rurales et mal desservies, d'utiliser les ressources TIC et de participer pleinement et en toute sécurité au monde numérique.
	Collaborer avec la société civile et les autorités locales sur les priorités nationales et locales en vue de l'accès universel et équitable aux TIC, aux plates-formes et aux appareils, et œuvrer au renforcement des infrastructures sous-jacentes pour les soutenir.

Promouvoir la technologie numérique en tant que moyen de favoriser l'engagement civique *(suite)*	Informer les clients et dialoguer avec eux, y compris les parents, les personnes s'occupant d'enfants, les enfants et les jeunes, sur les services proposés, par exemple: • le type de contenu et les contrôles parentaux correspondants; • les mécanismes de signalement des cas d'abus, d'utilisation abusive et des contenus inappropriés ou illégaux; • les procédures de suivi des signalements; • les types de services faisant l'objet d'une restriction d'âge; • l'utilisation sûre et responsable des services interactifs sous "marque propre".
	S'engager sur des questions plus larges liées à la citoyenneté numérique sûre et responsable, par exemple la réputation en ligne, l'empreinte numérique, les contenus nuisibles ou le pédopiégeage. Envisager de s'associer à des experts locaux, tels que des organisations non gouvernementales défendant la cause des enfants, des associations caritatives et des groupes de parents, afin de contribuer à façonner le message de l'entreprise et de toucher le public ciblé.
	Si l'entreprise travaille déjà avec des enfants ou des écoles, par exemple par le biais de programmes de responsabilité sociale des entreprises, étudier la possibilité d'étendre cet engagement pour inclure l'éducation et la participation des enfants, des jeunes et des **éducateurs** concernant les messages de la protection des enfants en ligne.
Investir dans la recherche	Investir dans la recherche factuelle et l'analyse approfondie concernant les technologies numériques, l'impact des technologies sur les enfants, la protection des enfants et les considérations relatives aux droits de l'enfant s'agissant de l'environnement numérique, afin d'intégrer les systèmes de protection en ligne dans les services utilisés par les enfants et les jeunes et de mieux comprendre quels types d'interventions sont les plus efficaces pour améliorer l'expérience en ligne des enfants.

Typologie des entreprises TIC

Bien que ces lignes directrices de l'UIT visent l'ensemble du secteur des TIC, il est important de reconnaître que les services proposés par les entreprises de TIC, les modes de fonctionnement de ces dernières, les régimes réglementaires sous lesquels elles fonctionnent, ainsi que la portée et l'échelle de leurs offres sont très différents. Toute entreprise technologique dont les produits et services ciblent directement ou indirectement les enfants peut tirer parti des principes généraux exposés précédemment, et s'adapter en fonction de son domaine d'activité spécifique. L'idée centrale est de soutenir et guider les professionnels des TIC dans la prise de mesures appropriées, en vue de mieux protéger les enfants en ligne contre les risques de préjudices tout en leur donnant les moyens d'optimiser leur navigation dans le monde virtuel. La typologie ci-dessous facilitera la compréhension de certaines des audiences cibles et de leur place dans les listes de contrôle fournies à la section suivante. Il convient de noter qu'il ne s'agit que de quelques exemples de catégories spécifiques et que cette liste n'est pas exhaustive:

a) Fournisseurs de services Internet, y compris par le biais de services fixes à large bande ou de services de données cellulaires des opérateurs de réseaux mobiles. Bien que cette catégorie concerne généralement les services offerts à plus long terme aux clients abonnés, elle pourrait également être étendue aux entreprises fournissant des hotspots WiFi publics gratuits ou payants.

b) Réseaux sociaux/plates-formes de messagerie et plates-formes de jeux en ligne.

c) Fabricants de matériel et de logiciels, tels que les fournisseurs d'appareils portables, y compris les téléphones mobiles, les consoles de jeux, les appareils domestiques à assistance vocale, l'Internet des objets et les jouets pour enfants intelligents connectés à l'Internet.
d) Entreprises fournissant des médias numériques (créateurs de contenu, fournisseurs d'accès à des contenus ou hébergeurs de contenu).
e) Entreprises fournissant des services de diffusion en continu (streaming), y compris des flux en direct.
f) Entreprises proposant des services de stockage de fichiers numériques, fournisseurs de services en nuage.

5 Listes de contrôle spécifiques par fonctionnalité

Cette section complète la liste de contrôle générale précédente destinée aux professionnels. Elle propose ainsi des recommandations aux entreprises qui fournissent des services incluant des fonctionnalités spécifiques sur le respect et le soutien des droits des enfants en ligne. Des listes récapitulatives spécifiques par fonctionnalité y présentent des moyens de compléter les principes et approches communs donnés dans le Tableau 1. En effet, elles s'appliquent à différents services et doivent donc être envisagées en plus des mesures suggérées dans ledit tableau.

Les fonctionnalités mises en évidence ici sont transversales, si bien que plusieurs de ces listes peuvent être pertinentes pour une même entreprise.

Les listes de contrôle par fonctionnalité suivantes renvoient aux mêmes domaines clés que les directives générales du Tableau 1, et sont organisées de la même façon. Chacune de ces listes a été élaborée en collaboration avec des contributeurs clés et, par conséquent, présente des variations mineures.

5.1 Fonctionnalité A: fournir des services de connectivité, de stockage de données et d'hébergement

L'accès à l'Internet est fondamental pour la réalisation des droits des enfants, et ces derniers peuvent accéder à de nouveaux mondes grâce à la connectivité. Les fournisseurs de services de connectivité, de stockage de données et d'hébergement ont d'immenses possibilités pour intégrer la sécurité et la confidentialité dans leurs offres pour les enfants et les jeunes. Cette fonctionnalité s'adresse, entre autres, aux opérateurs mobiles, aux fournisseurs d'accès Internet, aux systèmes de stockage de données et aux services d'hébergement.

Les opérateurs mobiles permettent d'accéder à Internet et proposent divers services de données spécifiques aux mobiles. De nombreux opérateurs ont déjà signé les codes de bonnes pratiques en matière de protection des enfants en ligne et proposent divers outils et ressources d'information pour honorer leurs engagements.

La plupart des fournisseurs de services Internet agissent aussi bien en tant que vecteurs, octroyant un accès vers et depuis Internet, que comme référentiels de données, grâce à leurs services d'hébergement, de mise en cache et de stockage. C'est pourquoi ils ont la responsabilité principale de protéger les enfants en ligne.

Accès Internet dans les espaces publics

Fournir un accès Internet via des points d'accès WiFi devient une pratique de plus en plus courante pour les municipalités, les commerçants, les sociétés de transport, les chaînes hôtelières ou d'autres entreprises et organisations. Cet accès est généralement gratuit ou fourni à un coût minime. Il implique parfois des formalités d'inscription minimales lorsqu'il s'agit d'un service public ou d'une entreprise souhaitant attirer des clients dans ses locaux ou persuader davantage de personnes d'utiliser ses services.

La promotion du WiFi est un moyen efficace d'assurer la disponibilité de l'Internet dans une zone donnée. Des précautions doivent cependant être prises lorsqu'un tel accès est fourni dans des espaces publics où des enfants sont susceptibles de se rendre régulièrement. Les utilisateurs doivent être conscients du fait que les signaux WiFi peuvent être accessibles aux passants et que leurs données sont susceptibles d'être compromises. Le fournisseur de WiFi ne sera donc pas en mesure de soutenir ou de superviser à tout moment l'utilisation d'une connexion Internet qu'il a fournie. Ainsi, les utilisateurs doivent veiller à ne pas partager d'informations sensibles sur le WiFi accessible au public.

Dans les espaces publics, les fournisseurs de WiFi peuvent envisager des mesures supplémentaires pour protéger les enfants et les jeunes, telles que:

- Le blocage proactif de l'accès aux adresses web connues pour comporter des contenus inappropriés pour un large public, en plus du blocage de l'accès à du matériel montrant des abus sexuels sur des enfants.
- L'inclusion dans les conditions générales d'utilisation de clauses qui interdisent l'utilisation des services WiFi pour consulter ou afficher des contenus susceptibles de ne pas convenir à un environnement où des enfants sont présents. Les conditions générales d'utilisation doivent également inclure des mécanismes clairs concernant les conséquences en cas de violation de ces règles.
- L'adoption de toutes les mesures nécessaires pour se protéger contre les accès non autorisés, qui pourraient entraîner une manipulation ou une perte de données personnelles.
- L'installation de filtres sur le système WiFi afin de mieux appliquer la politique sur le matériel inapproprié.
- La fourniture de procédures et de logiciels permettant de signaler toute infraction et offrant la possibilité d'un contrôle parental concernant l'accès des enfants et des jeunes aux contenus Internet.

Bonne pratique: la réglementation des télécommunications de la plupart des États membres de l'Union européenne, par exemple, stipule que l'accès au réseau doit être identifié au moyen d'outils tels que des cartes SIM individuelles.

Le Tableau 2 peut orienter les fournisseurs de services de connectivité, de stockage de données et d'hébergement concernant les mesures qu'ils peuvent prendre pour améliorer la protection des enfants en ligne et leur participation.

Tableau 2: Liste de contrôle aux fins de la protection des enfants en ligne pour la fonctionnalité A: fournir des services de connectivité, de stockage de données et d'hébergement

Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés	Les fournisseurs de services de connectivité, de stockage de données et d'hébergement peuvent repérer, prévenir et atténuer les effets néfastes des TIC sur les droits des enfants et des jeunes, et explorer les voies possibles en matière de promotion de ces droits.
	Veuillez-vous référer aux directives générales du Tableau 1.
Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants	En collaboration avec le gouvernement, les forces de l'ordre, la société civile et les organisations de signalement, les fournisseurs de services de connectivité, de stockage de données et d'hébergement peuvent jouer un rôle clé dans la lutte contre le matériel montrant des abus sexuels sur des enfants en prenant les mesures suivantes:
	Collaborer avec le gouvernement, les forces de l'ordre, la société civile et les plates-formes de signalement pour gérer efficacement le matériel montrant des abus sexuels sur des enfants et signaler les cas aux autorités compétentes. Si une relation avec les forces de l'ordre et une plate-forme de signalement n'est pas déjà établie, entrer en contact avec elles pour élaborer ensemble des processus. Les fournisseurs de services de connectivité, de stockage de données ou d'hébergement peuvent également fournir une formation aux TIC destinée aux forces de l'ordre. Si une entreprise opère sur des marchés où bonne application de la réglementation et des lois est moins surveillée, elle peut rediriger ceux qui souhaitent effectuer un signalement vers le réseau INHOPE, où les dépositions peuvent être transmises auprès de n'importe quelle ligne d'assistance internationale.
	Envisager de déployer des listes de blocage d'URL ou de sites web internationalement reconnues et créées par les autorités compétentes (par exemple, l'autorité nationale d'application de la loi ou la plate-forme de signalement nationale, Cyberaide Canada, Interpol, l'IWF), pour rendre plus difficile l'accès des utilisateurs au matériel montrant des abus sexuels sur des enfants établi.
	Élaborer des processus de notification, de retrait et de signalement; lier les dénonciations d'abus à ces processus au moyen d'une convention de service public sur la procédure d'intervention et les délais de retrait. Voir, par exemple, le Guide de l'UNICEF et de la GSMA sur les politiques et pratiques de notification et de retrait.
	Mettre en place un mécanisme de signalement accompagné d'informations claires sur son utilisation, qui indiquent par exemple quels contenus et comportements illégaux signaler; précisent les éléments qui ne peuvent pas être joints au rapport afin d'éviter toute diffusion ultérieure sur le web.

Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants ***(suite)***	Aider les services de police en cas d'enquête criminelle par le biais d'activités telles que le recueil de preuves. Énoncer dans les conditions d'utilisation l'interdiction spécifique d'utiliser les services en vue de stocker, de partager ou de diffuser du matériel montrant des abus sexuels sur des enfants. S'assurer que ces conditions indiquent clairement que le matériel montrant des abus sexuels sur des enfants ne sera pas toléré. Veiller à ce que les conditions d'utilisation stipulent que l'entreprise coopérera pleinement avec les autorités dans le cadre d'enquêtes policières en cas de découverte ou de signalement de matériel montrant des abus sexuels sur des enfants.
	Il existe actuellement deux méthodes de signalement du matériel montrant des abus sexuels sur des enfants en ligne au niveau national: les numéros d'écoute et les portails de signalement. Une liste complète et à jour de l'ensemble des plates-formes existantes est disponible sur INHOPE. Numéros d'écoute: si aucun numéro d'écoute n'est disponible au niveau national, étudier les possibilités d'en créer une (voir le guide élaboré par la GSMA et INHOPE sur les plates-formes de signalement pour découvrir quelques options, comme la collaboration avec INHOPE et la Fondation INHOPE. Une version interactive du guide d'INHOPE et de GSMA est disponible. Elle fournit des conseils sur l'élaboration de processus internes pour le personnel de service à la clientèle afin d'émettre des signalements de contenu douteux aux forces de l'ordre et à INHOPE). Portails de signalement: l'IWF met à disposition un portail de signalement en ligne sur mesure, qui permet aux internautes dans les pays et nations sans numéros d'écoute de signaler directement à l'IWF des images et des vidéos d'abus sexuels présumés sur des enfants.
	Pour les fournisseurs de services de connectivité, de stockage de données et d'hébergement dont les services impliquent un certain type d'hébergement de contenu (ce qui n'est pas le cas pour nombre d'entre eux), des processus de notification et de retrait doivent être mis en place.
Créer un environnement numérique plus sûr et adapté à l'âge	Les fournisseurs de services de connectivité, de stockage de données et d'hébergement peuvent contribuer à la création d'un environnement numérique plus sûr et plus agréable pour les enfants de tous âges, en prenant les mesures suivantes:
	Les fournisseurs de services de stockage de données/ d'hébergement doivent envisager de présenter la fonction de signalement sur tous leurs services et pages web. Ils doivent également élaborer et documenter des processus clairs afin de gérer rapidement les signalements d'abus ou toute autre violation des conditions générales.

Créer un environnement numérique plus sûr et adapté à l'âge*(suite)*	Les fournisseurs de connectivité doivent offrir des contrôles techniques internes ou indiquer si des outils créés par des fournisseurs spécialisés sont disponibles, si ces derniers sont appropriés pour les services proposés, faciles à mettre en œuvre par les utilisateurs finaux et s'ils permettent de bloquer ou de filtrer l'accès à l'Internet via les réseaux de l'entreprise. Fournir des mécanismes de vérification de l'âge appropriés si l'entreprise propose du contenu ou des services (y compris des services sous marque propre ou des services tiers promus par l'entreprise) qui ne sont légaux ou appropriés que pour des utilisateurs adultes (par exemple, certains jeux, loteries).
Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC	Les fournisseurs de services de connectivité, de stockage de données et d'hébergement doivent faire écho aux messages clés énoncés dans leurs conditions générales d'utilisation en rédigeant des directives communautaires dans un langage convivial pour soutenir les enfants et leurs parents ou responsables. Au sein du service à proprement parler, il est recommandé d'inclure des rappels au moment du téléchargement du contenu, sur des sujets tels que le type de contenu considéré comme inapproprié.
	Fournir aux enfants et aux jeunes des informations sur une utilisation plus sûre de l'Internet. Envisager des moyens créatifs de promouvoir des messages clés tels que: "Ne partagez jamais vos coordonnées, y compris votre emplacement physique et votre numéro de téléphone, avec des personnes que vous ne connaissez pas dans la vie réelle." "N'acceptez jamais un rendez-vous seul avec une personne que vous avez rencontrée en ligne sans en parler d'abord à un adulte. Dites toujours où vous vous trouvez à un ami de confiance." "Ne répondez pas aux messages d'intimidation, obscènes ou offensants. En revanche, ne supprimez pas le message afin de garder des preuves." "Si une situation ou une personne vous met mal à l'aise ou vous contrarie, dites-le à un adulte ou à un ami de confiance." "Ne donnez jamais votre mot de passe ou votre nom d'utilisateur! Sachez que d'autres personnes en ligne peuvent donner de fausses informations pour vous convaincre de partager vos informations personnelles."
	Les fournisseurs de services peuvent s'associer à des organisations bien placées pour éduquer les enfants sur une utilisation plus sûre de l'Internet et les problèmes connexes, et leur venir en aide. Le guide pratique de Child Helpline International et de la GSMA, intitulé "Child Helplines and Mobile Operators: Working together to protect children's rights" (Lignes d'assistance aux enfants et opérateurs mobiles: œuvrer ensemble à la protection des droits des enfants) est utile à ces fins.
Promouvoir les technologies numériques en tant que moyen de renforcer l'engagement civique	*Veuillez-vous référer aux directives générales du Tableau 1.*

5.2 Fonctionnalité B: proposer du contenu numérique soigneusement sélectionné

L'Internet propose tous types de contenus et d'activités, dont beaucoup sont destinés aux enfants et aux jeunes. Les services proposant du contenu soigneusement sélectionné présentent un potentiel incroyable en matière d'intégration de la sécurité et de la confidentialité dans leurs offres pour les enfants et les jeunes.

Cette fonctionnalité est destinée aussi bien aux entreprises qui créent leur propre contenu qu'à celles qui permettent d'accéder au contenu numérique. Il s'agit, entre autres, des services d'information et de diffusion multimédia, de services publics ou nationaux de radiodiffusion, et de l'industrie des jeux.

Le Tableau 3 fournit des conseils aux fournisseurs de services proposant du contenu soigneusement sélectionné sur les politiques et les mesures qu'ils peuvent entreprendre pour accroître la protection et la participation des enfants en ligne.

Tableau 3: Liste de contrôle aux fins de la protection des enfants en ligne pour la fonctionnalité B: proposer du contenu numérique soigneusement sélectionné

Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés	Les services proposant du contenu soigneusement sélectionné peuvent aider à repérer, prévenir et atténuer les effets néfastes des TIC sur les droits des enfants et des jeunes, et explorer les voies possibles en matière de promotion de ces droits en prenant les mesures suivantes:
	Établir des politiques qui protègent le bien-être des enfants et des jeunes contribuant à la diffusion de contenu en ligne, afin de prendre en compte le bien-être physique et émotionnel et la dignité des personnes de moins de 18 ans exposées à des programmes, des films, des jeux, des actualités, etc. sans l'accord d'un parent ou d'un autre adulte.
Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants	En collaboration avec le gouvernement, les forces de l'ordre, la société civile et les organisations de signalement, les entreprises proposant du contenu numérique soigneusement sélectionné peuvent jouer un rôle clé dans la lutte contre le matériel montrant des abus sexuels sur des enfants en prenant les mesures suivantes: Si du matériel montrant des abus sexuels sur des enfants est diffusé, par exemple par le biais de fonctionnalités qui permettent aux utilisateurs de mettre du contenu en ligne, comme les fonctions d'ajout de commentaires ou d'avis, le personnel doit contacter l'équipe de direction générale chargée de signaler ce type de matériel aux autorités compétentes. En outre, les membres du personnel doivent: • alerter immédiatement les services de police nationaux; • alerter leur responsable et signaler le matériel au responsable de la politique de protection de l'enfance; • fournir les détails de l'incident au service d'enquête interne par téléphone ou par e-mail et demander conseil; • attendre l'avis du service compétent avant de supprimer le matériel, de le sauvegarder dans un espace partagé ou de le transférer.

Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants *(suite)*	Si le contenu est identifié, il doit être signalé directement à une organisation spécialisée dans la sécurité sur Internet qui gère un système de signalement direct, permettant aux membres du public et aux professionnels des technologies de l'information de signaler des formes spécifiques de contenu en ligne potentiellement illégal. Par exemple, dans le cadre de sa politique de protection et de défense des enfants, la BBC a publié des directives éditoriales sur les interactions avec les enfants et les jeunes en ligne. Elle a élaboré d'autres listes de contrôle et codes de conduite concernant le travail avec les enfants et les jeunes en ligne, qui s'appliquent également aux sous-traitants et aux prestataires externes. La politique de l'Ofcom en matière de protection de l'enfance au Royaume-Uni concerne le contenu en ligne, les appareils mobiles et les consoles de jeu séparément. Mettre en œuvre une stratégie de transmission d'information rapide et solide si du matériel montrant des abus sexuels sur des enfants est publié ou si un comportement illégal est suspecté. Directives dans cette optique: • offrir aux utilisateurs une méthode simple et facilement accessible pour alerter le producteur de matériel de toute violation d'une règle de la communauté en ligne; • supprimer le matériel qui enfreint les règles; • offrir aux utilisateurs une méthode simple et facilement accessible pour alerter le producteur de matériel de toute violation d'une règle de la communauté en ligne; • supprimer le matériel qui enfreint les règles. Avant de télécharger du contenu sélectionné réservé à un certain public sur un réseau social, tenir compte des conditions générales d'utilisation du site. Prendre en considération l'âge minimum requis sur les différents sites de réseaux sociaux. Les conditions générales d'utilisation de chaque espace en ligne doivent également inclure des mécanismes clairs de signalement des infractions à ces règles.
Créer un environnement numérique plus sûr et adapté à l'âge	Les entreprises proposant des contenus numériques sélectionnés peuvent contribuer à la création d'un environnement numérique plus sûr et plus agréable pour les enfants et les jeunes de tous âges, en prenant les mesures suivantes:
	Travailler avec d'autres acteurs de l'industrie pour développer des systèmes de classification des contenus/de classification par âge basés sur des normes nationales ou internationales acceptées et conformes aux approches adoptées dans des médias équivalents. Dans la mesure du possible, les classifications de contenu doivent être cohérentes sur les différentes plates-formes médiatiques. Par exemple, une bande-annonce de film dans une salle de cinéma et sur un smartphone devrait indiquer les mêmes classifications.

Créer un environnement numérique plus sûr et adapté à l'âge *(suite)*	Créer pour les enfants et les jeunes des produits adaptés à leur âge qui sont sûrs dès leur conception et complétés par un solide système de vérification de l'âge.
	Pour aider les adultes, notamment les parents, à décider si un contenu est adapté à l'âge des enfants et des jeunes, créer des applications et des services dans tous les médias pour les aligner sur les systèmes de classification des contenus. Adopter des méthodes appropriées de vérification de l'âge pour empêcher les enfants et les jeunes d'accéder à des contenus, sites, produits ou services interactifs réservés à un certain public. Fournir des conseils et des rappels sur la nature et la classification par âge du contenu qu'ils utilisent.
	Une entreprise qui propose des services audiovisuels et multimédias peut envisager de fournir un numéro d'identification personnel aux utilisateurs qui cherchent à accéder à des contenus pouvant être nocifs pour les enfants et les jeunes.
	Être transparent concernant les prix des produits et services et concernant les informations collectées sur les utilisateurs. Veiller à ce que les politiques de collecte de données soient conformes aux lois applicables concernant la vie privée des enfants et des jeunes, notamment en examinant si le consentement des parents est requis avant que les entreprises commerciales ne puissent collecter des informations personnelles à propos d'un enfant.
	Garantir que la publicité ou la communication commerciale est clairement reconnaissable en tant que telle. Superviser le contenu mis en ligne et l'adapter aux groupes d'utilisateurs susceptibles d'y accéder au moyen, par exemple, de politiques appropriées sur la publicité en ligne auprès des enfants et des jeunes. Si l'offre de contenu prend en charge un élément interactif, tel que les commentaires, les forums en ligne, les réseaux sociaux, les plates-formes de jeu, les salons de discussion ou les forums, intégrer aux conditions et consignes d'utilisation un ensemble clair de "règles internes" dans un langage convivial.
	Décider du niveau d'engagement souhaité avant de lancer un service en ligne. Les services destinés à attirer les enfants ne devraient présenter que des contenus adaptés à un jeune public. En cas de doute, les autorités nationales chargées de la protection de l'enfance peuvent être consultées.
	Étiqueter le contenu de manière claire et factuelle. Garder à l'esprit que les utilisateurs peuvent tomber sur du contenu inapproprié en suivant des liens sur des sites tiers qui contournent les pages de contextualisation.

Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC	Les entreprises proposant du contenu numérique sélectionné peuvent accompagner les mesures techniques d'activités éducatives qui autonomisent les enfants en prenant les mesures suivantes:
	Fournir aux clients des informations spécifiques et claires sur le contenu proposé, telles que le type de contenu, les classifications/restrictions d'âge, la présence de langage grossier ou de violence et les options de contrôle parental correspondantes disponibles. Informer également sur le mode de signalement des abus et des contenus inappropriés ou illégaux et le traitement de ces rapports. Dans le monde interactif, ces informations doivent être fournies sous la forme d'étiquettes de contenu pour chaque programme.
	Encourager les adultes, en particulier les parents, les personnes s'occupant d'enfants et les éducateurs, à s'impliquer dans la consommation de contenu en ligne des enfants et des jeunes, afin qu'ils puissent les aider et les guider dans le choix de contenu au moment d'effectuer des achats, et les aider à établir des règles de conduite. Aider les enfants (ainsi que leurs parents ou les personnes s'occupant d'eux) à apprendre à gérer leur temps d'écran et à comprendre comment utiliser la technologie d'une manière qui leur convient, y compris quand s'arrêter et faire autre chose.
	Fournir des règles d'utilisation dans un langage clair et accessible qui encouragent les enfants et les jeunes à être vigilants et responsables lorsqu'ils naviguent sur l'Internet.
	Créer des outils adaptés à l'âge des utilisateurs, tels que des tutoriels et des centres d'aide. Travailler avec des programmes de prévention en ligne ou en personne et des cliniques de consultation, le cas échéant. Par exemple, s'il existe un risque que les enfants et les jeunes utilisent les technologies de façon excessive, les empêchant de développer des relations personnelles ou de participer à des activités physiques saines, un site peut fournir un lien de contact vers une ligne d'assistance téléphonique ou un service de consultation.

Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC *(suite)*	Faire en sorte que les informations de sécurité, telles que les liens vers des conseils, soient mises en avant, facilement accessibles et claires lorsque le contenu en ligne est susceptible de plaire à une forte proportion d'enfants et de jeunes.
	Proposer un outil d'orientation parental, tel qu'un "verrou" visant à contrôler le contenu accessible via un navigateur en particulier.
	Collaborer avec les parents pour garantir que les informations divulguées sur l'Internet concernant leurs enfants ne les mettent pas en danger. La manière dont les enfants sont identifiés dans les contenus sélectionnés nécessite un examen approfondi et variera en fonction du contexte. Dans la mesure du possible, obtenir le consentement éclairé des enfants lorsqu'ils figurent dans des programmes, films, vidéos, etc., et respecter tout refus de participer.
Promouvoir les technologies numériques en tant que moyen de renforcer l'engagement civique	Les entreprises proposant des contenus numériques sélectionnés peuvent encourager et autonomiser les enfants et les jeunes en soutenant leur droit à la participation grâce aux actions suivantes:
	Créer et/ou proposer une gamme de contenus de haute qualité, stimulants, éducatifs, amusants et intéressants, adaptés à l'âge des enfants et des jeunes, et qui les aident à comprendre le monde dans lequel ils vivent. En plus d'être attractifs, utilisables, fiables et sûrs, ces contenus peuvent contribuer au développement physique, mental et social des enfants et des jeunes en leur offrant de nouvelles possibilités de se divertir et d'apprendre. Les contenus permettant aux enfants d'accepter la diversité et d'être des modèles positifs doivent être fortement encouragés.

5.3 Fonctionnalité C: héberger du contenu produit par les utilisateurs et établir un lien entre ces derniers

Il fut un temps où le monde en ligne était dominé par les adultes, mais il est désormais clair que les enfants et les jeunes sont des acteurs majeurs dans les domaines en pleine expansion que sont la création et le partage de contenus produits par les utilisateurs, et ce, sur de multiples plates-formes. Cette fonctionnalité de service concerne, entre autres, les services de réseaux sociaux, les applications et les sites web liés à la réalisation créative.

Les services qui connectent les utilisateurs entre eux peuvent être répartis en trois catégories:

- Applications de messagerie principalement (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
- Services de réseaux sociaux principalement, qui recherchent et hébergent du contenu produit par les utilisateurs et permettent à ces derniers de partager du contenu et de se connecter au sein de leurs réseaux et en dehors (Instagram, Facebook, Snapchat, TikTok).
- Applications de diffusion en direct principalement (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Les fournisseurs de services exigent un âge minimum pour s'inscrire aux plates-formes, mais cette mesure est difficile à appliquer, car la vérification de l'âge dépend des données indiquées par l'utilisateur. La plupart des services qui connectent de nouveaux utilisateurs entre eux

autorisent également les fonctionnalités de partage de position, ce qui rend les enfants et les jeunes qui utilisent ces services encore plus vulnérables aux dangers hors ligne.

Le Tableau 4, qui a été adapté à partir des règles appliquées par l'un des plus grands réseaux sociaux, prodigue des conseils aux fournisseurs de services hébergeant du contenu produit par les utilisateurs et connectant les nouveaux utilisateurs. Ces conseils portent sur les politiques et les mesures qu'ils peuvent mettre en place pour accroître la protection et la participation en ligne des enfants.

Tableau 4: Liste de contrôle aux fins de la protection des enfants en ligne pour la fonctionnalité C: héberger du contenu produit par les utilisateurs et établir un lien entre ces derniers

Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés	Les services hébergeant du contenu produit par les utilisateurs et établissant un lien entre ces derniers peuvent repérer, prévenir et atténuer les effets néfastes des TIC sur les droits des enfants et des jeunes, et explorer les voies possibles en matière de promotion de ces droits.
	Veuillez-vous référer aux directives générales du Tableau 1.
Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants	En collaboration avec le gouvernement, les forces de l'ordre, la société civile et les organisations de signalement, les entreprises hébergeant du contenu produit par les utilisateurs et établissant un lien entre ces derniers peuvent jouer un rôle clé dans la lutte contre le matériel montrant des abus sexuels sur des enfants en prenant les mesures suivantes:
	Établir des procédures pour tous les sites afin de fournir une assistance immédiate aux forces de l'ordre en cas d'urgence et dans le cadre d'enquêtes de routine.
	Préciser qu'en cas de signalement ou de découverte de contenu illégal, l'entreprise coopérera pleinement dans le cadre des enquêtes des forces de l'ordre; spécifier les détails concernant les sanctions prévues le cas échéant (amendes ou annulation des privilèges de facturation).
	Travailler avec des services internes, tels que le service client, la prévention des fraudes et la sécurité, pour garantir que l'entreprise puisse signaler tout contenu illégal suspecté directement aux forces de l'ordre et aux plates-formes spécialisées. Idéalement, cela devrait être fait d'une manière qui n'expose pas le personnel de première ligne au contenu en question et qui ne revictimise pas les enfants et les jeunes touchés. Pour faire face aux situations où le personnel peut être exposé à du matériel abusif, mettre en œuvre une politique ou un programme favorisant la résilience, la sécurité et le bien-être du personnel.

Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants *(suite)*	Interdire les contenus et les comportements illégaux dans les conditions d'utilisation, en soulignant les points suivants: • Aucun contenu préjudiciable ne sera toléré, y compris le pédopiégeage dans l'intention de nuire avec ou sans contact. • Aucun contenu illégal ne sera toléré, y compris le téléchargement ou la diffusion ultérieure de matériel montrant des abus sexuels sur des enfants. • L'entreprise se référera et collaborera pleinement aux enquêtes des forces de l'ordre dans le cas où un contenu illégal ou une violation de la politique de protection de l'enfance seraient signalés ou découverts
	Documenter les pratiques de l'entreprise en matière de gestion du matériel montrant des abus sexuels sur des enfants, en commençant par la surveillance jusqu'au transfert final et à la destruction du matériel. Consigner une liste de tout le personnel responsable de la manipulation du matériel.
	Adopter des politiques concernant la propriété du contenu produit par les utilisateurs, et inclure la possibilité de supprimer ce contenu à la demande de l'utilisateur qui l'a créé. Supprimer le contenu qui enfreint les politiques du prestataire de services et avertir l'utilisateur qui l'a publié de la violation.
	Indiquer que le non-respect par un utilisateur des politiques d'utilisation acceptable aura des conséquences, notamment: • suppression du contenu, suspension ou fermeture de son compte; • révocation de sa capacité à partager des types particuliers de contenu ou à utiliser certaines fonctionnalités; • interdiction d'entrer en contact avec des enfants; • transmission des problèmes aux forces de l'ordre.
Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants	Promouvoir des systèmes de signalement du matériel montrant des abus sexuels sur des enfants ou de tout autre contenu illégal et s'assurer que les clients savent comment envoyer un rapport s'ils découvrent un contenu de ce type. Créer des systèmes et fournir du personnel qualifié pour évaluer les problèmes au cas par cas et prendre les mesures appropriées. Mettre en place des équipes opérationnelles d'assistance aux utilisateurs complètes et dotées de ressources suffisantes. Idéalement, ces équipes seraient formées pour gérer différents types d'incidents afin de garantir qu'une réponse adéquate est fournie et que des mesures appropriées sont prises. Lorsque l'utilisateur dépose une plainte, en fonction du type d'incident, celle-ci doit être acheminée vers le personnel approprié. L'entreprise peut également mettre en place des équipes spéciales pour traiter les appels des utilisateurs pour les cas où des rapports auraient été déposés par erreur.

Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants *(suite)*	Mettre en place des processus pour supprimer ou bloquer immédiatement l'accès au matériel montrant des abus sexuels sur des enfants, y compris des processus de notification et de retrait afin de supprimer les contenus illégaux dès qu'ils sont établis comme tels. Veiller à ce que les tiers avec lesquels l'entreprise entretient une relation contractuelle mettent en place des processus de notification et de retrait tout aussi solides. Si la législation le permet, le contenu peut être conservé comme preuve d'un crime en cas d'enquête.
	Mettre sur pied des systèmes techniques capables de détecter le contenu illégal connu et d'empêcher sa mise en ligne, y compris sur des groupes privés, ou de le signaler pour un examen immédiat par l'équipe de sécurité de l'entreprise. Prendre toutes les mesures appropriées pour protéger les services contre toute utilisation abusive visant à héberger, diffuser ou créer du matériel montrant des abus sexuels sur des enfants. Dans la mesure du possible, mettre en place des mesures techniques proactives pour analyser les objets et les métadonnées liés à un profil afin de détecter des comportements ou des schémas criminels, et prendre les mesures appropriées.
	Si l'application ou le service permet aux clients de mettre en ligne et de stocker des photographies sur des serveurs appartenant à l'entreprise ou exploités par celle-ci, mettre en place des processus et des outils pour identifier les images les plus susceptibles de montrer des abus sexuels sur des enfants. Envisager des techniques d'identification proactives telles que l'analyse technologique ou l'examen humain.
Créer un environnement numérique plus sûr et adapté à l'âge	Les fournisseurs de services proposant du contenu produit par les utilisateurs et établissant un lien entre ces derniers peuvent contribuer à la création d'un environnement numérique plus sûr et plus agréable pour les enfants de tous âges en prenant les mesures suivantes:
	Dans les conditions et consignes d'utilisation, communiquer, dans un langage convivial, un ensemble clair de "règles internes" qui définissent les éléments suivants: • la nature du service et les attentes vis-à-vis de ses utilisateurs; • les contenus, comportements et le langage acceptables ou non, ainsi que l'interdiction de toute utilisation illégale; • les conséquences de toute violation, par exemple, le signalement aux forces de l'ordre ou la suspension du compte de l'utilisateur.
	Les principaux messages sécuritaires et juridiques doivent être présentés dans un format adapté à l'âge (avec des icônes et des symboles intuitifs), aussi bien lors de l'inscription qu'en temps opportun lorsque différentes actions sont effectuées sur le site.

Créer un environnement numérique plus sûr et adapté à l'âge *(suite)*	Donner la possibilité aux clients de signaler facilement au service clientèle leurs préoccupations relatives à une utilisation abusive, grâce à des procédures types accessibles permettant de faire face à différentes préoccupations, telles que la réception de communications indésirables (spams, intimidation) ou la rencontre de contenus inappropriés.
	Fournir des paramètres de partage et de visibilité du contenu adaptés à l'âge des utilisateurs. Par exemple, rendre les paramètres de confidentialité et de visibilité pour les enfants et les jeunes plus restrictifs que ceux pour les adultes par défaut.
	Faire appliquer les règles sur l'âge minimal et soutenir la recherche et le développement de nouveaux systèmes de vérification de l'âge tels que la biométrie, en utilisant les normes internationales connues. Prendre des mesures propres à identifier et exclure les utilisateurs qui ont déformé la vérité pour accéder aux services. Il est important de tenir compte de la collecte de données personnelles supplémentaires que cela peut impliquer, ainsi que de la nécessité de limiter cette collecte, mais aussi le stockage et le traitement de ces informations. Si ce n'est déjà fait, établir des processus de connexion appropriés pour déterminer si les utilisateurs sont suffisamment âgés pour accéder au contenu ou au service sans compromettre leur identité, leur emplacement et leurs informations personnelles. Utiliser les systèmes de vérification de l'âge fonctionnels établis au niveau national, le cas échéant, lorsque des mesures pertinentes pour la confidentialité des données des enfants existent. Proposer une fonction de signalement ou un service/centre d'assistance qui peut encourager les utilisateurs à signaler les personnes qui ont falsifié leur âge.
	Protéger les jeunes utilisateurs des communications non sollicitées et garantir l'existence de directives relatives à la confidentialité et à la collecte d'informations.
	Trouver des moyens d'examiner les images et vidéos hébergées, et supprimer celles qui sont inappropriées lorsqu'elles sont détectées. Des outils tels qu'un système de recherche par hachage d'images connues et un logiciel de reconnaissance d'images sont disponibles à ces fins. Dans les services destinés aux enfants, les photos et les vidéos peuvent être vérifiées au préalable pour s'assurer que les enfants ne publient pas d'informations personnelles sensibles à leur sujet ou sur autrui.

Créer un environnement numérique plus sûr et adapté à l'âge *(suite)*	Un certain nombre de mesures peuvent être utilisées pour contrôler l'accès au contenu produit par les utilisateurs et protéger les enfants et les jeunes en ligne contre les contenus inappropriés ou illégaux. S'assurer que des mots de passe sécurisés sont utilisés pour protéger les enfants et les jeunes dans les paramètres de jeux et d'autres réseaux sociaux. Autres méthodes: • Examiner les groupes de discussion afin de détecter les éventuels thèmes préjudiciables, les discours de haine et les comportements illégaux, et de supprimer ces contenus lorsqu'ils enfreignent les conditions d'utilisation. • Créer des outils permettant de rechercher et de supprimer activement les contenus illégaux ou non conformes aux conditions générales de service de l'entreprise, ainsi que des outils empêchant la mise en ligne de contenus illégaux connus sur le site. • Garantir une prémodération des forums par une équipe de modérateurs spécialisés dans l'encadrement des enfants et des jeunes en ligne, qui vérifient que les messages sont conformes aux règles en usage. Les messages peuvent être lus avant leur publication, et les utilisateurs suspects (comme ceux qui ont besoin d'aide) pourront être repérés. • Mettre en place une équipe d'accueil faisant office de premier référent des modérateurs préoccupés par tel ou tel utilisateur.
	Assurer l'examen des contenus commerciaux, y compris sur les forums, les réseaux sociaux et les sites de jeux. Mettre en œuvre des normes et des règles pertinentes pour protéger les enfants contre la publicité inappropriée pour leur âge, et établir des limites claires pour la publicité en ligne destinée aux enfants et aux jeunes.
Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC	Les fournisseurs de services proposant du contenu produit par les utilisateurs peuvent accompagner les mesures techniques d'activités d'éducation et d'autonomisation en prenant les mesures suivantes:
	Créer une section consacrée spécialement aux conseils de sécurité, aux articles, aux fonctionnalités et au dialogue sur la citoyenneté numérique, et fournir des liens vers des contenus utiles d'experts tiers. Les conseils en matière de sécurité doivent être facilement repérables et fournis dans un langage compréhensible. Les fournisseurs de plates-formes sont également encouragés à avoir une interface de navigation uniforme sur différents appareils (ordinateurs, tablettes ou téléphones mobiles).
	Fournir aux parents des informations claires sur les types de contenu et de services disponibles. Inclure, par exemple, une explication sur les sites de réseaux sociaux et les services géolocalisés, sur la manière d'accéder à l'Internet à partir d'appareils mobiles, et énoncer les options à disposition des parents pour appliquer des contrôles.

Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC *(suite)*	Indiquer aux parents la marche à suivre pour signaler toute maltraitance, toute utilisation abusive et tout contenu inapproprié ou illégal, ainsi que la façon dont le signalement sera traité. Préciser quels services sont soumis à une limite d'âge et quels sont les comportements sûrs et responsables à adopter lors de l'utilisation de services interactifs.
	Établir un système fondé sur "la confiance et la réputation" afin d'encourager les bons comportements et de permettre l'enseignement entre pairs des bonnes pratiques par l'exemple. Souligner l'importance des signalements sociaux, qui permettent aux personnes de contacter d'autres utilisateurs ou des amis de confiance qui peuvent les aider à résoudre un conflit. Ils permettent également d'initier une conversation sur un contenu troublant.
	Fournir des conseils et des rappels sur la nature d'un service ou d'un contenu donné et comment en bénéficier en toute sécurité. Intégrer des orientations communautaires dans les services interactifs, par exemple, au moyen de fenêtres contextuelles de sécurité qui rappellent aux utilisateurs d'adopter un comportement approprié et sûr, comme le fait de ne pas donner leurs coordonnées.
	Collaborer avec les parents et les guider pour garantir que les informations divulguées sur l'Internet concernant leurs enfants ne les mettent pas en danger. Dans la mesure du possible, obtenir le consentement éclairé des enfants lorsqu'ils figurent dans un contenu destiné à la publication qu'ils ont eux-mêmes créé, et respecter tout refus.
Promouvoir les technologies numériques en tant que moyen de renforcer l'engagement civique	Les services hébergeant du contenu produit par les utilisateurs peuvent encourager et autonomiser les enfants et les jeunes en soutenant leur droit à la participation.
	Veuillez-vous référer aux directives générales du Tableau 1.

5.4 Fonctionnalité D: systèmes reposant sur l'IA

Avec l'attention accrue accordée aux technologies d'apprentissage profond, les termes "intelligence artificielle", "apprentissage automatique" et "apprentissage profond" sont utilisés de manière interchangeable par le grand public pour faire référence au concept de réplication d'un comportement "intelligent" dans les machines. Cette section porte sur l'impact de l'apprentissage automatique et des processus d'apprentissage profond sur la vie des enfants et, en définitive, sur leurs droits fondamentaux.

"En raison des progrès exponentiels des technologies basées sur l'intelligence artificielle au cours des dernières années, le cadre international actuel qui protège les droits de l'enfant n'aborde pas explicitement un grand nombre de problèmes soulevés par le développement et l'utilisation de l'intelligence artificielle. Cependant, il met en évidence plusieurs droits pouvant être remis en cause par ces technologies, et fournit ainsi un point de départ important pour

toute analyse des impacts positifs ou négatifs des nouvelles technologies sur les droits des enfants, notamment le droit à la vie privée, à l'éducation, au jeu et à la non-discrimination[18]".

L'utilisation de l'IA peut affecter l'impact sur les enfants des différents services utilisés sur les réseaux sociaux, tels que les plates-formes de streaming vidéo. Les algorithmes d'apprentissage automatique, moteur de recommandation principalement utilisé par les plates-formes de partage de vidéos populaires, sont optimisés pour garantir un maximum de vues de vidéos spécifiques dans un délai donné[19]. La technologie des écrans tactiles et la conception de ces plates-formes permettent aux très jeunes enfants de parcourir et d'explorer ces contenus. Le fait que les algorithmes utilisant des vidéos recommandées puissent piéger les enfants dans des "cyberbulles" constituées de contenus médiocres ou inappropriés est particulièrement inquiétant. Les enfants étant particulièrement sensibles aux recommandations de contenu, des "vidéos connexes" choquantes peuvent attirer leur attention et les détourner de programmes plus adaptés aux enfants[20].

L'IA a également un impact sur la protection des enfants en ligne en ce qui concerne les jouets intelligents. Les différents processus impliqués dans le fonctionnement des jouets intelligents présentent leurs propres défis: le jouet lui-même (avec lequel l'enfant interagit), l'application mobile (servant de point d'accès pour la connexion WiFi) et le compte en ligne personnalisé du jouet/consommateur (où les données sont stockées). Ces jouets communiquent avec des serveurs dans le nuage qui stockent et traitent les données fournies par les enfants interagissant avec les jouets. Ce modèle implique des problèmes de confidentialité si une sécurité n'est pas garantie à chaque niveau, comme en attestent les nombreux cas de piratage à l'occasion desquels des informations personnelles ont été divulguées. De plus, certains des appareils piratés (y compris les appareils intelligents dotés d'un accès au web, tels que les moniteurs pour bébé, les assistants vocaux, etc.) peuvent être utilisés pour surveiller les utilisateurs à leur insu ou sans leur consentement.

Lors de l'intégration de mécanismes de réponse aux menaces détectées contre les enfants utilisant ces appareils, par exemple au moyen de conseils et de recommandations basés sur le comportement détecté (comme mentionné précédemment avec l'application Own IT de la BBC), il est essentiel que les entreprises qui conçoivent des appareils intelligents fondent ces recommandations sur des données probantes et les élaborent en consultation avec des experts en protection de l'enfance.

Si certaines entreprises promeuvent des principes pour une utilisation éthique de l'IA[21], il ne semble pas encore exister de politiques publiques concernant l'IA et les enfants[22]. Plusieurs associations technologiques et commerciales, ainsi que des groupements scientifiques et informatiques, ont rédigé des principes éthiques s'appliquant à l'IA[23]. Cependant, ceux-ci ne font pas explicitement référence aux droits de l'enfant, aux risques que ces technologies d'IA peuvent impliquer pour les enfants, ni aux plans proactifs pour les atténuer.

---

18 UNICEF et université de Californie à Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.
19 Ibid.
20 Ibid.
21 Microsoft, rapport "Salient Human Rights Issues" concernant l'exercice 2017; Google, "Responsible Development of AI", 2018.
22 Official Microsoft Blog, "The Future Computed: Artificial Intelligence and its role in society", 2018.
23 The Guardian, "Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016.

À l'instar des entreprises, les gouvernements du monde entier ont adopté des stratégies pour devenir des chefs de file dans le développement et l'utilisation de l'IA, favorisant des environnements propices aux innovateurs et aux entreprises[24]. On ignore cependant l'approche de ces stratégies nationales en ce qui concerne directement les droits de l'enfant.

Améliorer la gestion par Facebook du contenu lié au suicide et à l'automutilation

En 2019, Facebook a commencé à organiser des consultations régulières avec des experts du monde entier pour discuter de certains des sujets les plus délicats associés au suicide et à l'automutilation. Il s'agit notamment de la manière de réagir face aux notes de suicide, aux risques liés au contenu triste en ligne et aux représentations médiatiques du suicide. De plus amples informations sur ces réunions sont disponibles sur la nouvelle page Facebook de prévention du suicide, dans le Centre de sécurité. Ces consultations ont abouti sur plusieurs améliorations dans la manière dont Facebook gère ce type de contenu. La politique concernant l'automutilation, par exemple, a été renforcée de sorte à interdire les images explicites de personne s'infligeant des blessures, afin d'éviter de promouvoir ou d'inciter involontairement à l'automutilation. Même lorsqu'une personne cherche de l'aide ou s'exprime pour parvenir à son rétablissement, Facebook affiche désormais un écran de sensibilité sur les images de cicatrices guéries résultant de l'automutilation. Ce type de contenu est maintenant détecté grâce à des technologies d'IA, grâce auxquelles des mesures sur les contenus potentiellement dangereux, y compris leur suppression ou l'ajout d'écrans de sensibilité, peuvent être prises automatiquement. Entre avril et juin 2019, Facebook a traité plus de 1,5 million de contenus liés au suicide et à l'automutilation sur son site, et en a détecté plus de 95% avant leur signalement par un utilisateur. Au cours de la même période, Instagram a traité plus de 800 000 contenus similaires, dont plus de 77% ont été détectés avant d'être signalés par un utilisateur.

Reconnaître en temps réel les potentiels cas d'intimidation ou de violence entre utilisateurs, et contacter les utilisateurs par message

Instagram met en place un système d'IA visant à éliminer les comportements tels que les insultes, les humiliations et le manque de respect. Équipés d'outils de signalement sophistiqués, les modérateurs sont en mesure de fermer rapidement le compte appartenant à un auteur d'intimidation en ligne.

[24] Ibid.

Bonne pratique: s'appuyer sur l'IA pour détecter du matériel montrant des abus sexuels sur des enfants

S'appuyant sur la généreuse contribution de Microsoft, avec PhotoDNA, pour lutter contre l'exploitation des enfants et le récent lancement de l'API Content Safety de Google, Facebook a également développé des technologies permettant de détecter le matériel montrant des abus sexuels sur des enfants.

Connues sous le nom de PDQ et TMK+PDQF, ces technologies font partie d'une suite d'outils utilisés par Facebook pour détecter les contenus préjudiciables. Parmi les autres algorithmes et outils disponibles pour l'industrie, on retrouve pHash, aHash et dHash. PDQ, l'algorithme de mise en correspondance de photos Facebook, est largement inspiré de pHash, bien qu'il ait été conçu à partir de zéro comme un algorithme distinct avec une implémentation logicielle indépendante. Quant à la technologie de mise en correspondance de vidéos, TMK+PDQF, elle a été développée conjointement par l'équipe de recherche sur l'IA de Facebook et des universitaires de l'Université de Modène et de Reggio d'Émilie, en Italie.

Ces technologies représentent un moyen efficace de stocker des fichiers sous forme de hachages numériques courts. Elles sont capables de déterminer si deux fichiers sont identiques ou similaires, même sans disposer de l'image ou de la vidéo d'origine. Les hachages peuvent également être plus facilement partagés avec d'autres entreprises et organisations à but non lucratif.

PDQ et TMK+PDQF ont été conçus pour fonctionner à grande échelle et pour prendre en charge le hachage de trames vidéo et les applications en temps réel.

Des recommandations permettant aux entreprises d'aligner leurs principes lors de la conception et de la mise en œuvre de solutions basées sur l'IA ciblant les enfants sont présentées dans le Tableau 5.

Ces recommandations s'appuient sur les travaux de l'UNICEF visant à élaborer des orientations politiques mondiales sur l'IA et les enfants, qui seront destinées aux gouvernements et aux professionnels. Consulter le site https://www.unicef.org/globalinsight/featured-projects/ai-children pour en savoir plus sur le projet. Les recommandations s'inspirent également du document de l'UNICEF et de l'université de Californie à Berkeley sur l'IA et les droits de l'enfant[25].

[25] UNICEF et université de Californie à Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Tableau 5: Liste de contrôle aux fins de la protection des enfants en ligne pour la fonctionnalité D: systèmes reposant sur l'IA

Intégrer les considérations liées aux droits de l'enfant dans l'intégralité des politiques et processus de gestion des entreprises appropriés	Les fournisseurs de systèmes reposant sur l'IA peuvent repérer, prévenir et atténuer les effets néfastes des TIC sur les droits des enfants et des jeunes, et explorer les voies possibles en matière de promotion de ces droits.
	Les systèmes d'IA doivent être conçus, développés, mis en œuvre et faire l'objet de recherches dans l'optique de respecter, promouvoir et réaliser les droits des enfants, tels qu'ils sont entérinés par la Convention relative aux droits de l'enfant. Les enfants, de plus en plus expérimentés dans l'environnement numérique, ont besoin de soins et d'une assistance spécifiques. Les systèmes d'IA doivent être mis à profit pour fournir un soutien optimal.
	Incorporer une approche de conception inclusive lors du développement des produits destinés aux enfants, qui maximise la diversité de genre, géographique et culturelle, et qui inclut un large éventail de parties prenantes, telles que les parents, les enseignants, les psychologues pour enfants et, le cas échéant, les enfants eux-mêmes.
	Des cadres de gouvernance, comme des directives éthiques, des lois, des normes et des organismes de réglementation, doivent être établis pour superviser les processus qui garantissent que l'application des systèmes d'IA ne porte pas atteinte aux droits de l'enfant.
Établir des processus standard pour la gestion du matériel montrant des abus sexuels sur des enfants	En collaboration avec le gouvernement, les forces de l'ordre, la société civile et les organisations de signalement, les fournisseurs de systèmes reposant sur l'IA jouent un rôle clé dans la lutte contre le matériel montrant des abus sexuels sur des enfants en prenant les mesures suivantes:
	Veuillez-vous référer aux directives générales du Tableau 1.
Créer un environnement numérique plus sûr et adapté à l'âge	Les fournisseurs de systèmes reposant sur l'IA peuvent contribuer à la création d'un environnement numérique plus sûr et plus agréable pour les enfants de tous âges en prenant les mesures suivantes:
	Adopter une approche multidisciplinaire lors du développement de technologies qui affectent les enfants et consulter la société civile, y compris le monde universitaire, pour cerner les retombées potentielles de ces technologies sur les droits d'un large éventail d'utilisateurs finaux potentiels.

Créer un environnement numérique plus sûr et adapté à l'âge *(suite)*	Garantir la sécurité et la confidentialité dès la conception pour les produits et services destinés aux enfants ou couramment utilisés par ceux-ci.
	Les systèmes d'IA étant gourmands en données, les entreprises qui les utilisent pour leurs services doivent faire preuve d'une vigilance particulière en ce qui concerne la collecte, le traitement, le stockage, la vente et la publication des données personnelles des enfants. Les systèmes d'IA doivent être transparents, en ce sens qu'il devrait être possible de déterminer comment et pourquoi un système a pris une décision en particulier ou, dans le cas d'un robot, a agi de telle ou telle manière. Cette transparence est essentielle pour développer la confiance et faciliter les audits, les enquêtes et les recours en cas de suspicion de préjudice porté à des enfants. Veiller à ce qu'il existe des mécanismes fonctionnels et juridiques de recours si des enfants ont subi ou déclarent avoir subi un préjudice par le biais des systèmes d'IA. Des processus doivent être établis pour corriger en temps opportun toute pratique discriminatoire, et des organes de contrôle doivent être mis en place pour gérer les appels et le suivi continu de la sécurité et de la protection des enfants. La responsabilité et les mécanismes de recours vont de pair.
	Élaborer des plans pour traiter des données particulièrement sensibles, y compris des révélations de maltraitance ou d'autres préjudices pouvant être partagés avec l'entreprise par le biais de ses produits. Les plates-formes numériques et les systèmes d'IA doivent minimiser la collecte de données sur les enfants et optimiser le contrôle de ces derniers sur les données qu'ils créent. Les conditions d'utilisation doivent être compréhensibles pour les enfants, afin de renforcer leur sensibilisation et leur capacité d'action.
Éduquer les enfants, les personnes s'occupant d'enfants et les éducateurs au sujet de la sécurité des enfants et de l'utilisation responsable des TIC	Les fournisseurs de systèmes reposant sur l'IA peuvent compléter ces mesures techniques par des activités d'éducation et d'autonomisation.
	Il doit être possible d'expliquer l'objectif des systèmes d'IA aux utilisateurs mineurs et à leurs parents ou tuteurs, afin qu'ils soient en mesure de décider ou de refuser d'utiliser de telles plates-formes.

Promouvoir les technologies numériques en tant que moyen de renforcer l'engagement civique	Les fournisseurs de systèmes reposant sur l'IA peuvent encourager et autonomiser les enfants et les jeunes en soutenant leur droit à la participation. *Veuillez-vous référer aux directives générales du Tableau 1.*
Protéger et éduquer les enfants grâce aux avancées technologiques	Le développement et le bien-être des enfants doivent constituer des objectifs lors de la conception, l'élaboration et la mise en œuvre de tous les systèmes basés sur l'IA. Les meilleurs indicateurs de développement et de bien-être disponibles et largement acceptés doivent représenter des bases de référence. Les entreprises doivent investir dans la recherche et le développement d'outils éthiques basés sur l'IA pour détecter le matériel montrant des abus sexuels sur des enfants en ligne, ainsi que le harcèlement et l'intimidation en ligne. Ces mesures doivent être prises en collaboration avec des experts clés du droit des enfants, mais aussi avec des enfants. Les progrès réalisés par les technologies d'IA doivent être appliqués afin de cibler les messages adaptés à l'âge des enfants, sans toutefois compromettre leur identité, leur emplacement et leurs informations personnelles.

Références

Texte du RGPD (Règlement [UE] 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE [règlement général sur la protection des données]), et texte tel que publié au Journal officiel de l'Union européenne.

Directive (UE) 2018/1808 du parlement européen et du conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive "Services de médias audiovisuels"), compte tenu de l'évolution des réalités du marché, et texte tel que publié au Journal officiel de l'Union européenne.

Politique de la BBC:

- Child protection and safeguarding policy (Politique de protection et de sauvegarde de l'enfant) version 2017, révisée en 2018, etmise à jour en 2019
- Working with young people and children at the BBC (Travailler avec des jeunes et des enfants à la BBC)
- Framework for Independent Production Companies working on BBC Productions (Cadre pour les sociétés indépendantes travaillant sur des productions de la BBC) – porte sur les règles des fournisseurs externes à propos de la protection de l'enfance
- Guidance: Interacting with children and young people online (Orientations: interagir avec les enfants et les jeunes en ligne) – fournit des directives éditoriales pour les activités en ligne

Enquête prouvant le non-respect de la vérification de l'âge sur les réseaux sociaux au Royaume-Uni: 2016, 2017, 2020.

Glossaire

Les définitions ci-dessous sont principalement tirées de la terminologie existante énoncée dans la Convention relative aux droits de l'enfant de 1989, ainsi que par le Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels du Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants (Luxembourg, 2016), par la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (2007), ainsi que par le rapport Global Kids Online de l'UNICEF (2019).

Adolescent

Les adolescents sont des personnes âgées de 10 à 19 ans. Il est important de noter que le terme "adolescent" n'est pas contraignant en vertu du droit international et que les personnes de moins de 18 ans sont considérées comme des enfants, tandis que les personnes âgées de 18 à 19 ans sont considérées comme des adultes, sauf si la majorité est atteinte plus tôt en vertu du droit national[26].

Intelligence artificielle

Au sens large, l'expression intelligence artificielle (IA) 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 déjà opérationnels en capacité d'exécuter des tâches très complexes (reconnaissance de visage ou de voix, conduite de véhicule – ces systèmes sont qualifiés d'IA "faibles" ou "modérées")[27].

Système reposant sur l'intelligence artificielle

Un système reposant sur l'IA (ou système d'IA) est un système automatisé qui, pour un ensemble donné d'objectifs définis par des êtres humains, est en mesure d'établir des prévisions, de formuler des recommandations, ou de prendre des décisions influant sur des environnements réels ou virtuels. Les systèmes d'IA sont conçus pour fonctionner à des degrés d'autonomie divers[28].

Alexa

Amazon Alexa, connu simplement sous le nom d'Alexa, est un assistant virtuel conçu par Amazon et reposant sur l'IA. Cet outil est capable d'interagir vocalement, de lire de la musique, de créer des listes de tâches, de définir des alarmes, de diffuser des podcasts, de lire des livres audio et d'indiquer la météo, le trafic routier, les résultats sportifs et d'autres informations en temps réel, telles que les actualités. Alexa peut également contrôler plusieurs appareils intelligents en s'utilisant comme système domotique. Les utilisateurs peuvent étendre les capacités d'Alexa en installant des "compétences" (fonctionnalités supplémentaires développées par des fournisseurs tiers, dans d'autres milieux plus communément appelés "applications", comme des bulletins météo et des fonctionnalités audio)[29].

---

26 UNICEF et UIT, "Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne", 2014.
27 Conseil de l'Europe, "L'IA, c'est quoi?".
28 OCDE, "Recommandation du Conseil sur l'intelligence artificielle", 2019.
29 UNICEF et UIT, "Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne", 2014.

Intérêt supérieur de l'enfant

Fait référence à tous les éléments nécessaires pour prendre une décision dans une situation spécifique pour un enfant ou un groupe d'enfants spécifique[30].

Enfant

Conformément à l'Article 1 de la Convention relative aux droits de l'enfant, un enfant s'entend de tout être humain âgé de moins de 18 ans, sauf si la majorité est atteinte plus tôt en vertu du droit national[31].

Exploitation et abus sexuels à l'encontre des enfants

Décrit toutes les formes d'exploitation et d'abus sexuels, 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; et c) que des enfants [soient] exploités aux fins de la production de spectacles ou de matériel de caractère pornographique"[32], ainsi que tout "contact sexuel qui implique généralement l'usage de la force sur une personne sans son consentement"[33]. 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.

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[34]. 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 problèmes sous le terme "matériel montrant des abus sexuels sur des enfants". Ce terme, conforme aux lignes directrices de la Commission sur le large bande et au modèle de réponse nationale de l'Alliance mondiale WePROTECT[35], 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 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". Lorsque nous utilisons terme "matériel montrant des abus sexuels sur des enfants", nous faisons 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

30 Voir la Convention des Nations Unies relative aux droits de l'enfant.
31 UNICEF et UIT, "Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne", 2014.
32 Article 34 de la Convention des Nations Unies relative aux droits de l'enfant.
33 Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels. Luxembourg , 2016.
34 Guide de terminologie du Luxembourg (voir supra), 2016, et rapport Global Kids Online de l'UNICEF, 2019.
35 Commission "Le large bande au service du développement durable", Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019; WePROTECT Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévention et lutte contre l'exploitation et les abus sexuels à l'encontre des enfants: modèle de réponse nationale), 2016.

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.

Consulter le Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels pour connaître la définition de termes tels que "matériel d'abus sexuels d'enfants généré informatiquement".

Enfants et jeunes

Décrit toutes les personnes de moins de 18 ans, les "enfants" (également appelés "jeunes enfants" dans les présentes lignes directrices de l'UIT) englobant toutes les personnes de moins de 15 ans et les "jeunes" regroupant les personnes âgées entre 15 et 18 ans.

Jouets connectés

Les jouets connectés se connectent à l'Internet grâce à des technologies telles que le WiFi et le Bluetooth, et fonctionnent généralement conjointement avec des applications associées pour permettre aux enfants de jouer de façon interactive. Selon Juniper Research, en 2015, le marché des jouets connectés atteignait 2,8 milliards USD et devrait passer à 11 milliards USD d'ici à 2020. Ces jouets collectent et stockent les informations personnelles des enfants, y compris leur nom, leur géolocalisation, leur adresse, leurs photographies et leurs enregistrements audio et vidéo[36].

Cyberintimidation

La cyberintimidation désigne un acte intentionnellement agressif commis à plusieurs reprises par un groupe ou un individu à l'aide de la technologie numérique, et visant une victime qui n'est pas en mesure de se défendre facilement[37]. Cela consiste généralement à utiliser la technologie numérique et l'Internet pour publier des informations blessantes sur une personne, partager délibérément des informations, des photos ou des vidéos privées de manière blessante, envoyer des messages menaçants ou insultants (par e-mail, messagerie instantanée, chat ou SMS), répandre des rumeurs et de fausses informations sur la victime ou l'exclure délibérément des communications en ligne[38].

Cyberhaine, discrimination et extrémisme violent

La cyberhaine, la discrimination et l'extrémisme violent sont des formes distinctes de cyberviolence dans la mesure où ces comportements visent une identité collective, plutôt que des individus. Ils sont souvent liés à l'appartenance éthique ou religieuse, à l'orientation sexuelle, à la nationalité ou au statut d'immigration, au sexe/genre et aux convictions politiques[39].

Citoyenneté numérique

La citoyenneté numérique se réfère à la capacité de s'engager positivement, de manière critique et compétente dans l'environnement numérique, en s'appuyant sur des aptitudes de

---

36 Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security". *Georgetown Law Technology Review*, 2017.

37 Anna Costanza Baldry *et al.* "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities", *Children and Youth Services Review*, 2019.

38 Guide de terminologie du Luxembourg, 2016, et rapport Global Kids Online de l'UNICEF, 2019 (voir supra).

39 UNICEF, rapport Global Kids Online, 2019 (voir supra).

communication et de création efficaces, pour pratiquer des formes de participation sociale respectueuses des droits de l'homme et de la dignité grâce à l'utilisation responsable de la technologie[40].

Culture numérique

La culture numérique fait référence aux compétences nécessaires pour vivre, apprendre et travailler dans une société où la communication et l'accès à l'information sont en plein essor grâce aux technologies numériques telles que les plates-formes Internet, les réseaux sociaux et les appareils mobiles[41]. Elle fait référence à une communication claire, des compétences techniques et une pensée critique.

Résilience numérique

Ce terme désigne la capacité d'un enfant à faire face sur le plan émotionnel aux préjudices rencontrés en ligne. Il fait également référence à l'intelligence émotionnelle nécessaire pour comprendre lorsqu'un enfant est exposé à des risques en ligne, pour savoir comment demander de l'aide, pour tirer des leçons des expériences et pour se rétablir lorsque les choses tournent mal[42].

Direction

Désigne l'ensemble des personnes qui occupent un poste dans une structure de gestion ou de gouvernance d'école.

Pédopiégeage ou manipulation psychologique sur Internet à des fins sexuelles

Désigné sous le terme "grooming" dans le Guide de terminologie, cette expression désigne le processus d'établissement/de création d'une relation avec un enfant, que ce soit en personne ou via l'utilisation d'Internet ou d'autres technologies numériques, afin de faciliter des contacts sexuels *en ligne ou hors ligne* avec cet enfant. Il s'agit de l'activité criminelle consistant à se lier d'amitié avec un enfant, afin d'essayer de le persuader d'avoir une relation sexuelle.

Technologies de l'information et de la communication

Les technologies de l'information et de la communication (TIC) désignent toutes les technologies de l'information qui mettent l'accent sur l'aspect de la communication. Cela comprend l'ensemble des services et appareils de connexion Internet tels que les ordinateurs, les ordinateurs portables, les tablettes, les smartphones, les consoles de jeux et les montres intelligentes[43]. Sont également inclus les services de radio et de télévision, ainsi que le large bande, le matériel de réseau et les systèmes satellitaires.

Jeu en ligne

Désigne tout type de jeu numérique commercial à un ou plusieurs joueurs, utilisable via un appareil connecté à Internet quel qu'il soit, y compris les consoles de jeu, les ordinateurs de

---

40 Conseil de l'Europe, "Citoyenneté numérique et éducation à la citoyenneté numérique".
41 Université occidentale de Sydney, "What is digital literacy?".
42 Dr. Andrew K. Przybylski *et al.*, "A Shared Responsibility: Building children's' online resilience". *Virgin Media and Parent Zone*, 2014.
43 UNICEF et UIT, "Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne", 2014 (voir supra).

bureau, les ordinateurs portables, les tablettes et les téléphones mobiles. L'"écosystème des jeux en ligne" inclut le fait de regarder d'autres personnes jouer à des jeux vidéo via des plates-formes de sports électroniques, de diffusion en direct ou de partage de vidéos, qui offrent généralement aux spectateurs la possibilité de commenter ou d'interagir avec les joueurs et d'autres membres du public[44].

Outil de contrôle parental

Logiciel permettant aux utilisateurs, généralement un parent, de contrôler certaines ou l'ensemble des fonctions d'un ordinateur ou d'un autre appareil pouvant se connecter à l'Internet. En règle générale, ces programmes peuvent limiter l'accès à des types ou des catégories particuliers de sites web ou de services en ligne. Certains proposent également des fonctionnalités de gestion du temps: l'appareil peut alors être configuré pour avoir accès à l'Internet entre certaines heures uniquement. Des versions plus avancées peuvent enregistrer tous les messages envoyés depuis un appareil ou reçus sur ce dernier. Ces programmes sont normalement protégés par un mot de passe[45].

Information personnelle

Cette expression désigne toute information collectée en ligne et individuellement identifiable à propos d'une personne. Il peut s'agir du nom complet, des coordonnées (adresses postale et e-mail, numéros de téléphone), des empreintes digitales ou du matériel de reconnaissance faciale, de numéros d'assurance ou de tout autre facteur permettant la prise de contact physique ou virtuel avec une personne, ou bien sa localisation. Dans ce contexte, les informations personnelles désignent en outre toute information sur un enfant et son entourage qui est collectée en ligne par des fournisseurs de services Internet, y compris les jouets connectés et l'Internet des objets, et toute autre technologie connectée.

Confidentialité

La confidentialité est souvent évaluée sur le plan du partage d'informations personnelles en ligne, comme le fait d'avoir un profil public sur les réseaux sociaux, de partager des informations avec des personnes rencontrées en ligne, d'utiliser des paramètres de confidentialité, de partager des mots de passe avec des amis et des préoccupations concernant la confidentialité[46].

Média de service public

Il s'agit de tout diffuseur ou média national ayant reçu sa licence de diffusion sur la base d'une série d'obligations contractuelles auprès de l'État ou du parlement. Ces dernières années, ces obligations ont été étendues dans de nombreux pays afin de lutter contre les conséquences négatives de la transformation numérique. Cela a été rendu possible grâce à des programmes d'éducation médiatique et numérique, ainsi qu'à des obligations de réduire la fracture numérique.

---

44 UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry" (Droits de l'enfant et jeux en ligne: possibilités et défis pour les enfants et l'industrie), 2019.

45 UNICEF et UIT, "Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne", 2014 (voir supra).

46 Commission fédérale du commerce des États-Unis, "Children's Online Privacy Protection Act", 1998.

Sexting

Le sexting est généralement défini comme le fait d'envoyer, de recevoir ou d'échanger du contenu sexualisé autoproduit, y compris des images, des messages ou des vidéos via des téléphones mobiles et/ou l'Internet[47]. La création, la diffusion et la possession d'images d'enfants à caractère sexuel sont illégales dans la plupart des pays. Si des images sexuelles autoproduites d'enfants sont divulguées, les adultes ne sont pas autorisés à les voir. Tout partage d'images sexuelles par un adulte avec un enfant constitue un acte criminel et potentiellement préjudiciable. Il peut être obligatoire de signaler ces images et de les supprimer.

Sextorsion ou chantage à la webcam

La sextorsion 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)"[48].

Internet des objets

L'Internet des objets représente la prochaine étape vers la numérisation de notre société et de notre économie, où les objets et les personnes sont interconnectés via des réseaux de communication et rendent compte de leur état et/ou de leur environnement[49].

URL

Cette abréviation signifie "uniform resource locator" (localisateur uniforme de ressource) et correspond à l'adresse d'une page Internet[50].

Réalité virtuelle

La réalité virtuelle consiste à utiliser la technologie informatique pour créer l'effet d'un monde interactif en trois dimensions dans lequel les objets semblent être présents dans l'espace[51].

WiFi

Le WiFi (ou Wireless Fidelity, qui signifie "fidélité sans fil") représente le groupe de normes techniques qui permettent la transmission de données sur des réseaux sans fil[52].

47 Guide de terminologie du Luxembourg, 2016 (voir supra).
48 Guide de terminologie du Luxembourg, 2016 (voir supra).
49 Commission européenne, "Policy: The Internet of Things".
50 UNICEF et UIT, "Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne", 2014 (voir supra).
51 NASA, "Virtual Reality: Definition and Requirements".
52 Commission fédérale du commerce des États-Unis, "Children's Online Privacy Protection Act", 1998.

'Avec le soutien de:

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

ISBN: 978-92-61-30412-6

Publié en Suisse
Genève, 2020
Crédits photos: Shutterstock