ITU Publications

Union Internationale des Télécommunications
Bureau de Développement des Télécommunications

Lignes directrices sur la protection en ligne des enfants à l'intention des parents et des éducateurs

2020

Lignes directrices sur la protection en ligne des enfants à l'intention des parents et des éducateurs

2020

Remerciements

Les présentes lignes directrices ont été élaborées par l'Union internationale des télécommunications (UIT) avec le concours d'un groupe de travail d'auteurs collaborateurs issus des principales organisations actives dans le secteur des technologies de l'information et de la communication (TIC) et dans les domaines concernant la protection (en ligne) des enfants, à savoir:

ECPAT International, réseau "Global Kids Online", International Disability Alliance, Union internationale des télécommunications (UIT), London School of Economics and Political Science, Internet matters, Parent Zone International et UK Safer Internet Centres/SWGfL.

La réunion du groupe de travail s'est tenue sous la présidence de Karl Hopwood (Insafe network of Safer Internet Centres (Insafe))[1] et a été coordonnée par Fanny Rotino (UIT).

Une précieuse contribution a également été apportée par le réseau COFACE-Families Europe, la Commissaire australienne à la sécurité en ligne, la Commission européenne, le Conseil de l'Europe, le Groupe e-Worldwide (e-WWG), l'ICMEC (Centre international pour les enfants disparus et exploités) et le programme Youth and Media du Berkman Klein Center for Internet and Society à l'Université de Harvard, ainsi que par certains gouvernements nationaux et des parties prenantes du secteur privé qui ont pour objectif commun de faire de l'Internet un lieu plus sûr et sans danger pour les enfants et les jeunes.

L'établissement des présentes lignes directrices n'aurait pas été possible sans les efforts, l'enthousiasme et l'engagement des auteurs collaborateurs.

L'UIT remercie les rédacteurs énumérés ci-après (par ordre alphabétique des organisations qu'ils représentent) pour leur précieuse contribution en temps et en réflexion:

- Julia Fossi et Ella Serry (Commissaire australienne à la sécurité en ligne)
- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Conseil de l'Europe)
- John Carr (ECPAT International)
- Manuela Marta (Commission européenne)
- Salma Abbasi (e-WWG)
- Laurie Tasharski (ICMEC)
- Lucy Richardson (International Disability Alliance)
- Carolyn Bunting (Internet matters)
- Fanny Rotino (UIT)
- Sonia Livingstone (London School of Economics et Global Kids Online)
- Cliff Manning et Vicki Shotbolt (Parent Zone International)
- David Wright (UK Safer Internet Centres/SWGfL)
- Sandra Cortesi (Youth and Media)

[1] Dans le cadre du mécanisme pour l'interconnexion en Europe (MIE), le réseau European Schoolnet déploie, au nom de la Commission européenne, la plateforme Better Internet for Kids, chargée entre autres de coordonner le réseau Insafe des European Safer Internet Centres ("centres européens pour un Internet plus sûr"). De plus amples informations sont disponibles sur la page suivante: www.betterinternetforkids.eu.

ISBN

978-92-61-30142-2 (version papier)

978-92-61-30472-0 (version électronique)

978-92-61-30132-3 (version EPUB)

978-92-61-30482-9 (version Mobi)

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

Avant-propos

L'UIT a élaboré son tout premier ensemble de lignes directrices sur la protection en ligne des enfants en 2009. Notre objectif était alors de créer un cadre convenu au niveau international à l'intention des différentes parties prenantes (parents et éducateurs, secteur privé, décideurs et enfants), afin de permettre aux plus jeunes d'utiliser l'Internet en toute sécurité, dans la joie et la confiance.

Depuis lors, l'Internet a évolué au-delà de l'imaginable. Il est devenu une mine de ressources infiniment plus riche pour les enfants, qui leur donne accès à une large gamme de jeux éducatifs et d'activités de loisirs et leur offre de nombreuses façons de partager, d'apprendre et de se mettre facilement en lien avec des amis, des membres de leur famille et le monde extérieur. Mais dans le même temps, il est également devenu un environnement bien plus dangereux pour les enfants, où ils ne peuvent s'aventurer sans être accompagnés.

Les nombreux risques et difficultés auxquels les enfants – et les personnes qui s'occupent d'eux – peuvent être confrontés comprennent les atteintes à la vie privée, les fausses informations, les trucages vidéo, mais aussi l'accès à des contenus violents et inappropriés, la piraterie en ligne et la menace de manipulation psychologique en ligne à des fins sexuelles (*grooming*) ainsi que l'abus et l'exploitation sexuels en ligne.

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

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

À l'intention des utilisateurs de ces lignes directrices, nous avons cherché à faire connaître les principaux enjeux dans ce domaine et à fournir des ressources qui leur permettront d'aider efficacement les enfants et les jeunes à interagir dans le monde en ligne. Ces lignes directrices contribueront à sensibiliser les lecteurs aux risques et menaces potentielles, ainsi qu'à instaurer un environnement numérique sain et formateur dans les foyers comme dans les salles de classe. Elles insistent également sur le fait qu'il est important de communiquer ouvertement et de dialoguer constamment avec les enfants pour créer un espace sûr où les jeunes utilisateurs se sentent libres d'exprimer leurs inquiétudes.

Cette nouvelle édition aborde les évolutions récentes des technologies et plates-formes numériques, mais comble également une lacune de taille en traitant de la situation des enfants handicapés, pour qui l'Internet constitue un moyen essentiel de participer et de s'intégrer

pleinement à la société. Les besoins particuliers des enfants migrants et des enfants issus d'autres groupes vulnérables ont également été pris en considération.

Conformément à l'esprit de l'UIT et à son rôle en tant qu'organisation internationale, je suis fière de pouvoir dire que ces lignes directrices révisées sont le fruit d'une collaboration mondiale, puisqu'elles ont été corédigées par des experts provenant d'une vaste communauté multi-parties prenantes.

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

À une période où de plus en plus de jeunes rejoignent la communauté en ligne, ces lignes directrices revêtent plus d'importance que jamais. Les parents et les éducateurs, le secteur privé, les décideurs – sans parler des enfants eux-mêmes – ont tous un rôle vital à jouer pour assurer la sécurité en ligne des enfants. J'espère que ces lignes directrices sauront vous aider pour accompagner les enfants placés sous votre responsabilité dans ce voyage extraordinaire à la découverte des innombrables possibilités que l'Internet a à nous offrir.

Doreen Bogdan-Martin
Directrice du Bureau de développement des télécommunications

Table des matières

Liste des tableaux et figures

Tableaux

Figures

Résumé analytique

D'après les données de l'UIT, on a estimé que 4,1 milliards de personnes utilisaient l'Internet en 2019, soit une augmentation de 5,3% par rapport aux estimations de 2018.

Les enfants et les jeunes se servent de l'Internet à diverses fins, telles que la recherche d'informations dans le cadre d'un projet scolaire ou la conversation avec un ami. Ils ont une excellente maîtrise des programmes et des applications complexes et de la connexion à l'Internet via un téléphone mobile, une tablette ou d'autres dispositifs portables (montres, iPods Touch, liseuses de livres numériques, consoles de jeu, etc.)[1].

L'Internet constitue également un outil important dans la vie de différents groupes d'enfants et de jeunes vulnérables. Il permet aux enfants migrants d'entretenir un lien avec leur famille et leurs amis et représente une fenêtre sur la culture de leur nouveau pays. Pour les enfants et les jeunes handicapés, il représente la possibilité de se socialiser et de participer à des activités qui ne leur sont pas accessibles hors ligne, ainsi que d'échanger en ligne avec leurs pairs sur un pied d'égalité, en mettant en avant leurs compétences plutôt que leurs handicaps.

Toutefois, bien que l'Internet soit un lieu de découverte et d'opportunités, il comporte également des risques et des dangers, auxquels certains enfants sont plus exposés que d'autres. Par exemple, en ce qui concerne les enfants et les jeunes migrants, les conséquences de la divulgation en ligne d'informations confidentielles peuvent s'avérer catastrophiques: dans de mauvaises mains, ces données peuvent être utilisées pour recenser et cibler des personnes sur la base de leur appartenance ethnique, de leur statut migratoire ou d'un autre marqueur d'identité[2]; pour ce qui est des enfants et des jeunes touchés par des troubles du spectre autistique (TSA), les difficultés sociales telles que le manque de compréhension des intentions d'autrui peuvent rendre ce groupe vulnérable à des "amis" malintentionnés; et les enfants et jeunes handicapés sont plus exposés à l'exclusion, la stigmatisation et la manipulation.

De nombreux parents et tuteurs croient à tort qu'il est plus sûr pour leurs enfants d'utiliser un ordinateur à la maison, ou à l'école, qu'à l'extérieur. Cette fausse idée est dangereuse, car via l'Internet, les enfants et les jeunes peuvent accéder virtuellement à n'importe quel endroit du monde, et ce faisant, ils peuvent être exposés à des risques potentiellement dangereux, de la même manière que dans le monde physique. Le risque de subir un préjudice est toutefois légèrement accru lorsque les enfants et les jeunes se connectent à l'Internet sur un smartphone, une tablette ou d'autres dispositifs portables. En effet, ce type d'appareils donne un accès instantané à l'Internet depuis n'importe quel endroit et est plus difficile à surveiller par les parents ou les personnes s'occupant d'enfants.

Les présentes lignes directrices ont été élaborées dans le cadre de l'initiative Protection en ligne des enfants (COP, *child online protection*), au sein du Programme mondial cybersécurité de l'UIT[3], dans le but d'établir les fondations d'un cyberespace sans danger pour les jeunes d'aujourd'hui, mais aussi pour les générations à venir. Elles portent également sur les enfants vulnérables, en particulier les enfants migrants, les enfants atteints de TSA et les enfants handicapés.

1 UIT (2019), *Measuring digital development: Facts and figures 2019*, (Mesurer le développement numérique: faits et chiffres 2019) https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.
2 UNICEF (2017), *La situation des enfants dans le monde 2017: Les enfants dans un monde numérique*, https://www.unicef.org/uzbekistan/media/711/file/SOWC:%20Children%20in%20a%20Digital%20World.pdf.
3 UIT (2020), *Programme mondial cybersécurité (GCA)*, https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

Elles sont destinées à servir de prototype pouvant être adapté et utilisé en cohérence avec les lois et coutumes nationales ou locales et abordent les problèmes que peuvent rencontrer tous les enfants et jeunes de moins de 18 ans.

La convention des Nations Unies relative aux droits de l'enfant définit un enfant comme étant une personne de moins de 18 ans. Les présentes lignes directrices traitent des problématiques qui touchent toutes les personnes âgées de moins de 18 ans dans toutes les régions du monde. Cependant, un internaute de 7 ans n'aura pas les mêmes besoins ni les mêmes centres d'intérêt qu'un jeune collégien de 12 ans ou qu'un adolescent de 17 ans à l'aube de sa majorité. Ces lignes directrices ont été conçues pour fournir des conseils ou des recommandations dans différents contextes, car il convient d'apporter une attention particulière aux besoins spécifiques des enfants, et parce que les différents facteurs locaux, juridiques et culturels ont une grande incidence sur la façon dont ces lignes directrices peuvent être utilisées ou interprétées dans un pays ou une région donnés.

1 Introduction

Au niveau mondial, un internaute sur trois est âgé de moins de 18 ans[4] – chiffre édifiant puisqu'en 2018, plus de la moitié de la population mondiale utilisait l'Internet. Dans les pays en développement, les enfants sont les premiers utilisateurs de l'Internet: ils grandissent avec et se connectent souvent pour la première fois via un téléphone mobile[5].

Étant donné qu'un nombre croissant d'enfants dans le monde a accès à l'Internet, le respect de leurs droits dépendra de plus en plus de l'environnement numérique. L'accès à l'Internet est fondamental pour la réalisation des droits de l'enfant.

Alors qu'un enfant sur trois utilise l'Internet, environ 346 millions d'enfants dans le monde ne sont toujours pas connectés[6]. Les enfants qui pourraient retirer le plus de bénéfices des possibilités offertes par l'Internet sont souvent ceux qui n'y ont pas accès. Dans la région Afrique, on constate que près de 60 pour cent des enfants ne sont pas connectés, alors qu'en Europe, la proportion est de 4 pour cent[7].

En termes d'accès à l'Internet, on constate également d'importantes différences entre les filles et les garçons. Des recherches[8] ont montré que dans toutes les régions, sauf la région des Amériques, le nombre d'internautes masculins est supérieur au nombre d'internautes féminins. Dans beaucoup de pays, les filles n'ont pas les mêmes possibilités d'accès que les garçons, et lorsque c'est le cas, elles sont souvent surveillées et soumises à des restrictions d'usage bien plus importantes.

Mais la fracture numérique ne porte pas sur la seule question de l'accès. Les enfants qui se connectent via un téléphone mobile plutôt que sur un ordinateur ont tendance à vivre une expérience en ligne de moindre qualité, et ceux qui disposent de compétences numériques insuffisantes ou parlent une langue minoritaire n'arrivent souvent pas à obtenir des contenus pertinents en ligne. Les enfants des zones rurales sont davantage exposés à la pratique du vol de mots de passe ou d'argent. En outre, ils ont généralement moins de compétences numériques, passent plus de temps en ligne (en particulier pour jouer à des jeux) et font l'objet d'une médiation et d'un contrôle parentaux moins soutenus[9].

La fracture numérique est une préoccupation actuelle, tant pour les enfants que pour les adultes, et pour en venir à bout, il est nécessaire de consentir des investissements ciblés et de trouver des solutions créatives. Dans ce contexte, le nombre d'enfants connectés ne cesse d'augmenter, mais ils sont nombreux à ne pas bénéficier d'une orientation appropriée de la part de leurs parents, professeurs ou autres adultes concernés. Cette situation participe à la mise en danger des enfants.

---

4 Livingstone S., Carr J. et Byrne J. (2015) *One in three: The task for global internet governance in addressing children's rights*. Global Commission on Internet Governance: Paper Series. Londres: CIGI et Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

5 UIT (2020), *Mesurer la société de l'information*, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

6 UNICEF (2017), La situation des enfants dans le monde 2017: Les enfants dans un monde numérique, https://www.unicef.org/uzbekistan/media/711/file/SOWC:%20Children%20in%20a%20Digital%20World.pdf.

7 UNICEF.

8 Araba Sey et Nancy Hafkin (2019), Rapport du groupe de recherches EQUALS, élaboré par l'université des Nations Unies (université des Nations Unies et Partenariat mondial EQUALS), https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf.

9 UNICEF (2019). *Growing up in a connected world*. UNICEF Centre de recherches Innocenti de l'UNICEF, Florence, https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf.

L'Internet est devenu un outil technologique extrêmement enrichissant et formateur. Les enfants et les jeunes en sont les premiers bénéficiaires et profitent aussi des technologies numériques qui lui sont associées. Ces techniques ont transformé notre façon de communiquer et démultiplié les nouvelles façons de jouer, d'écouter de la musique et de se livrer à toutes sortes d'activités culturelles et d'échanges, par-delà les frontières. Les enfants peuvent élargir leur horizon en ligne, en tirant parti de la possibilité d'obtenir des informations et d'entretenir des relations. L'accès aux technologies de l'information et de la communication (TIC) donnent aux enfants des compétences élémentaires qui étayent les autres formes de participation hors ligne. L'Internet offre un accès à la santé, à des services éducatifs et à des informations sur des sujets qui sont importants pour les jeunes, mais qui peuvent être tabous dans leur société. Les enfants et les jeunes sont très souvent en première ligne lorsqu'il s'agit de s'adapter aux nouvelles possibilités offertes par l'Internet et de les adopter.

Nul ne peut ignorer toutefois que l'Internet a généré dans son sillage divers problèmes relatifs à la sécurité des enfants et des jeunes auxquels il convient de remédier, non seulement parce qu'ils peuvent avoir des répercussions considérables, mais aussi parce qu'il est important de faire savoir à toutes les personnes concernées que l'Internet est un média dans lequel on peut avoir confiance. De la même façon, il est essentiel que la volonté de protéger les enfants et les jeunes en ligne ne devienne pas une excuse pour justifier des atteintes à la liberté de parole, d'expression ou d'association.

Il est de la plus haute importance que la nouvelle génération utilise l'Internet en toute confiance pour pouvoir, à son tour, continuer de profiter de son évolution. Un équilibre doit donc impérativement être trouvé au sujet de la sécurité des enfants et des jeunes en ligne.

Il est fondamental de discuter ouvertement avec les enfants et les jeunes des risques auxquels ils sont exposés en ligne et de leur apprendre à les reconnaître, ainsi qu'à prévenir et à gérer les préjudices, pour autant que ceux-ci soient matérialisés, sans toutefois exagérer les dangers ni générer des craintes infondées.

L'approche qui consiste à présenter exclusivement ou essentiellement les aspects négatifs de la technologie n'aura que très peu de chances d'être prise au sérieux par les enfants et les jeunes. Les parents et les enseignants ont souvent une longueur de retard car les jeunes en savent généralement plus sur la technologie et ses possibilités que les générations antérieures. Des recherches ont montré que la plupart des enfants sont capables de faire la distinction entre le harcèlement et les vexations ou brimades en ligne, et reconnaissent que le harcèlement en ligne est malveillant. Dans de nombreux pays, les enfants comprennent d'ailleurs très bien certains des risques auxquels ils sont exposés en ligne[10].

Toutefois, bien que les efforts visant à apprendre aux enfants à gérer les risques en ligne semblent efficaces, de nombreux enfants dans le monde doivent encore être sensibilisés, en particulier au sein des groupes vulnérables, et des efforts concertés doivent se concentrer sur ces enfants, notamment pour les informer de l'existence de services d'aide aux victimes de harcèlement en ligne ainsi que des autres formes de risques que présente le cyberespace.

Il reste encore de nombreux défis à relever, outre la question de l'accès à l'environnement connecté. La rapidité d'évolution des technologies est problématique du point de vue

[10] Depuis 2016, l'UIT mène des consultations dans le cadre de l'initiative COP avec un certain nombre de parties prenantes, enfants et adultes, concernant des sujets importants tels que le harcèlement en ligne, la maîtrise du numérique et les activités des enfants en ligne.

de la sécurité des enfants en ligne. Nombreux sont les enfants qui naviguent au sein d'un environnement numérique complexe. Les avancées dans des domaines tels que l'intelligence artificielle et l'apprentissage automatique, la réalité virtuelle et augmentée, les mégadonnées, la reconnaissance faciale, la robotique et l'Internet des objets vont transformer encore davantage l'utilisation que les enfants font des médias.

Il est indispensable que toutes les parties prenantes anticipent et étudient les conséquences de ces évolutions pour les enfants, et trouvent des moyens de les aider à se doter des compétences numériques nécessaires non seulement pour survivre, mais aussi pour s'épanouir dans le monde numérique de demain. Il faudra investir davantage pour transmettre aux parents et aux enseignants les connaissances et les compétences numériques minimales qui leur permettront d'aider les enfants à développer leur esprit critique et leur capacité d'évaluation pour naviguer dans des flux d'informations rapides et de qualité variable, dans le but qu'aussi bien les parents et les éducateurs que les enfants deviennent des citoyens numériques[11].

Les consultations menées par l'UIT ont montré que certains pays peinent à allouer des ressources suffisantes pour s'atteler à la question de la maîtrise du numérique et à la sécurité des enfants en ligne. Cependant, d'après les enfants, les parents, les enseignants, les entreprises du secteur des technologies et les gouvernements ont tous un rôle important à jouer dans l'élaboration de solutions permettant d'assurer leur sécurité en ligne. Une enquête menée par l'UIT auprès des États Membres indique qu'il existe une réelle volonté d'améliorer le partage de connaissances et de déployer des efforts coordonnés pour assurer la sécurité d'un plus grand nombre d'enfants en ligne.

Trouver un équilibre entre les possibilités offertes aux enfants par l'Internet et les risques que son utilisation comporte reste un défi. Les États Membres de l'UIT ont également fait savoir que, même si les efforts visant à promouvoir les possibilités en ligne pour les enfants doivent rester une priorité, il convient d'accorder une attention équivalente au droit de participer au monde numérique et d'en tirer profit en toute sécurité[12].

[11] Conseil de l'Europe (2016), *Éducation à la citoyenneté numérique,* https://www.coe.int/en/web/digital-citizenship-education/home.

[12] ITU News (2018), *Celebrating 10 Years of Child Online Protection,* https://news.itu.int/celebrating-10-years-child-online-protection/.

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

Les technologies en ligne offrent aux enfants et aux jeunes de nombreuses possibilités de communiquer, d'acquérir de nouvelles compétences, de donner libre cours à leur créativité et de contribuer à l'édification d'une société meilleure. Mais elles peuvent aussi être porteuses de nouveaux risques, comme l'exposition aux atteintes à la vie privée, à des contenus illicites, au harcèlement, à la cyberintimidation, à l'utilisation abusive des données personnelles, à la manipulation psychologique et même aux abus sexuels sur les enfants.

Les présentes lignes directrices définissent une approche générale visant à répondre à toutes les menaces et préjudices potentiels que les enfants et les jeunes peuvent rencontrer au cours de l'acquisition de compétences numériques. Elles mettent en avant le fait que tous les acteurs concernés ont un rôle à jouer en ce qui concerne leur résilience numérique et leur bien-être et protection en ligne, lorsqu'ils profitent des possibilités offertes par l'Internet.

La protection des enfants est une responsabilité commune et il appartient à toutes les parties prenantes de garantir un avenir durable pour tous. Pour ce faire, les décideurs, le secteur privé, les parents, les personnes s'occupant d'enfants, les éducateurs et autres acteurs doivent veiller à ce que les enfants puissent réaliser tout leur potentiel – en ligne et hors ligne.

Les parents, les tuteurs et les éducateurs ont également la responsabilité de s'assurer que les enfants et les jeunes utilisent les sites Internet de manière sûre et responsable.

Ces dernières années, l'accès à l'Internet mobile a considérablement augmenté et il n'existe pas de solution miracle pour garantir la protection en ligne des enfants et des jeunes. Il s'agit d'une problématique mondiale, qui appelle une solution globale provenant de tous les secteurs de la société, y compris les enfants et les jeunes eux-mêmes.

Afin de répondre aux défis croissants soulevés par l'évolution rapide des TIC, l'initiative pour la protection en ligne des enfants (COP)[13], une initiative internationale multi-parties prenantes lancée par l'UIT en novembre 2008, continue de rassembler des partenaires de tous les secteurs de la communauté mondiale afin de donner aux enfants et aux jeunes du monde entier les moyens de naviguer en toute sécurité sur l'Internet. Dans ce cadre, des lignes directrices ont été élaborées à l'intention de toutes les parties prenantes concernées, y compris les enfants et les jeunes du monde entier, sur la manière d'agir pour leur propre sécurité en ligne et celle des autres. Ces lignes directrices sont conçues pour servir de prototype pouvant être adapté et utilisé dans le respect des coutumes et des lois nationales et locales.

Le présent rapport a été établi dans le cadre de l'initiative COP par un groupe de travail composé d'experts multi-parties prenantes, et a pour objectif de fournir des informations, des avis et des conseils en matière de sécurité aux parents, tuteurs et éducateurs concernant la protection en ligne des enfants.

Un groupe de travail d'experts de l'UIT a participé à la rédaction des lignes directrices que constitue le présent rapport, en s'appuyant sur la première version des lignes directrices de l'UIT sur la protection en ligne des enfants, publiée en 2009 et mise à jour en 2016. À la demande des États Membres de l'UIT, l'UIT a entamé en 2019 un processus de révision visant à élaborer une deuxième version des lignes directrices.

[13] UIT (2020), Child Online Protection, https://www.itu.int/en/cop/Pages/default.aspx.

Ces nouvelles lignes directrices abordent la situation particulière des enfants handicapés en ce qui concerne les risques et les dangers en ligne, ainsi que des problématiques liées aux nouvelles avancées technologiques telles que l'Internet mobile, les applications, l'Internet des objets, les jouets connectés, les jeux en ligne, la robotique, l'apprentissage automatique et l'intelligence artificielle.

3 Les enfants et les jeunes dans un monde connecté[14]

Au niveau mondial, on estime qu'un enfant sur trois utilise l'Internet et qu'un internaute sur trois est âgé de moins de 18 ans[15]. En 2017, la moitié de la population mondiale utilisait l'Internet et dans la tranche d'âge des 15 à 24 ans, cette proportion passe à environ deux tiers.

"Nous avons grandi avec l'Internet. Il a toujours été là, avec nous. Pour les adultes, l'Internet c'était vraiment une nouveauté, alors que pour nous, c'est juste normal." Garçon, 15 ans, Serbie.

Chez les enfants et les jeunes, le téléphone portable est le dispositif le plus couramment utilisé pour accéder à l'Internet. Cela constitue l'une des transformations majeures de la dernière décennie. En Europe et en Amérique du Nord, la première génération d'utilisateurs de l'Internet s'est connectée via un ordinateur de bureau, mais dans la plupart des pays en développement, ce sont les internautes mobiles qui ont été les premiers à utiliser l'Internet.

Les enfants et les jeunes préfèrent utiliser le téléphone portable car ils peuvent l'emporter partout et n'ont pas à le partager avec les autres membres du ménage; le téléphone portable peut remplir plusieurs fonctions en même temps (envoi de SMS, appel, consultation et partage de photos, navigation, etc.) et reste toujours allumé.

"Le téléphone est en quelque sorte plus simple. Nous pouvons l'avoir partout avec nous, c'est plus petit et plus facile de travailler dessus. Je préfère [l'utiliser] comme ça, avec les doigts, pas avec le clavier." Fille, 12 ans, Serbie.

Des enquêtes ont montré que parmi les enfants et les jeunes qui ont accès à l'Internet, les filles utilisent tout autant leur téléphone portable que les garçons pour se connecter. On constate cependant que les ordinateurs de bureau sont généralement plus utilisés par les garçons.

Dans la pratique, la plupart des enfants et des jeunes ont accès à l'Internet sur plusieurs appareils, et les garçons ont tendance à utiliser davantage d'appareils que les filles, dans tous les pays étudiés.

En moyenne, les enfants et les jeunes passent environ deux heures par jour en ligne pendant la semaine et environ le double chaque jour du week-end. Certains d'entre eux disent se sentir connectés en permanence. Mais beaucoup d'autres n'ont toujours pas accès à l'Internet chez eux – ou n'y ont qu'un accès limité. Toutefois, les statistiques donnent des résultats très variables et les avis divergent quant au temps que les enfants passent en ligne. Selon une

[14] Ce chapitre est principalement tiré de la source suivante: UNICEF (2019). *Growing up in a connected world*. (Grandir dans un monde connecté) Centre de recherche Innocenti de l'UNICEF, Florence (https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf). Cette recherche exhaustive, qui s'inscrit dans le cadre l'initiative Global Kids Online et comprend des données factuelles d'aussi bonne qualité, a recueilli les voix d'enfants issus de 11 pays et 4 régions, entre 2016 et 2018 (14 733 enfants âgés de 9 à 17 ans). Le rapport se concentre sur les effets positifs des TIC pour les enfants et pose parallèlement la question de savoir à quel moment leur utilisation devient problématique dans la vie des enfants. Toutes les figures du chapitre 4 ci-après proviennent de ce rapport. La méthodologie qualitative et quantitative sur laquelle ces résultats s'appuient est décrite dans le rapport de Livingstone S., Kardefelt Winther D. et Saeed M. (2019) – *Global Kids Online Comparative Report, Innocenti Research Report*, Centre de recherche Innocenti de l'UNICEF, Florence, qui peut être consulté à l'adresse suivante: https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html. Vous trouverez de plus amples informations sur le projet international de recherche Global Kids Online à l'adresse suivante: http://globalkidsonline.net.

[15] Livingstone S., Carr J. et Byrne J. (2015) *One in three: The task for global internet governance in addressing children's rights*. Global Commission on Internet Governance: Paper Series. Londres: CIGI et Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

étude récente du DQ Institute, en Australie, les enfants et les jeunes passeraient jusqu'à 38 heures par semaine en ligne[16].

"Je vais dans un café parce que nous n'avons pas d'ordinateur à la maison... Nous n'avons pas accès à l'Internet à l'école." Garçon, 15-17 ans, Afrique du Sud.

"[Je suis connecté] toute la journée, mais ça ne veut pas dire que j'utilise Internet toute la journée." Garçon, 13-14 ans, Argentine.

Malgré les conclusions des recherches de Global Kids Online (GKO), selon lesquelles, dans l'ensemble, le nombre de filles et de garçons ayant accès à l'Internet est similaire, dans certains pays, les garçons peuvent se connecter à l'Internet plus librement que les filles, et ces dernières sont plus souvent surveillées et soumises à des restrictions d'usage.

Tout un monde de divertissement

Les enfants et les jeunes se connectent la plupart du temps pour avoir accès à des activités positives et agréables. Dans les onze pays étudiés, l'activité la plus populaire – tant pour les filles que pour les garçons – est le visionnage de clips vidéo. Plus des trois quarts des enfants et des jeunes qui utilisent l'Internet affirment regarder des vidéos en ligne au moins une fois par semaine, seuls ou avec des membres de leur famille.

"Quand ma mère a acheté l'ordinateur portable, nous avons commencé à passer plus de temps ensemble; chaque week-end, nous choisissions un film et le regardions avec ma grand-mère." Fille, 15 ans, Uruguay.

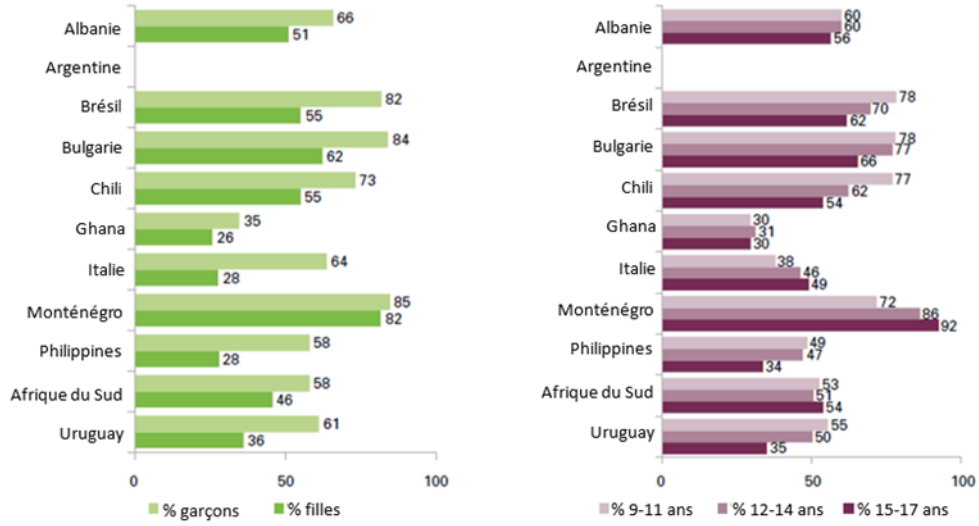
Les enfants et les jeunes aiment également jouer en ligne, et exercent ainsi leur droit de jouer et parfois leur droit d'apprendre. Dans tous les pays étudiés, ce sont les garçons les plus enclins à jouer à des jeux en ligne, mais de nombreuses filles utilisatrices de l'Internet y jouent également: par exemple, cela concerne une majorité de filles en Bulgarie (60%) et au Monténégro (80%). Comme pour le visionnage de vidéos, les enfants et les jeunes tendent davantage à jouer à des jeux en ligne lorsqu'ils peuvent accéder facilement à l'Internet.

"Je joue à des jeux en ligne et ça me permet de gagner de l'argent." Garçon, 17 ans, Philippines.

Les adultes sont préoccupés par le fait que les enfants et les jeunes passent trop de temps sur l'écran ou estiment qu'ils perdent leur temps avec les divertissements en ligne. Selon Global Kids Online, ces activités de divertissement grand public peuvent offrir des possibilités utiles aux enfants et aux jeunes pour débuter dans un domaine, et ainsi les aider à élargir leurs centres d'intérêt et à améliorer leurs compétences pour se lancer dans d'autres expériences en ligne plus approfondies sur le plan éducatif, informatif ou social.

[16] DQ Institute (2020), Child Safety Index, https://www.dqinstitute.org/child-online-safety-index/.

Figure 1: Enfants (%) qui jouent à des jeux en ligne au moins une fois par semaine, par sexe et par âge[17]



Question C4z-aa: Combien de fois avez-vous joué à des jeux en ligne, seul ou avec d'autres personnes, au cours du mois écoulé? Base: Tous les enfants qui utilisent l'Internet.

Question C4z-aa: Combien de fois avez-vous joué à des jeux en ligne, seul ou avec d'autres personnes, au cours du mois écoulé? Base: Tous les enfants qui utilisent l'Internet.

Origine: UNICEF

Établir de nouvelles connexions

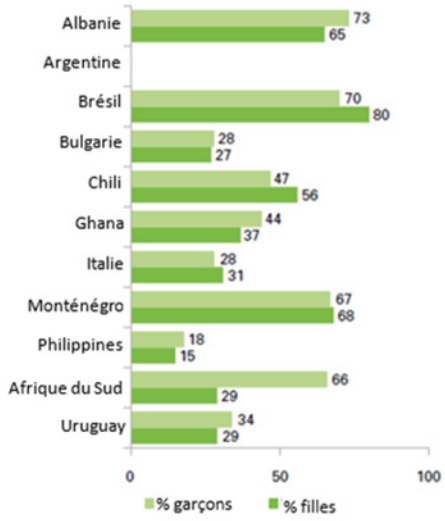
Avec ses outils de messagerie instantanée et ses réseaux sociaux, l'Internet est devenu un point de rencontre essentiel où les enfants et les jeunes peuvent exercer leur droit à la liberté d'expression en se connectant avec leurs amis et les membres de leur famille, ainsi qu'avec d'autres enfants et jeunes partageant les mêmes intérêts. Dans les 11 pays sondés, on peut estimer que de nombreux enfants et jeunes sont "socialement actifs", dans la mesure où ils participent chaque semaine à une série d'activités sociales en ligne, comme la conversation instantanée avec des amis et des membres de la famille, l'utilisation de divers outils de messagerie et la mise en réseau avec des personnes ayant des intérêts similaires. Certains enfants déclarent également qu'il leur est plus facile d'exprimer leur véritable personnalité en ligne.

"En ligne, je peux me montrer sous mon vrai jour, il n'y a pas de règles... J'ai plus de 5 000 amis en ligne". Garçon qui se définit comme étant homosexuel, 15 ans, Philippines.

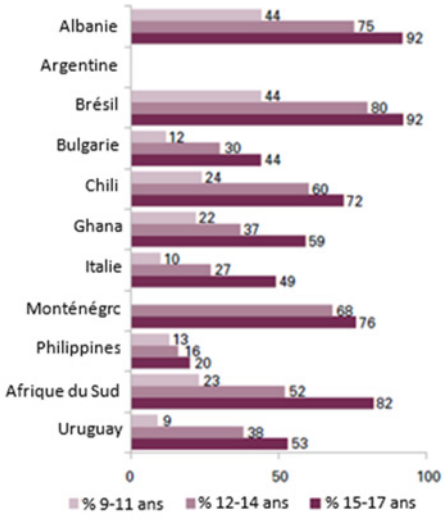
Les interactions sociales en ligne augmentent également avec l'âge pour plusieurs raisons. Par exemple, certains sites de réseaux sociaux fixent un âge minimum pour l'inscription d'enfants et de jeunes, qui acquièrent généralement plus de liberté avec l'âge.

[17] Cette figure provient de: UNICEF (2019), *Growing up in a connected world* (Grandir dans un monde connecté), Centre de recherche Innocenti de l'UNICEF, Florence, https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf.

Figure 2: Enfants (%) qui effectuent trois activités sociales en ligne ou plus, au moins une fois par semaine, par sexe[18]



Question C4: Combien de fois vous êtes-vous livré(e) à ces activités sociales en ligne au cours du mois écoulé? Base: Tous les enfants qui utilisent l'Internet.



Question C4: Combien de fois vous êtes-vous livré(e) à ces activités sociales en ligne au cours du mois écoulé? Base: Tous les enfants qui utilisent l'Internet.

Note: On a demandé aux enfants et aux jeunes de préciser combien de fois ils avaient participé aux activités sociales en ligne ci-après au cours du mois écoulé: conversation avec des personnes résidant ailleurs ou provenant d'un milieu différent; visite d'une plateforme de réseau social; échange avec des membres de la famille ou des amis vivant loin; utilisation d'une messagerie instantanée; connexion à un site web où les utilisateurs partagent leurs intérêts ou leurs passe-temps.

Origine: UNICEF

Il ressort clairement des données ci-dessus que l'Internet ouvre de nouvelles perspectives en matière de socialisation, bien que les parents se plaignent souvent du fait que les interactions en ligne des enfants et des jeunes se font au détriment des échanges en personne dans le monde physique.

"Dans une fête, ils sont assis à une table, et tous les dix ont leur petit appareil dans les mains." Parent d'un adolescent âgé de 15 à 17 ans, Chili.

On constate néanmoins que ce type de comportement n'est pas spécifique aux enfants et aux jeunes. Certains parents téléphonent ou naviguent sur l'Internet pendant des réunions sociales, ce qui dérange beaucoup d'enfants et de jeunes.

"À table, quand nous mangeons, et que papa utilise son téléphone. C'est le seul moment où nous sommes tous ensemble, et cela m'agace vraiment." Fille, 14 ans, Uruguay.

Avec un meilleur accès à l'Internet, les enfants et les jeunes peuvent élargir leurs horizons, recueillir des informations et tisser de nouvelles relations. En multipliant les interactions sociales, que ce soit en ligne ou en personne, ils acquièrent de l'expérience et des compétences. Les recherches menées par GKO montrent que les enfants et les jeunes qui ont une vie sociale

[18] Cette figure provient de: UNICEF (2019), *Growing up in a connected world* (Grandir dans un monde connecté), Centre de recherche Innocenti de l'UNICEF, Florence, https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf.

plus active sur l'Internet gèrent mieux leur vie privée en ligne, ce qui contribue à préserver leur sécurité.

La joie de créer

Certains des contenus en ligne que les enfants et les jeunes trouvent et apprécient ont été produits par leurs pairs. En général, dans les onze pays étudiés par Global Kids Online, 10 à 20% des enfants et des jeunes créent et mettent en ligne leurs vidéos ou créations musicales, écrivent un blog ou des histoires, ou créent des pages web, chaque semaine.

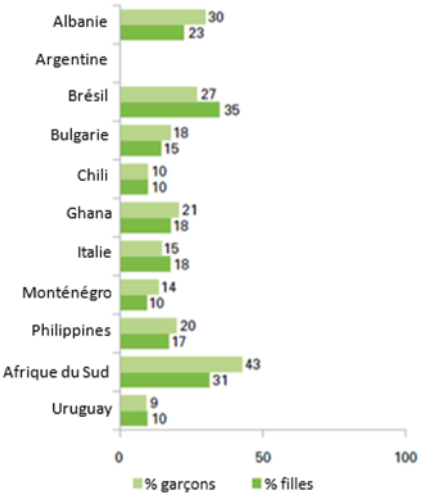
"J'ai un blog et je le mets régulièrement à jour." Fille, 15-17 ans, Philippines.

"On peut partager des vidéos et des jeux. On peut partager de la musique. On peut aussi partager des photos, des idées, des jeux." Fille, 9-11 ans, Ghana.

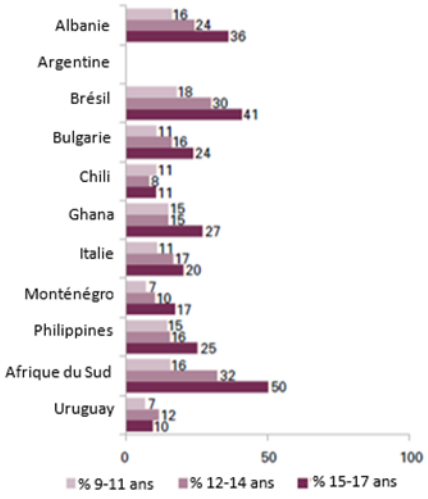
"Je fabrique moi-même des cartes et je les mets en ligne. Mes amis les aiment bien." Fille, 15-17 ans, Philippines.

"Oui, je sais comment [pirater des ordinateurs], mais j'ai arrêté." Garçon, 15-17 ans, Philippines.

Figure 3: Enfants (%) qui effectuent une activité créative en ligne ou plus, au moins une fois par semaine, par sexe et par âge[19]



Question C4m-n: Combien de fois vous êtes-vous livré(e) à des activités créatives en ligne au cours du mois écoulé? Note: En Uruguay, les activités visées ne comprenaient pas la création de blogs en ligne. Base: Tous les enfants qui utilisent l'Internet.



Question C4m-n: Combien de fois vous êtes-vous livré(e) à des activités créatives en ligne au cours du mois écoulé? Note: En Uruguay, les activités visées ne comprenaient pas la création de blogs en ligne. Base: Tous les enfants qui utilisent l'Internet.

Note: On a demandé aux enfants et aux jeunes d'indiquer combien de fois ils s'étaient livrés aux activités créatives en ligne ci-après au cours du mois écoulé: création et mise en ligne de leur propre vidéo ou création musicale; création d'un blog ou d'histoires, ou d'un site web en ligne; publication de vidéos ou de morceaux de musique créés par quelqu'un d'autre.

Origine: UNICEF

Le goût de l'information

[19] Cette figure provient de: UNICEF (2019), *Growing up in a connected world* (Grandir dans un monde connecté), Centre de recherche Innocenti de l'UNICEF, Florence, https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf.

Comme les adultes, les enfants et les jeunes tirent parti de l'Internet pour exercer leur droit à l'information. Un à deux cinquièmes des enfants et des jeunes peuvent être considérés comme des "chercheurs d'informations", en ce sens qu'ils effectuent chaque semaine de multiples formes de recherche d'informations en ligne, par exemple pour acquérir de nouvelles connaissances, pour chercher des possibilités d'emploi ou d'études, pour s'informer sur l'actualité ou la santé ou pour trouver des événements dans leur quartier.

De nombreux enfants et jeunes de tous âges utilisent l'Internet pour faire leurs devoirs ou pour rattraper des cours.

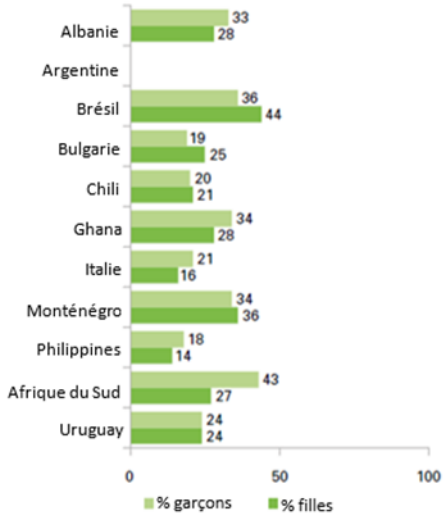
"Ils nous ont demandé de trouver les noms des ministres au Ghana, de faire des recherches sur les pays et leurs monnaies. On peut obtenir des informations sur d'autres pays." Fille, 12-14 ans, Ghana.

"Sur l'Internet, nous pouvons chercher tout ce dont nous avons besoin pour l'école, et que nous ne trouvons pas dans les livres." Fille, 9 ans, Serbie.

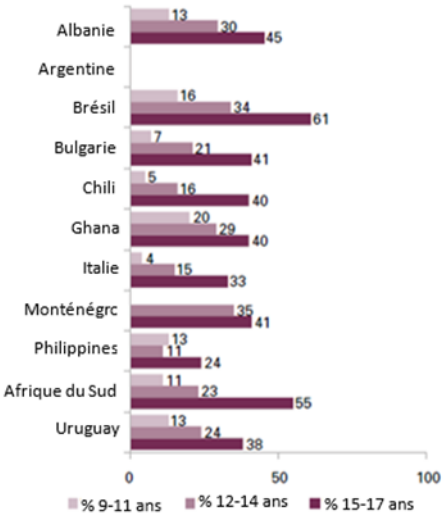
"J'ai eu de mauvais résultats en maths, alors j'ai regardé quelques vidéos qui expliquaient ce que je devais réviser." Garçon, 15-17 ans, Argentine.

"Si on ne va pas à l'école, on peut demander à nos amis ce qu'on a raté et tout ça. Donc, c'est important d'avoir ses amis sur WhatsApp." Fille, 16-17 ans, Afrique du Sud.

Figure 4: Enfants (%) qui effectuent trois activités de recherche d'information en ligne ou plus, au moins une fois par semaine, par sexe et par âge[20]



Question C4: Combien de fois avez-vous effectué des recherches d'informations en ligne au cours du mois écoulé?
Base: Tous les enfants qui utilisent l'Internet.



Question C4: Combien de fois avez-vous effectué des recherches d'informations en ligne au cours du mois écoulé?
Base: Tous les enfants qui utilisent l'Internet.

Note: On a demandé aux enfants et aux jeunes d'indiquer combien de fois ils s'étaient livrés aux activités de recherche d'information ci-après au cours du mois écoulé: acquérir de nouvelles connaissances en faisant des recherches en ligne; chercher des possibilités d'emploi ou d'études; effectuer des travaux scolaires; chercher des ressources au niveau local ou des événements dans leur quartier; s'informer sur

[20] Cette figure provient de: UNICEF (2019), *Growing up in a connected world* (Grandir dans un monde connecté), Centre de recherche Innocenti de l'UNICEF, Florence, https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf.

l'actualité en ligne et chercher des informations sur la santé pour eux-mêmes ou pour quelqu'un d'autre. L'Argentine n'est pas prise en considération pour cause de données manquantes.
Origine: UNICEF

Certains enfants et jeunes sont plus enclins que d'autres à utiliser l'Internet pour rechercher des informations. Les données montrent, d'une part, que les enfants et les jeunes qui utilisent l'Internet pour mener diverses activités de recherche d'informations sont souvent plus âgés et capables de participer à un éventail d'activités en ligne globalement plus large, et d'autre part, qu'ils sont encouragés par leurs parents dans leur utilisation de l'Internet. Cela semble indiquer que lorsque les enfants et les jeunes grandissent en étant convenablement soutenus par leurs parents, ils ont tendance à acquérir plus d'expérience en ligne et à utiliser l'Internet à leur avantage.

Compte tenu de la quantité d'informations disponibles en ligne, les enfants et les jeunes doivent être dotés des compétences nécessaires pour cibler le contenu recherché et vérifier la véracité des informations trouvées.

Il y a peu de différences entre les filles et les garçons sur ce plan: les enfants et les jeunes acquièrent des compétences plus approfondies dans la recherche de contenus en ligne au moment de l'adolescence. Il semblerait que les enfants et les jeunes qui regardent davantage de clips vidéo en ligne ont de meilleures compétences en matière de recherche d'informations, peut-être parce qu'en effectuant plus fréquemment des recherches de contenu en ligne, ils élaborent une méthode de recherche.

La quantité d'informations que les enfants et les jeunes recueillent en ligne, ainsi que leur qualité, dépendent de leurs intérêts et de leur motivation. Mais les résultats de leurs recherches seront également influencés par la quantité d'informations disponibles, qui est plus importante pour les langues les plus répandues. Cela dit, les minorités peuvent également bénéficier des possibilités de recherche d'informations, bien qu'elles soient plus limitées en nombre.

"Parfois, comme personne ne parle notre langue dans cette école, je tape quelque chose en Roumain sur YouTube et j'écoute notre voix, et c'est chouette, je comprends tout." Garçon rom, 12 ans, Serbie.

Être compétent dans la recherche d'informations sur l'Internet est une chose, mais savoir vérifier la véracité des informations trouvées en ligne en est une autre.

"Je regarde les actualités étrangères, parce que j'aime voir le point de vue de différents pays sur une même situation. Une médaille a toujours deux faces. Par exemple, les États-Unis peuvent voir les choses d'une certaine façon, et la Russie peut voir les choses différemment." Fille, 16 ans, Serbie.

Parmi les enfants et jeunes qui ont déclaré avoir de solides compétences en matière de recherche d'informations, seul un petit nombre s'est dit véritablement capable de porter un jugement critique sur les informations qu'ils trouvent.

"Il y a tellement de fausses informations en ligne." Garçon, 15 ans, Philippines.

Dans l'ensemble, il semblerait que les enfants et les jeunes ne tirent pas encore pleinement parti des possibilités de recherche et de vérification des informations en ligne. Pour y parvenir, les jeunes enfants en particulier devront être davantage soutenus par leurs parents, leurs enseignants ou les fournisseurs de services numériques, afin de les encourager et de les aider à faire progresser leurs droits dans le monde numérique.

Devenir des citoyens actifs

Outre la recherche d'informations et la création de contenus, les enfants et les jeunes peuvent également utiliser l'Internet pour participer à des activités civiques ou politiques. D'après la Convention relative aux droits de l'enfant, un enfant a des droits civiques, y compris le droit d'être entendu, de s'exprimer et de rencontrer d'autres personnes. Il ressort toutefois clairement des recherches menées par Global Kids Online que relativement peu d'enfants et de jeunes profitent de toutes les possibilités de participation citoyenne en ligne.

Les jeunes sont les plus susceptibles de s'engager dans la vie politique en ligne.

"La politique ... ce n'est peut-être pas ce qu'elle cherche en premier. Mais ma fille, par exemple, lit des articles à ce sujet sur Facebook." Parent d'une enfant âgée de 13 à 14 ans, Argentine.

"Ils donnent aussi leurs opinions ... sur Twitter ... et c'est dans leurs habitudes." Parent d'un enfant âgé de 15 à 17 ans, Argentine.

Encourir des risques et subir des préjudices

Lorsqu'ils sont en ligne, les enfants et les jeunes sont exposés à de nouveaux risques, qui pourraient leur porter atteinte. Ils peuvent par exemple trouver sur l'Internet des informations sur l'automutilation ou le suicide, mais peuvent aussi être confrontés à des discours haineux ou à des contenus à caractère violent ou sexuel. L'enquête menée par Global Kids Online dans plusieurs pays semble indiquer que les enfants et les jeunes qui participent à un nombre plus important d'activités en ligne ont été confrontés à davantage de risques en ligne, ce qui peut notamment découler de leur exposition accrue ou de leur attitude plus confiante lorsqu'ils naviguent sur l'Internet.

Il est important de rappeler qu'un risque ne conduit pas nécessairement à un préjudice. Les enfants et les jeunes exposés à des risques en ligne peuvent ne pas subir de préjudices s'ils ont les connaissances et la capacité d'adaptation nécessaires pour bien réagir à cette expérience. Il est donc important de déterminer qui, parmi eux, sont les plus vulnérables aux dangers en ligne et dans quelles conditions les risques peuvent se transformer en préjudices, afin d'assurer une protection efficace des enfants et des jeunes en ligne, sans toutefois limiter les possibilités qui leur sont offertes.

Dans l'ensemble, environ 20% des enfants et des jeunes interrogés dans le cadre de l'enquête de Global Kids Online ont déclaré qu'au cours de l'année précédente, ils avaient consulté des sites web ou été témoins de discussions en ligne concernant des personnes qui se faisaient du mal ou se blessaient physiquement, tandis qu'environ 15% des enfants et des jeunes ont accédé à des contenus liés au suicide. L'enquête a également montré que les enfants et les jeunes ont été exposés à des discours haineux.

Au Chili, près de la moitié des adolescents âgés de 15 à 17 ans déclarent avoir été dérangés ou contrariés par un événement survenu sur Internet au cours de l'année écoulée. Lorsqu'on leur a demandé de donner des détails, ils ont évoqué divers problèmes, notamment les escroqueries via Internet, les fenêtres publicitaires incrustées à caractère pornographique, les comportements blessants, les faits divers ou images désagréables ou effrayantes, la discrimination et le harcèlement. En Bulgarie, les enfants et les jeunes sont menacés par des sites web qui encouragent la perte de poids rapide, lesquels ont été consultés par un quart des répondants à l'enquête.

"Il y a des commentaires insultants sur d'autres personnes." Fille, 13-14 ans, Afrique du Sud.

Entre un quart et un tiers des enfants et des jeunes interrogés à ce sujet ont été confrontés à des contenus en ligne à caractère violent ou sexuel, tous types de média confondus. Parfois, les enfants et les jeunes tombent par hasard sur un contenu à caractère sexuel; il arrive également que des amis leur recommandent ce type de contenu ou qu'il leur soit envoyé par d'autres personnes, y compris des inconnus. Certains enfants et jeunes ont déjà demandé des images sexuelles à leurs pairs.

"J'ai été vraiment furieuse quand le type m'a envoyé des photos pornographiques." Fille, 12-14 ans, Ghana.

"Une fois, un inconnu m'a demandé combien je "prenais", c'est-à-dire combien cela lui coûterait d'avoir des rapports sexuels avec moi." Garçon, 16 ans, Philippines.

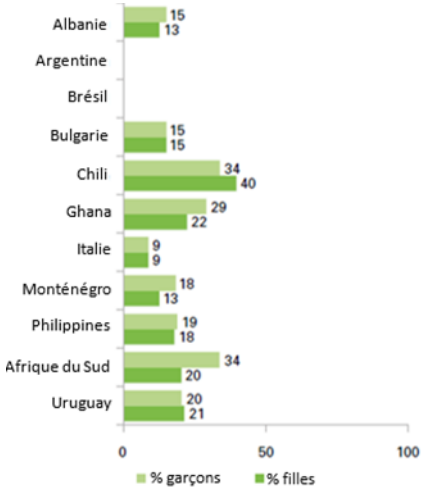
Dans plusieurs pays, beaucoup d'enfants et de jeunes déclarent avoir été exposés à divers risques en ligne, mais ils sont beaucoup moins nombreux à estimer avoir subi des préjudices en conséquence. Les résultats varient selon les pays, mais les jeunes sont relativement plus susceptibles de subir des préjudices que les enfants, probablement parce qu'ils passent plus de temps en ligne et ont tendance à participer à un plus grand éventail d'activités en ligne.

"J'étais sur Instagram et j'ai cliqué sur un commentaire; c'était tellement drôle que je voulais voir les commentaires des autres et j'ai cliqué sur un lien, et soudain il y avait des femmes nues à l'écran." Garçon, 10 ans, Serbie.

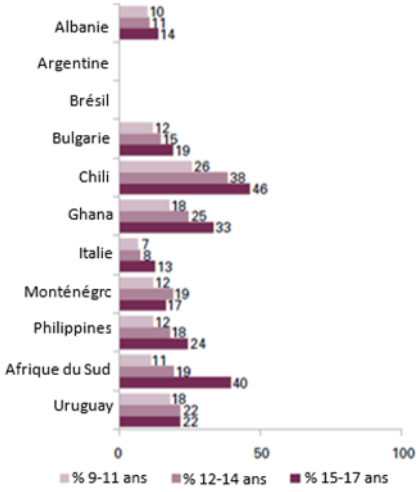
"J'aime les chevaux, tout le monde le sait. Je cherchais des photos pour mon fond d'écran et je suis tombé sur une photo horrible d'un homme en train de découper un cheval." Fille, 10 ans, Serbie.

"J'ai eu très peur... J'ai vu la photo d'un garçon tué par balle." Garçon, 12-14 ans, Ghana.

Figure 5: Enfants (%) ayant subi un préjudice en ligne, par sexe et par âge[21]



Question F11: Au cours de l'année écoulée, vous est-il déjà arrivé quelque chose en ligne qui vous ait dérangé ou contrarié de quelque façon que ce soit (par exemple, mis mal à l'aise, effrayé ou mis face à quelque chose que vous n'auriez pas dû voir)? Base: Tous les enfants qui utilisent l'Internet.



Question F11: Au cours de l'année écoulée, vous est-il déjà arrivé quelque chose en ligne qui vous ait dérangé ou contrarié de quelque façon que ce soit (par exemple, mis mal à l'aise, effrayé ou mis face à quelque chose que vous n'auriez pas dû voir)? Base: Tous les enfants qui utilisent l'Internet.

Origine: UNICEF

Les enfants et les jeunes peuvent être victimes de traitements blessants en ligne et hors ligne. Sur les plates-formes en ligne, les préjudices peuvent comprendre des messages blessants ou méchants, l'exclusion de certaines activités de groupe ou des menaces. Ces expériences sont souvent désignées par le terme "harcèlement en ligne" (*cyberbullying* ou "cyberintimidation"). Mais les enfants et les jeunes peuvent aussi subir ce type de comportements dans le cadre des interactions quotidiennes hors ligne. La part d'enfants et de jeunes victimes d'intimidation en personne et en ligne est à peu près égale.

"Tout le monde s'est mis à taquiner un garçon et à faire des blagues sur lui. Il a fini par quitter le groupe." Garçon, 13-14 ans, Argentine.

"Je crains le harcèlement en ligne parce que cela peut me faire beaucoup de tort au niveau émotionnel." Fille, 14 ans, Uruguay.

Comment les enfants et les jeunes réagissent-ils aux expériences blessantes en ligne? Dans un premier temps, ils se tournent vers leurs amis ou leurs frères et sœurs. Ils en parlent ensuite parfois à leurs parents. Dans les pays étudiés, il est rare que les enfants et les jeunes cherchent du soutien auprès de leurs enseignants. Bien que les jeunes soient exposés à davantage de risques que les enfants, ils ne subissent pas de préjudices plus importants, ce qui porte à croire que l'expérience améliore la capacité de faire face à certaines situations.

Il convient de noter que les enfants et les jeunes ne font pas nécessairement la distinction entre la réalité "en ligne" et "hors ligne". Pour eux, les expériences en ligne – qu'elles soient bonnes ou mauvaises – sont entremêlées avec les autres aspects de leur vie.

Protection de la vie privée: une priorité

[21] Cette figure provient de: Global Kids Online (2019). Global Kids Online: Rapport comparatif, Centre de recherches Innocenti de l'UNICEF.

D'après la Convention des droits de l'enfant, tout enfant a le droit d'être protégé contre une atteinte à sa vie privée. En effet, celle-ci est importante pour parvenir à l'autonomie et l'autodétermination et elle est corrélée à d'autres droits de l'enfant comme le droit à l'information et le droit à la liberté d'expression et d'association. Les enfants et les jeunes peuvent se prémunir contre l'exploitation en protégeant leur vie privée. Ils doivent pour cela gérer attentivement leurs identités numériques et préserver autant que possible leurs données personnelles.

De nombreux enfants et jeunes disent être pleinement capables de protéger leur vie privée dans le cadre de leurs relations interpersonnelles en ligne. Par exemple, ils savent quelles sont les informations qu'ils doivent ou ne doivent pas partager en ligne ou comment modifier les paramètres de confidentialité de leurs comptes de réseaux sociaux ou supprimer des personnes de leurs listes de contacts. On peut donc en déduire que les premiers efforts visant à promouvoir la sécurité des enfants et des jeunes en ligne ont été plutôt fructueux. De nombreux enfants et jeunes ont mis au point des stratégies pour se protéger en ligne et sont conscients qu'ils doivent tenir compte de certains risques lorsqu'ils utilisent l'Internet.

"J'ai un compte Facebook pour mes vrais amis et un autre pour les amis que je rencontre en ligne." Fille, 14 ans, Philippines.

"Quand je suis connectée, je suis moi-même responsable de ce que je fais." Fille, 17 ans, Uruguay.

Par ailleurs, les enfants et les jeunes en ligne peuvent exposer des informations, photographies et communications privées à une utilisation potentiellement abusive et les rendre accessibles à des contacts inappropriés et indésirables, ce qui est plus problématique.

Les enfants et les jeunes peuvent également entrer en lien sur l'Internet avec des personnes qu'ils rencontreront ensuite en personne, mais cela reste relativement rare. Moins d'un quart des enfants et des jeunes dans tous les pays se sont déjà réunis avec une personne qu'ils avaient d'abord connue en ligne.

Il peut être surprenant de constater que, la plupart du temps, les enfants et les jeunes apprécient ces rencontres en personne et déclarent se sentir heureux par la suite – ce qui laisse entendre qu'ils parviennent de cette façon à élargir leur cercle d'amis. Néanmoins, même pour les rares cas où les enfants et les jeunes se disent contrariés par ces rencontres, il y a lieu de s'inquiéter.

Les parents qui mettent en ligne des contenus concernant leurs enfants et leurs adolescents doivent réfléchir à l'incidence que cela peut avoir pour ces derniers. Certains craignent que ce type de pratique – les parents qui partagent des informations et des photos de leurs enfants en ligne ou *sharenting* – puisse porter atteinte à la vie privée d'un enfant, conduire à des formes de harcèlement, lui causer des ennuis ou avoir des conséquences néfastes pour son avenir[22]. Les parents d'enfants handicapés partagent parfois ces informations afin d'obtenir un soutien ou des conseils, et expose ainsi davantage ces enfants à d'éventuelles répercussions négatives.

Le WiFi à la maison

[22] UNICEF et le Centre de recherches Innocenti (2017), Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

L'une des façons d'assurer que les risques en ligne ne causent pas de préjudices aux enfants et aux jeunes est de faire en sorte que les parents et autres adultes soient mieux en mesure d'accompagner les enfants et les jeunes dans leur utilisation de l'Internet.

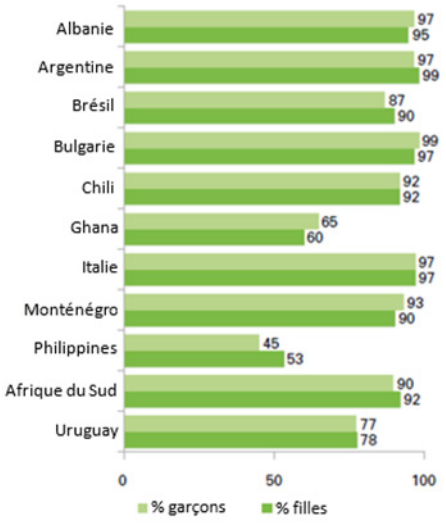
"Les adultes ont beaucoup d'influence sur les jeunes et doivent leur donner un bon exemple à suivre." Fille, 13 ans, Uruguay.

En principe, les parents sont bien placés pour soutenir les enfants et les jeunes dans leur utilisation de l'Internet puisque ces derniers y ont d'abord accès à la maison.

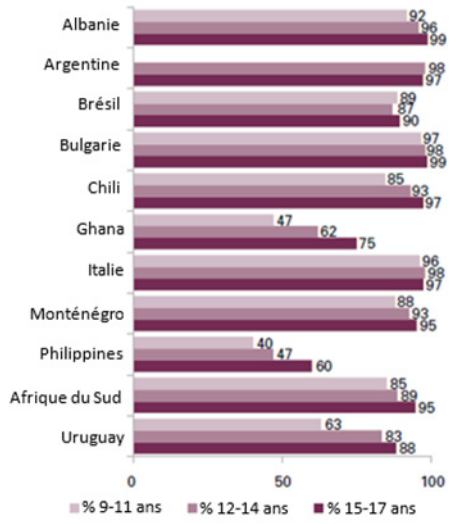
Mais face à la complexification et à l'évolution rapide des technologies, de nombreux parents ne se sentent plus suffisamment à l'aise ou compétents pour encadrer leurs enfants férus de technologie. Les parents sont également influencés par des inquiétudes répandues au sujet du temps passé devant l'écran, de la dépendance à l'Internet et du danger que représentent les inconnus. Les parents ont donc tendance à se concentrer davantage sur les restrictions à imposer à leurs enfants concernant leur utilisation de l'Internet – par exemple, en limitant leur temps en ligne ou en leur interdisant d'utiliser des appareils numériques dans leur chambre, pendant les repas ou après le coucher – plutôt que sur la façon de les accompagner ou de les orienter vers une participation plus productive en ligne.

Dans la plupart des pays, les parents interviennent surtout dans le cadre de l'utilisation de l'Internet des plus jeunes enfants, les aidant à naviguer dans l'environnement numérique, tout en leur imposant davantage de restrictions qu'aux plus âgés. Ils tendent à moins intervenir à mesure que leurs enfants grandissent, alors qu'il serait sans doute bénéfique pour les adolescents de continuer à recevoir des conseils constructifs de la part de leurs parents concernant les possibilités ainsi que les risques de l'Internet.

Figure 6: Enfants (%) qui utilisent l'Internet à la maison, au moins une fois par semaine, par sexe et par âge[23]



Question B6b: Utilisation de l'Internet à la maison, au moins une fois par semaine. Base: Tous les enfants qui utilisent l'Internet.



Question B6b: Utilisation de l'Internet à la maison, au moins une fois par semaine. Base: Tous les enfants qui utilisent l'Internet.

Origine: UNICEF

[23] Cette figure provient de: Global Kids Online (2019). Global Kids Online: Rapport comparatif, Centre de recherches Innocenti de l'UNICEF.

Certains parents hésitent à intervenir dans l'utilisation que font leurs enfants de l'Internet parce qu'ils manquent eux-mêmes de compétences en la matière.

4 Enfants vulnérables

La vulnérabilité des enfants et des jeunes peut être liée à diverses raisons. Des recherches menées en 2019[24] ont révélé "*que la vie numérique des enfants vulnérables fait rarement l'objet de la même attention, nuancée et sensible, que celle que suscite l'adversité dans la "vraie vie"*". En outre, le rapport affirme qu'"*au mieux, [les enfants et les jeunes] reçoivent les mêmes conseils génériques sur la sécurité en ligne que tous les autres enfants et jeunes, alors qu'une intervention spécialisée est nécessaire*".

Trois exemples de vulnérabilités spécifiques sont abordés ici (enfants migrants, enfants atteints de troubles du spectre autistique et enfants handicapés), mais il en existe bien d'autres.

Enfants migrants

La plupart du temps, les enfants et les jeunes issus de l'immigration arrivent (ou vivent déjà) dans un pays avec un ensemble particulier d'expériences socioculturelles et d'attentes. Bien que l'on considère généralement la technologie comme un vecteur de mise en lien et de participation, les risques et les possibilités de l'Internet peuvent varier considérablement selon les contextes. De plus, les conclusions des recherches empiriques[25] indiquent que les médias numériques jouent en général un rôle crucial, pour les raisons suivantes:

- Ils permettent de s'orienter (lors d'un voyage dans un nouveau pays).
- Ils contribuent de façon essentielle à l'appropriation et à la connaissance de la société/culture du pays d'accueil.
- Les réseaux sociaux peuvent jouer un rôle fondamental en permettant aux migrants de maintenir le contact avec leur famille et leurs pairs, et d'accéder à des informations générales.

Outre leurs nombreux aspects positifs, les médias numériques peuvent également poser des problèmes aux migrants, notamment sur les plans suivants:

- Infrastructure – il est important d'identifier des espaces en ligne sûrs où les enfants et les jeunes migrants peuvent préserver leur vie privée et être en sécurité.
- Ressources – les migrants dépensent la majeure partie de leur argent en cartes téléphoniques prépayées.
- Intégration – en plus de l'accès aux technologies, les enfants et jeunes migrants doivent également bénéficier d'une éducation numérique de qualité.

Enfants atteints de troubles du spectre autistique (TSA)

Le spectre de l'autisme regroupe deux domaines essentiels du processus de diagnostic comportemental défini dans le manuel DSM-5[26].

- Répertoire restreint et répétitif des comportements (besoin de similitude).
- Difficulté à adopter des comportements sociaux et communicatifs.
- Cooccurrence fréquente avec une déficience intellectuelle, des problèmes linguistiques ou d'autres difficultés analogues.

---

[24] Adrienne Katz (2018), Vulnerable Children in a Digital World, https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf.

[25] Better Internet for Kids (2017), *Report on the proceedings of the Safer Internet Forum 2017*, https://www.betterinternetforkids.eu/documents/167024/1738388/Report+on+the+proceedings+of+the+Safer+Internet+Forum+2017/fa4db409-4fae-45b1-96ec-35943b7d975d.

[26] Cardwell C. Nuckols (2013), The Diagnostic and Statistical Manual of Mental Disorders, https://dhss.delaware.gov/dsamh/files/si2013_dsm5foraddictionsmhandcriminaljustice.pdf.

La technologie et l'Internet offrent aux enfants et aux jeunes d'innombrables possibilités d'apprendre, de communiquer et de jouer. Toutefois, ces avantages s'accompagnent de nombreux risques auxquels les enfants et les jeunes atteints de TSA peuvent être plus exposés, par exemple:

- L'Internet peut offrir aux enfants et aux jeunes autistes une possibilité de se socialiser et d'explorer certains domaines qu'ils n'ont peut-être pas hors ligne.
- Les difficultés sociales, telles que la difficulté à comprendre les intentions des autres, peuvent rendre les personnes de ce groupe vulnérables aux "amis" malintentionnés.
- Les difficultés en ligne sont souvent liées aux caractéristiques fondamentales de l'autisme: des conseils concrets et spécifiques pourraient améliorer leur expérience en ligne, mais n'effaceront pas les difficultés sous-jacentes.

Enfants handicapés

Selon certaines des premières recherches consultatives menées sur l'expérience des enfants handicapés dans l'environnement numérique, ces enfants estiment qu'à bien des égards, leur vie en ligne est très similaire à celle des enfants non handicapés. Néanmoins, un certain nombre de différences majeures ont été soulevées[27]. Avant de les passer en revue, il est important de garder à l'esprit que les difficultés et les obstacles auxquels sont confrontés les enfants handicapés varient considérablement selon le type et la nature du handicap. Il convient d'envisager leurs besoins particuliers de façon individuelle[28].

Les enfants et les jeunes handicapés sont exposés aux mêmes risques en ligne que les enfants et les jeunes non handicapés, mais ils peuvent aussi être confrontés à des dangers spécifiquement liés à leur handicap. La probabilité qu'ils soient victimes de harcèlement en ligne est supérieure de 12% à celle des autres enfants et jeunes sans handicap. Certains enfants et jeunes handicapés peuvent rencontrer plus de difficultés à gérer leurs relations interpersonnelles en ligne ou à faire la distinction entre les vraies et les fausses informations; ils peuvent aussi facilement être manipulés pour dépenser de l'argent, ou encore partager des informations inappropriées. Les enfants et les jeunes de ce groupe sont souvent confrontés à l'exclusion, à la stigmatisation et à des obstacles (physiques, économiques, sociétaux et comportementaux) lorsqu'ils prennent part à la vie de leur communauté. Ces expériences peuvent avoir une incidence négative sur un enfant handicapé qui cherche à avoir des interactions sociales et à se faire des amis en ligne, alors que pour d'autres enfants, elles peuvent s'avérer positives et contribuer à renforcer l'estime de soi et à créer des réseaux d'entraide. Toutefois, ces situations peuvent également les exposer davantage à des risques tels que la manipulation psychologique (*grooming*), la sollicitation en ligne ou le harcèlement sexuel. Les recherches montrent que les enfants et les jeunes qui éprouvent des difficultés hors ligne et ceux qui sont touchés par des troubles psychosociaux sont plus exposés à ce type d'incidents[29].

Les auteurs d'actes comme la sollicitation en ligne, la manipulation psychologique ou le harcèlement sexuel envers les enfants et les jeunes handicapés peuvent comprendre les agresseurs préférentiels, qui ciblent les enfants et les jeunes, mais aussi ceux qui visent les enfants et les jeunes handicapés. Ces agresseurs peuvent être des "handiphiles" (*devotee*), c'est-à-dire des personnes valides attirées sexuellement par des personnes handicapées (le

---

27 Lundy et al. (2019), *DEUX CLICS EN AVANT ET UN CLIC EN ARRIÈRE: Rapport sur les enfants en situation de handicap dans l'environnement numérique*, https://rm.coe.int/deux-clics-en-avant-et-un-clic-en-arriere-rapport-sur-les-enfants-en-s/168098bd10.

28 ibid.

29 Andrew Schrock et al. (2008), *Solicitation, Harassment, and Problematic Content*, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

plus souvent des personnes amputées et paraplégiques), et prétendent parfois qu'ils sont eux-mêmes handicapés[30]. Ils agissent notamment en téléchargeant des photos et des vidéos d'enfants et de jeunes handicapés (à caractère ordinaire) et/ou en publiant ces contenus sur des forums dédiés ou des comptes de réseaux sociaux. Les fonctions de signalement sur les forums et les réseaux sociaux ne permettent généralement pas de traiter ces agissements.

Certains enfants et jeunes handicapés peuvent rencontrer des difficultés d'utilisation, voire se retrouver exclus de certains environnements en ligne, lorsque la conception ne prévoit pas de mesures d'accessibilité (par exemple, une application qui ne permet pas d'augmenter la taille du texte) ou que les aménagements demandés sont refusés (par exemple, un logiciel de lecture d'écran ou des commandes informatiques adaptables), ou s'ils ont besoin d'une aide particulière (par exemple, un accompagnement pour utiliser un équipement, ou une aide individuelle pour participer aux interactions sociales)[31].

Certains parents d'enfants et de jeunes handicapés peuvent être surprotecteurs parce qu'ils ne savent pas quelle est la meilleure façon de guider leurs enfants dans l'utilisation de l'Internet ou de les protéger contre les brimades ou le harcèlement[32]. Ils partagent parfois des informations ou des contenus (photos et vidéos) de leurs enfants dans le but d'obtenir du soutien ou des conseils, et mettent ainsi en danger la vie privée, actuelle ou future, de ces derniers. Ce faisant, ces parents risquent également d'être ciblés par des personnes mal informées ou sans scrupules qui proposent des traitements, des thérapies ou des "remèdes" pour le handicap de leur enfant[33].

30 Richard L Bruno (1997), *Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability* Disorder, Sexual and Disability, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

31 ONU (2008), *Convention relative aux droits des personnes handicapées et Protocole facultatif*, https://www.un.org/disabilities/documents/convention/convoptprot-f.pdf. Pour consulter les directives relatives à ces droits, voir l'article 9 sur l'accessibilité et l'article 21 sur la liberté d'expression et d'opinion, et l'accès à l'information.

32 Lundy et al. (2019), *DEUX CLICS EN AVANT ET UN CLIC EN ARRIÈRE: Rapport sur les enfants en situation de handicap dans l'environnement numérique*, https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

33 Sonia Livingstone et al. (2019), *UNICEF Innocenti Research Brief: Is There a Ladder of Children's Online Participation?*, https://www.unicef-irc.org/publications/pdf/IRB_2019-02%2013-2-19.pdf.

5 Nouveaux risques et difficultés émergentes

Internet des objets

L'Internet a bouleversé notre manière de vivre. Il donne accès à la totalité des connaissances humaines, à tout moment et en tout lieu. Pour certains, la vie est devenue beaucoup plus facile et "confortable" qu'auparavant. Mais cette transformation a également détruit certains modes de vie traditionnels, que ce soit dans le monde des affaires ou au niveau personnel. Par exemple, certains anciens modèles commerciaux ont été complètement modifiés ou invalidés et, sur le plan personnel, les interactions humaines physiques semblent avoir diminuées avec l'essor de l'Internet.

Il est important de distinguer l'Internet ouvert et l'Internet des objets: l'Internet ouvert est simplement virtuel; il n'existe pas dans la réalité quotidienne et le fait de l'utiliser suppose d'en avoir fait le choix. Ce n'est pas le cas de l'Internet des objets, qui donne aux objets physiques l'aura de la connectivité, dans le but d'améliorer nos vies – le grille-pain connecté à twitter en est un exemple!

Les possibilités qu'offre l'Internet des objets (IoT, *Internet of Things*) sont innombrables. L'IoT est déjà présent sous la forme d'accessoires vestimentaires, luminaires domestiques, appareils photo, voitures, toilettes, emballages, compteurs d'énergie, capteurs médicaux... la liste est longue. L'IoT a le potentiel d'apporter des améliorations dans tous les domaines. En effet, certains considèrent qu'il relève de la "quatrième révolution industrielle".

Lorsque ce type d'articles est utilisé à proximité des enfants (à savoir, à leur domicile), ils peuvent présenter des risques pour ces derniers, tels que ceux qui découlent de l'utilisation de vêtements ou d'accessoires intelligents pouvant potentiellement donner accès à leur emplacement.

Les débouchés commerciaux sont énormes, mais peuvent également soulever certains des problèmes ci-après:

Problèmes techniques/liés au respect de la vie privée

- Sécurité des dispositifs – garantir une sécurité adéquate peut être relativement coûteux; exposition aux virus/logiciels malveillants.
- Sécurité des communications – le cryptage est moins performant car l'énergie est un facteur limitant. Risque de manipulation par des tiers, de vol d'identité, etc.
- Communications permanentes – utilisation croissante d'appareils basés sur la communication permanente.
- Sécurité des données dans le nuage – en réalité, on ne sait pas qui utilise nos données.

Problèmes sociaux

- Phénomène d'exclusion sociale
- Risque d'utilisation abusive des données
- Risque que la technologie favorise les situations de violence domestique[34]

[34] Julie Inman Grant, 2019, When "smart" is not necessarily safe: the rise of connected devices extending domestic violence ("Quand "connecté" ne rime pas nécessairement avec sécurité: dispositifs connectés et violences domestiques"), https://www.esafety.gov.au/about-us/blog/when-smart-not-necessarily-safe-rise-connected-devices-extending-domestic-violence.

Problèmes économiques

- Perte d'emplois

Problèmes environnementaux

- Pollution, à tous les stades (50 milliards d'appareils seront produits dans les cinq ans à venir)

Jouets connectés et robotique

Les avancées technologiques ont profondément modifié la vie humaine et ces changements ne concernent pas seulement les adultes mais aussi les enfants et les jeunes, avec l'apparition de "l'Internet des jouets". Alors que de plus en plus d'aspects de notre vie sont transformés en données informatisées, il convient d'envisager des solutions pour assurer la protection des enfants et des jeunes et leur donner la possibilité de grandir dans un monde numérique sûr et sécurisé.

Les opinions sur la robotique ont évolué et la "robotisation" de l'enfance[35] a fait l'objet de nombreux débats. Autrefois considérés comme des objets industriels inanimés, sales et dangereux, mais aussi comme une menace pour l'emploi dans les usines, les robots sont devenus des outils jugés sophistiqués, utiles et à caractère social, avec lesquels on peut interagir à son domicile et pendant les temps de loisirs. Bien que les jouets soient conçus depuis longtemps comme des robots, de grandes transformations ont rendu les robots bien plus complexes. Non seulement ils n'ont plus la forme du robot classique de science-fiction, mais ils prennent maintenant vie sous forme de jouets qui marchent, parlent et pensent.

La *robotisation* fait suite à des progrès technologiques considérables, parmi lesquels on peut citer les suivants:

- Augmentation exponentielle de la puissance de calcul
- Connectivité mobile
- Mise en données ("datafication") et information en réseau
- Miniaturisation des capteurs, des microphones et des appareils photos
- Informatique robotique en nuage
- Avancées en matière d'intelligence artificielle et d'apprentissage automatique

L'un des robots avec lesquels les enfants et les jeunes interagissent probablement le plus souvent aujourd'hui est Siri; aussi amusante que puisse être une conversation avec un assistant numérique, elle montre le degré de maturité de l'intelligence artificielle (IA) et des algorithmes qui la régissent. Un robot social peut être défini comme un "*dispositif artificiel et incorporé, capable de percevoir son environnement (social) et d'interagir de manière ciblée et autonome avec (les agents présents au sein de) cet environnement en suivant les règles sociales associées à son rôle*". Les robots sociaux peuvent être particulièrement attrayants pour les enfants et les jeunes car ces derniers sont des utilisateurs précoces des nouvelles technologies et sont aussi souvent ciblés en tant que tels. En outre, les divers centres d'intérêt des enfants et des jeunes sont généralement en cours de formation, mais restent dispersés. Il en résulte néanmoins que les enfants et les jeunes sont sans doute plus sensibles aux effets de l'interaction avec les robots.

[35] Jochen Peter au Forum pour un Internet plus sûr 2017: Better Internet for Kids (2017), *Report on the proceedings of the Safer Internet Forum 2017*, https://www.betterinternetforkids.eu/documents/167024/1738388/Report+on+the+proceedings+of+the+Safer+Internet+Forum+2017/fa4db409-4fae-45b1-96ec-35943b7d975d.

Les caractéristiques typiques de l'interaction enfants/robots sont les suivantes:

- Mobilité
- Interactivité/réciprocité
- Caractère naturel (parole, gestes et aspects visuels, plutôt que du texte)
- Adaptation de l'interaction
- Personnalisation
- (Dés)incorporation

Les processus incorporés évoquent, pour leur part, les qualités suivantes:

- Anthropomorphisme (caractéristiques ou comportements humains)
- Présence sociale
- Participation
- Perception de similitude

L'interaction des enfants et des jeunes avec les robots peut entraîner une série de conséquences, tant positives que négatives, pour leur développement cognitif. Parmi les retombées positives, on peut citer l'optimisation de l'apprentissage, qui s'adapte à chaque enfant, est constamment mis à jour et favorise l'acquisition autonome des compétences. Les conséquences moins positives sont liées à ce qu'on appelle les "bulles éducatives", par analogie avec les "bulles de filtres" sur l'Internet, qui induisent une restriction du contenu en fonction de l'utilisateur. Dans ces cas, le risque de fragmentation des connaissances chez l'enfant côtoie la diffusion excessive d'informations, alors que le type d'enseignement s'appuie uniquement sur l'apprentissage algorithmique. Par exemple, lorsqu'un enfant pose une question à Alexa (tout comme il pourrait poser une question à Google ou à Bing), il n'obtient qu'une seule réponse, ce qui l'empêche de pouvoir mener une évaluation critique du contenu présenté.

Des préoccupations analogues portent sur la construction de l'identité chez l'enfant. D'après certaines études fondées sur la recherche[36], les robots peuvent jouer un rôle important dans la vie des enfants et des jeunes en les aidant à approfondir et à préciser leur recherche d'identité à l'adolescence. Cependant, l'utilisation de robots pose des problèmes en matière de respect de la vie privée: ils pourraient par exemple être utilisés comme des machines de surveillance chargées d'enregistrer toute personne se trouvant près d'eux, ce qui soulève de graves problèmes de sécurité, tant pour les parents que pour les enfants et les jeunes.

Pour ce qui est des aspects relationnels, les relations avec les robots ne reflètent pas toujours les relations humaines dans la vie réelle. D'une part, ce type d'interaction peut conduire les enfants et les jeunes à s'isoler de la société, en leur permettant de se réfugier dans un algorithme qui les apaise et les réconforte. Mais d'autre part, cela peut également vouloir dire que les robots offrent un espace de "discussion" possible pour échanger sur des sujets difficiles à aborder dans une conversation avec ses parents ou ses pairs. Notre relation avec les robots sera toujours une relation dominant/dominé, mais les robots savent de mieux en mieux imiter le ressenti, ce qui pourrait pousser les enfants et les jeunes à croire à tort qu'il s'agit d'une relation authentique et mutuelle.

[36] Van Straten C. L., Peter J. et Kühne R. (2019). Child-robot relationship formation: A narrative review of empirical research. *International Journal of Social Robotics*.

Comme l'a affirmé Jochen Peter, "les robots offrent plus de fonctionnalités que les jouets traditionnels, mais ils présentent aussi des risques considérables pour les plus jeunes utilisateurs"[37].

Jeux en ligne

L'industrie des jeux en ligne a dépassé celles du cinéma et de la musique en termes d'utilisateurs et de recettes. En outre, avec l'arrivée des jeux sur téléphone portable, accessibles sur un petit appareil mobile, le nombre de personnes qui participent à des jeux est plus élevé que jamais. L'étude intitulée *The State of Online Gaming 2019* indique que 51,8% des joueurs sont des hommes et que 48,2% d'entre eux sont des femmes – chiffres établis à partir des réponses de 4 500 utilisateurs issus de divers pays (France, Allemagne, Inde, Italie, Japon, Singapour, République de Corée, Royaume-Uni et États-Unis d'Amérique), qui sont âgés d'au moins 18 ans et jouent à des jeux vidéo au moins une fois par semaine[38]. Aux États-Unis, d'après les données recueillies depuis 2010, il a été estimé que 21 pour cent des joueurs de jeux vidéo ont moins de 18 ans[39].

Des recherches menées récemment en France, en Allemagne, en Espagne et au Royaume-Uni ont révélé que 54% des personnes de 6 à 64 ans jouent à des jeux vidéo et que 77% d'entre elles y jouent au moins une heure par semaine. En outre, les trois quarts des jeunes de 6 à 15 ans en Allemagne, en Espagne, en Italie, au Royaume-Uni et en France sont des joueurs de jeux vidéo, ce qui représente plus de 24 millions d'utilisateurs sur les cinq marchés européens suivis par GameTrack. Ces jeunes jouent sur divers appareils, mais environ 7 joueurs sur 10 jouent sur des consoles ou des appareils intelligents[40].

On compte aujourd'hui plus de 2,5 milliards de joueurs de jeux vidéo dans le monde. Le jeu PUBG a enregistré le plus grand nombre de joueurs simultanés, avec 3 millions de joueurs pendant 1 heure[41].

L'une des principales plates-formes de streaming de jeux vidéo dans le monde est Twitch, qui a concentré 54% des revenus des plates-formes de streaming de jeux vidéo en 2017.

Les achats intégrés au jeu constituent une part de plus en plus importante dans les jeux vidéo en ligne. Avec l'amélioration de la connectivité et de la vitesse de l'Internet, les joueurs préfèrent généralement télécharger les jeux plutôt qu'en acheter un exemplaire physique. En Afrique du Sud, la part des transactions en ligne revenant aux joueurs de jeux vidéo a augmenté de 13% entre 2018 et 2019[42].

Bien que les publics se diversifient, l'industrie des jeux est toujours dominée par des développeurs hommes et s'adresse souvent à un public masculin présumé hétérosexuel.

---

37 Van Straten C. L., Peter J. & Kühne R. (2019). *Child-robot relationship formation: A narrative review of empirical research. International Journal of Social Robotics.*

38 Limelight Networks (2019), *Market Research: The State of Online Gaming*, http://img03.en25.com/Web/LLNW/%7B02ca9602-173c-43a4-9ee1-b8980c1ea459%7D_SOOG2019_MR_8.5x11.pdf.

39 Statista.com (2019), *U.S. Average Age of Video Gamers in 2019 | Statista*, https://www.statista.com/statistics/189582/age-of-us-video-game-players-since-2010/.

40 Isfe.eu (2019), *GameTrack In-Game Spending in 2019*, https://www.isfe.eu/wp-content/uploads/2019/12/GameTrack-In-Game-Spending-2019.pdf.

41 *WEPC (2018), 2018 Video Game Industry Statistics, Trends & Data – The Ultimate List*, https://www.wepc.com/news/video-game-statistics/.

42 Chris Cleverly (2019), *Mobile Gaming in Africa*, https://medium.com/kamari-coin/mobile-gaming-in-africa-cc8bb6d7c49b.

Hélas, cela conduit souvent à une hypersexualisation des personnages féminins et à un manque flagrant de personnages autres que des hommes, blancs, à incarner.

Parallèlement à l'offre de jeux sur téléphone portable, les jeux vidéo en ligne ont également connu une croissance considérable. Tous les jeux ne peuvent pas être joués en ligne, mais toutes les consoles de jeu peuvent désormais être connectées à l'Internet. Jouer à des jeux en ligne signifie également que les utilisateurs peuvent jouer en même temps que d'autres personnes sur l'Internet. Avec certains jeux, les utilisateurs peuvent jouer uniquement avec des personnes avec lesquelles ils sont "amis", et avec d'autres, il est possible de se regrouper avec des joueurs du monde entier – sélectionnés au hasard ou en fonction du niveau de compétences ou de certains critères.

Il existe de nombreux types de jeux différents, qui sont en constante évolution. Certains des jeux et des genres les plus populaires sont énumérés ci-dessous:

First-person shooter (FPS, "tireur à la première personne") – Jeux d'action axés sur le combat à l'aide d'armes ou de projectiles, et joués du point de vue du personnage principal (par exemple Call of Duty, Overwatch, BioShock ou Battlefield).

Action – aventure – Jeux dans lesquels le joueur parcourt et explore des environnements faisant souvent intervenir des combats et la résolution de puzzles (par exemple, Grand Theft Auto (GTA), Super Mario, Uncharted, The Legend of Zelda ou God of War).

Sport – Jeux qui simulent la stratégie et les compétences physiques des sports professionnels du monde réel (par exemple, FIFA, Madden NFL ou NBA).

Sandbox/Open World ("bac à sable"/monde ouvert) – Jeux basés sur un récit ou cadre minimaliste, voire absent, qui permettent au joueur d'errer dans l'environnement virtuel et de le modifier à son gré (par exemple, Minecraft, Terraria, Skyrim ou Fallout).

Multiplayer Online Battle Arena (Moba, "arène de combat en ligne multijoueur") – Jeux en ligne où deux équipes rivales tentent de prendre ou de détruire la base de l'autre (par exemple, Dota 2, League of Legends, Heroes of the Storm ou Paragon).

L'addiction aux jeux vidéo en ligne, définie comme un *trouble du jeu vidéo* par l'Organisation mondiale de la santé en 2018, suscite des inquiétudes[43]. Dans la 11ème révision de la Classification internationale des maladies, le trouble du jeu est décrit comme un *comportement lié à la pratique des jeux vidéo ou des jeux numériques, qui se caractérise par une perte de contrôle sur le jeu, une priorité accrue accordée au jeu, au point que celui-ci prenne le pas sur d'autres centres d'intérêt et activités quotidiennes, et par la poursuite ou la pratique croissante du jeu en dépit de répercussions dommageables*. Il est important de noter que pour diagnostiquer un trouble du jeu, les schémas comportementaux qui y sont associés doivent être observés pendant au moins 12 mois.

Une autre préoccupation majeure concerne le lien entre les jeux vidéo et les jeux d'argent en ligne. Certains jeux invitent les utilisateurs à tenter d'ouvrir des *lootbox* ("boîtes à butin"): par exemple, un joueur achète une boîte en utilisant la monnaie en cours dans le jeu (qui est achetée avec une devise réelle) dans le but de recevoir une récompense aléatoire[44].

[43] OMS (2018), *OMS| Trouble du jeu vidéo*, https://www.who.int/fr/news-room/q-a-detail/gaming-disorder.
[44] Parentzone.org.uk (date?), *What Are Loot Boxes?,* https://parentzone.org.uk/article/what-are-loot-boxes.

D'après des recherches récentes, le marché mondial des boîtes à butin est estimé à 20 milliards de livres sterling[45].

Intelligence artificielle et apprentissage automatique

L'intelligence artificielle suscite beaucoup d'intérêt de la part des médias. Les applications de l'IA qui font l'objet de tests sont de plus en plus diversifiées, mais les aspects potentiellement négatifs de cette technologie soulèvent également des inquiétudes et des préoccupations.

Il est important de définir l'IA et l'apprentissage automatique, mais il n'existe pas, à l'heure actuelle, de définition universelle et suffisamment souple pour s'appliquer à tout ce qu'ils englobent. Les définitions varient selon la fonction du dispositif, le point de vue adopté et les tâches spécifiques effectuées. Cette diversité reflète également les diverses définitions de l'"intelligence humaine". On peut aussi distinguer les tâches spécifiques des tâches générales: les humains sont compétents en ce qui concerne les tâches générales, alors que l'IA est bien plus efficace pour les tâches spécifiques.

L'apprentissage automatique fait la plupart du temps référence à des méthodes permettant aux machines d'apprendre à partir de données. Il consiste à généraliser des données pour créer des modèles. L'apprentissage automatique est utilisé dans 80% des applications actuelles de l'IA.

L'intelligence artificielle pose toutefois un certain nombre de problèmes qu'il convient de prendre en considération, à savoir:

- Mauvaise définition des problèmes – La définition des problèmes est indispensable pour leur résolution.
- Disponibilité des données – La plupart du temps, les données sont erronées, non appropriées, de mauvaise qualité ou insuffisantes. Les données utilisées pour entraîner et développer les services et algorithmes de l'IA sont généralement obtenues auprès d'utilisateurs adultes. Cela peut avoir comme conséquence que les systèmes de prise de décision algorithmique et la reconnaissance de formes utilisés par l'IA soient fortement centrés sur les adultes et se traduisent de ce fait par des services qui comprennent ou classent mal les risques et les comportements des enfants. De même, les ensembles de données et les modèles utilisés pour établir et informer les processus décisionnels de l'IA peuvent ne pas représenter ou prendre en compte avec exactitude les besoins de certaines personnes liés à leur appartenance ethnique, leur sexe, leur handicap, etc. Par conséquent, les enfants qui font partie de ces groupes sous-représentés peuvent subir d'autres inconvénients transversaux, susceptibles d'être amplifiés ou utilisés par l'IA.
- Compréhension partielle – Il arrive qu'un modèle fonctionne par hasard ou soit performant, mais pour effectuer d'autres tâches que ce sur quoi porte le problème initial; par exemple, les médias ont épinglé à plusieurs reprises les cas où l'IA avait mal identifié des images au cours de recherches[46].
- Coût des erreurs.

L'intelligence artificielle constitue une avancée sans précédent, mais elle est un casse-tête aussi difficile à résoudre que celui de la voiture autonome[47].

---

45 RSPH (2019), *Skins in the Game A High-Stakes Relationship between Gambling and Young People's Health and Wellbeing?* https://www.rsph.org.uk/uploads/assets/uploaded/a9986026-c6d7-4a76-b300ba35676d88f9.pdf.

46 James Vincent (2019), *If You Can Identify What's in These Images, You're Smarter than AI,* https://www.theverge.com/2019/7/19/20700481/ai-machine-learning-vision-system-naturally-occuring-adversarial-examples.

47 Amy Maxmen (2018), *Self-Driving Car Dilemmas Reveal That Moral Choices Are Not Universal,* https://www.nature.com/articles/d41586-018-07135-0.

6 Comprendre les risques et les dangers

La Figure 7 présente une classification des risques encourus par les enfants en ligne. Il est reconnu que certains risques ont également trait à la santé et au bien-être (utilisation excessive, privation de sommeil, etc.).

Figure 7: Classification des risques encourus par les enfants en ligne[48]

	Contenu L'enfant reçoit (des productions de masse)	Contact L'enfant participe (à une activité initiée par un adulte))	Conduite L'enfant agit (auteur/victime)
Agressivité	contenu violent/sordide	harcèlement, traque	intimidation, actes hostiles de la part des pairs
Caractère sexuel	contenu violent/sordide	manipulation psycholog. à des fins sexuelles, abus sexuel lors de rencontres avec des inconnus	harcèlement sexuel, "sexting"
Valeurs	contenu raciste/haineux	propagande idéologique	contenu potentiellement préjudiciable généré par un utilisateur
Aspect commercial	publicité, marketing intégré	propagande exploitation et utilisation abusive de données personnelles	jeux d'argent, violation des droits d'auteur

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

[48] Livingstone S., Haddon L., Görzig A. et Ólafsson K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, Londres: EU Kids Online, http://eprints.lse.ac.uk/33731/.

Cas d'étude 1:

Prenons l'exemple d'un garçon qui a regardé une vidéo montrant l'assassinat d'un pilote de ligne jordanien par l'État islamique[1]. Le garçon a entendu parler de cette histoire à la radio, alors que sa mère le ramenait de l'école en voiture. Il lui a posé des questions à ce sujet, mais elle n'était pas préparée pour en parler. Elle a éteint la radio et ils sont rentrés chez eux sans avoir échangé sur ce sujet. Le garçon a vraiment été perturbé par ce qu'il avait entendu – le pilote avait été brûlé vif – et lorsqu'il est arrivé chez lui, il a fait des recherches en ligne pour en savoir plus et essayer de comprendre cette situation. Le moteur de recherche lui a entre autres proposé une vidéo, qui avait été mise en ligne par une chaîne d'information. Le garçon savait qu'il n'aurait pas dû regarder la vidéo en entier, mais il n'a pas pu s'en empêcher. Cela l'a bouleversé; il en a fait des cauchemars et a été très angoissé à la suite de cette expérience. Cependant, il n'en a parlé à personne parce qu'il avait peur de la réaction des autres et craignait sincèrement d'être réprimandé.

[1] CBS News (2015), *ISIS Video Shows Jordanian Pilot Being Burned to Death*, https://www.cbsnews.com/video/isis-video-shows-jordanian-pilot-being-burned-to-death/.

On peut comprendre la réponse de la mère; elle révèle en effet que les adultes peuvent avoir du mal à gérer certains des contenus disponibles en ligne. Mais quels que soient les difficultés soulevées par ce type de conversations, il est important qu'elles aient lieu. Les parents doivent être prêts à écouter leurs enfants et à créer un environnement au sein duquel ces derniers peuvent aborder toutes les questions qui les inquiètent.

Contenu

- Exposition à des contenus illicites et potentiellement dangereux, tels que la pornographie, les jeux d'argent, les sites web relatifs à l'automutilation et autres contenus inappropriés pour des enfants et des jeunes. Dans la plupart des cas, les opérateurs de ces sites web ne prennent pas de mesures efficaces pour restreindre l'accès des enfants et des jeunes.
- Exposition à la mise en lien avec d'autres utilisateurs.
- Automutilation, comportements destructeurs et violents.
- Exposition à la radicalisation, au racisme ou à d'autres discours et images discriminatoires.
- Utilisation ou exploitation d'informations inexactes ou incomplètes trouvées en ligne, ou d'informations provenant d'une source inconnue ou peu fiable.
- Création, réception et diffusion de contenus illicites et dangereux.

Manipulation en ligne

Les enfants et les jeunes sont de plus en plus présents dans les environnements en ligne tels que les réseaux sociaux, où ils sont exposés à une diversité de contenus filtrés par des algorithmes, dans le but de les manipuler d'une façon ou d'une autre. La manipulation en ligne peut notamment prendre les formes suivantes: manipulation politique (promotion de

certaines convictions politiques), fausses informations (diffusion de fausses informations à des fins politiques, commerciales ou autres), publicité (incitation à l'apparition d'un intérêt précoce des enfants et des jeunes pour certaines marques ou certains produits).

Ces environnements personnalisés via des algorithmes peuvent avoir une incidence considérable sur le bon développement des enfants et des jeunes, sur leurs opinions, leurs préférences, leurs valeurs et leurs habitudes, en les isolant dans des "bulles de filtres" et en les empêchant d'explorer et d'accéder librement à une grande variété d'opinions et de contenus.

Contact

- Prétendre être quelqu'un d'autre, souvent un autre enfant, dans le cadre d'une tentative délibérée de nuire, de harceler ou d'intimider une autre personne.

Sollicitation en ligne d'enfants à des fins sexuelles ou *grooming*

La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote) définit le *grooming* (sollicitation d'enfants à des fins sexuelles) comme suit: le fait pour un adulte de proposer intentionnellement, par le biais des technologies de l'information et de la communication, une rencontre à un enfant n'ayant pas atteint l'âge légal pour entretenir des activités sexuelles, dans le but de commettre à son encontre des abus sexuels ou de produire du matériel montrant des abus sexuels sur des enfants [49]. La sollicitation n'aboutit pas nécessairement à une rencontre en personne. Elle peut rester en ligne et néanmoins être très préjudiciable à l'enfant, moyennant par exemple la production, la possession et la transmission de matériel montrant des abus sexuels sur des enfants[50].

Dans le contexte de la sollicitation sexuelle, ou *grooming*, une attention plus importante est portée sur le processus de victimisation, car les recherches ont accordé une place importante aux enfants et aux jeunes eux-mêmes.

[49] Conseil de l'Europe (1957), *article 23 du traité N° 201: Convention sur la protection des enfants contre l'exploitation et les abus sexuels*, https://www.coe.int/fr/web/conventions/full-list.

[50] Comité des Parties à la Convention sur la protection des enfants contre l'exploitation et les abus sexuels (2015), *Avis sur l'article 23 de la Convention de Lanzarote et sa note explicative*, https://rm.coe.int/168064de99.

Cas d'étude 2:

Prenons l'exemple d'une jeune fille de 13 ans qui a reçu des photos inappropriées de la part d'un homme sur Instagram. L'homme diffusait des photos de lui nu et avait également demandé à la fille de lui envoyer des photos d'elle nue. La jeune fille n'a pas accédé à cette demande, elle a bloqué l'homme, l'a dénoncé à Instagram et en a également parlé à certains de ses amis au cas où la même chose leur serait arrivée – ce qui s'est effectivement produit. Bien qu'elle ait fait tout ce qu'il fallait, la jeune fille n'en a pas parlé à ses parents par crainte de leur réaction. Elle était convaincue qu'ils lui interdiraient d'utiliser Instagram et pour elle, ce n'était pas envisageable. Elle a expliqué qu'Instagram était le lieu où tous ses amis partageaient des informations et des ragots, organisaient leurs réunions sociales, discutaient de ce qui se passait à l'école, etc. La jeune fille croyait véritablement que ses parents (pour la protéger) lui demanderaient de cesser d'utiliser la plate-forme (Instagram). Mais cette jeune fille n'avait rien fait de mal: c'est le comportement de l'homme qui lui envoyait des images qui était inapproprié. C'est une réaction compréhensible de la part de parents de vouloir protéger ses enfants, mais il n'est certainement pas juste de pénaliser son enfant pour un acte commis par quelqu'un d'autre. Nous devrions supposer que toutes les actions, ou presque, de cette jeune fille sur Instagram étaient tout à fait acceptables. Il est important que les parents réfléchissent à leur réaction lorsque leurs enfants évoquent avec eux un problème qu'ils ont rencontré en ligne. Ils doivent également écouter et apporter un soutien à leurs enfants.

Intimidation et harcèlement

Le harcèlement est une pratique néfaste, quelles qu'en soient les circonstances. Le harcèlement en ligne peut être particulièrement pénible et préjudiciable, car il a tendance à se diffuser plus facilement et peut toucher un vaste public. En outre, les contenus diffusés par voie électronique peuvent resurgir à tout moment, ce qui rend plus difficile pour les victimes de clore l'incident; il peut faire intervenir des images dommageables ou des mots blessants, et est disponible en permanence. La cyberintimidation ou harcèlement en ligne peut se produire à tout moment, et donc porter atteinte à la vie privée de la victime, même dans des lieux habituellement jugés "sûrs" comme le domicile; ces situations peuvent comprendre la manipulation d'informations personnelles ou l'altération d'images et leur transmission à d'autres personnes. En outre, ces actions peuvent être effectuées de manière anonyme[51].

Les enfants et les jeunes qui sont pris pour cible hors ligne sont également susceptibles de l'être en ligne[52]. Selon des études récentes, les enfants handicapés risquent davantage d'être

[51] Tanya Byron (2008), *The Report of the Byron Review: Safer Children in a Digital World*, https://webarchive.nationalarchives.gov.uk/20120107041050/, http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf.

[52] Schrock et al. (2008), Online Threats to Youth: Solicitation, Harassment, and Problematic Content, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/RAB_Lit_Review_121808_0.pdf.

victimes d'abus de toutes sortes[53], et plus particulièrement de subir des violences sexuelles[54], ce qui les rend plus vulnérables que les autres enfants en ligne. Les agressions peuvent inclure 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 parle, ou les équipements ou services qu'il utilise. Parmi les risques encourus par ces enfants, on peut citer les suivants:

- Diffamation ou atteinte à la réputation.
- Utilisation non autorisée des cartes bancaires des parents ou d'autres personnes pour payer des frais d'adhésion, d'autres frais de services ou des marchandises.
- Tentatives criminelles de se faire passer pour des utilisateurs de l'Internet, en premier lieu dans l'espoir d'obtenir un gain financier. Dans certains cas, cela peut inclure le vol d'identité, bien que cela soit en général associé à des tentatives visant à escroquer des adultes.
- Publicité indésirable: certaines entreprises font du publipostage abusif (spam) à destination des enfants par l'intermédiaire de sites web pour leur vendre des produits. Cela soulève le problème du consentement de l'utilisateur et de la manière dont celui-ci doit être obtenu. La législation en la matière est insuffisante et il est très difficile de déterminer à partir de quel âge les enfants et les jeunes sont en mesure de comprendre les enjeux des échanges de données. En effet, l'application de ces règles sur l'Internet pose déjà un problème majeur, qui est d'autant plus accentué par l'accès via des téléphones mobiles.
- Relations indésirables, en particulier avec des imposteurs adultes qui se font passer pour des enfants ou des jeunes.

Conduite

- Divulgation d'informations personnelles entraînant un risque de dommages physiques.
- Dommages physiques dans le cadre de rencontres en personne de connaissances faites en ligne, avec un risque d'abus physique et sexuel.
- "Sexting", partage d'images intimes, qui peut entraîner des situations de harcèlement sexuel, de "sextorsion", de sollicitation en ligne et d'abus basés sur l'image[55].

Sexting

Le "sexting" (partage d'images ou de textes à connotation sexuelle par téléphone portable) est un comportement courant chez les adolescents. Ces images et textes sont souvent partagés avec des partenaires au sein d'une relation ou avec des partenaires potentiels mais il arrive qu'un public nettement plus large finisse par y accéder. Il est peu probable que les jeunes adolescents évaluent correctement toutes les répercussions de ces comportements et les risques qu'ils peuvent présenter[56].

L'un des problèmes principaux que pose la pratique du sexting est que les enfants et les jeunes peuvent contribuer à la création de matériel montrant des abus sexuels sur des enfants

[53] Mueller-Johnson, Eisner et Obsuth (2014), Sexual Victimization of Youth With a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors, http://journals.sagepub.com/doi/10.1177/0886260514534529.

[54] UNICEF (2013), *La situation des enfants dans le monde 2013 – Les enfants handicapés,* https://www.unicef.org/french/sowc2013/files/FRENCH-SOWC13-Ex_Summary_Lo-Res.pdf.

[55] Comité de Lanzarote (2019), *Avis sur les images et/ou vidéos sexuellement suggestives ou explicites produites, partagées ou reçues par des enfants*, https://rm.coe.int/avis-du-comite-de-lanzarote-sur-les-images-et-ou-videos-d-enfants-sexu/168094e72f.

[56] UNICEF (2011), *La sécurité des enfants en ligne: Défis et stratégies mondiaux,* https://www.unicef-irc.org/publications/pdf/ict_fre.pdf.

illégal, et de ce fait encourir de graves sanctions judiciaires. Parmi les dangers, on peut citer les suivants:

- Prise pour cible de publipostage abusif (spam) et de publicités d'entreprises utilisant des sites Internet pour promouvoir des produits ciblés par âge ou centre d'intérêt.
- Conduite entraînant des risques pour la santé, comme le temps passé à l'écran: utilisation excessive et compulsive de l'Internet ou des jeux d'argent, au détriment d'activités sociales ou d'extérieur bénéfiques pour la santé, le renforcement de la confiance, le développement social et le bien-être en général.
- Violation de ses propres droits ou des droits d'autrui par le plagiat et le téléchargement de contenu (en particulier de photos) sans autorisation. Il a été démontré que prendre et télécharger des photographies inappropriées sans autorisation peut porter préjudice à autrui.
- Violation des droits d'auteur d'autres personnes, par exemple en téléchargeant de la musique, des films ou des émissions télévisées pour lesquels il faudrait payer.
- Déclaration trompeuse concernant l'âge d'une personne: un enfant qui prétend être plus âgé afin d'avoir accès à des sites web inappropriés pour son âge, ou un adulte qui se fait passer pour un enfant.
- Utilisation du compte de messagerie des parents sans leur accord: l'accord des parents est parfois nécessaire pour activer des comptes en ligne; une fois activés, les parents peuvent avoir du mal à supprimer ces comptes. Les enfants et les jeunes utilisent cette méthode pour contourner le besoin d'autorisation.

L'enquête *EU Kids Online 2020* illustre la manière dont les enfants et les jeunes utilisent les nouveaux médias – par opposition à l'idée que beaucoup s'en font[57]. D'autres recherches interrogent les enfants sur la façon dont ils pensent que leurs droits devraient être protégés dans l'environnement numérique[58] et abordent l'expérience d'enfants handicapés[59].

Le principal objectif d'une campagne sur la sécurité en ligne est de modifier les comportements, y compris encourager les enfants et les jeunes à avoir une conduite en ligne plus sûre, promouvoir le rôle actif des parents en ligne et inviter les personnes qui interagissent avec des enfants et des jeunes (membres de la famille élargie, enseignants, etc.) à leur apprendre à préserver leur sécurité en ligne.

La promotion de la sécurité des enfants et des jeunes sur l'Internet ne doit pas être considérée comme un fait isolé, car elle partage un certain nombre de points communs avec diverses initiatives relatives aux enfants et aux jeunes, à leur sécurité et à l'Internet.

[57] Smahel D., Machackova H., Mascheroni G., Dedkova L., Staksrud E., Ólafsson K., Livingstone S. et Hasebrink U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online, http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf.

[58] Conseil de l'Europe (2017*), Ce monde est le nôtre: l'avis des enfants sur la protection de leurs droits dans l'environnement numérique*, https://rm.coe.int/ce-monde-est-le-notre-l-avis-des-enfants-sur-la-protection-de-leurs-dr/1680765dfe.

[59] Lundy et al. (2019), *DEUX CLICS EN AVANT ET UN CLIC EN ARRIÈRE: Rapport sur les enfants en situation de handicap dans l'environnement numérique*, https://rm.coe.int/deux-clics-en-avant-et-un-clic-en-arriere-rapport-sur-les-enfants-en-s/168098bd10.

7 Le rôle que peuvent jouer les parents, les tuteurs et les personnes s'occupant d'enfants

Les parents doivent soutenir les enfants et les jeunes afin qu'ils puissent bénéficier de la technologie en toute sécurité. Ils doivent avoir une approche nuancée et reconnaître les multiples avantages que l'Internet peut offrir. Les parents peuvent avoir tendance à se concentrer sur les nombreux aspects positifs de l'environnement numérique en matière d'éducation et de compétences, mais il est important qu'ils prennent également en considération et valorisent les bénéfices sociaux que les enfants peuvent en retirer – le jeu et l'exploration des intérêts personnels peuvent avoir une place centrale dans la façon dont les enfants utilisent l'Internet. Comprendre cela peut aider les parents à participer davantage et à donner un meilleur soutien à leurs enfants. Afin de garantir que les enfants et les jeunes utilisent les sites Internet de manière sûre et responsable, les personnes qui s'occupent d'eux, les parents et les tuteurs doivent tenir compte des orientations suivantes:

1) Se familiariser avec les risques et les possibilités que peut comporter l'Internet pour leurs enfants. Il est important de pouvoir reconnaître les menaces auxquelles les enfants peuvent être confrontés, tout en gardant à l'esprit que ces risques ne se traduisent pas nécessairement par un préjudice.
2) Suivre activement l'activité des enfants en ligne, le type de contenu qu'ils regardent, partagent ou créent, les services, les plates-formes et les jeux qu'ils utilisent ainsi que les personnes avec lesquelles ils sont en lien. Il est toujours utile que les parents essayent les services préférés de leurs enfants.
3) Chercher à se familiariser avec les sites web et les jeux ludiques et didactiques dont ils peuvent se servir avec les enfants. Un bon site web ou jeu doit comprendre une page dédiée à la sécurité contenant des liens clairs, des mécanismes de signalement et des conseils à l'intention des enfants et des jeunes ainsi que de leurs parents/responsables.
4) Entretenir un dialogue régulier, franc et ouvert avec les enfants et les jeunes, qui soit adapté à leur âge et qui évolue dans le temps.

    a) S'assurer que les enfants et les jeunes comprennent les risques qu'ils peuvent rencontrer, et convenir des mesures à prendre le cas échéant – il peut s'agir simplement de vous en parler.

    b) Encourager les enfants et les jeunes à réfléchir à ce que veut dire "être un bon citoyen numérique" en se souciant des contenus qu'ils partagent sur eux-mêmes et sur les autres, et les aider à avoir une attitude positive en ligne.

    c) Encourager une réflexion critique sur les contenus que les enfants et les jeunes voient en ligne et évoquer le fait que tout le monde n'est pas la personne qu'elle prétend être ou que tous les contenus ne sont pas forcément vrais. Aborder la manipulation de l'image de soi et les fausses informations qui visent à exploiter les gens.

    d) Parler de la pression exercée par des pairs, de l'angoisse de l'occasion manquée (*fear of missing out*) et de la façon de gérer ses amitiés en ligne.

    e) Évoquer l'attrait des technologies addictives et immersives, en particulier sur les services gratuits, où le temps passé en ligne et les données partagées constituent la monnaie ou sont à la base du modèle commercial.

5) Veiller à ce que l'enfant sache comment (où et quand) obtenir de l'aide: auprès d'un parent, d'un enseignant ou d'un autre adulte de confiance ou personne responsable. Encourager les enfants et les jeunes à être ouverts à l'idée de parler avec un adulte de confiance d'un événement en ligne qui les aurait dérangés.

6) Convenir de règles familiales applicables à l'utilisation des appareils connectés, étant entendu que les parents ou les personnes qui s'occupent d'enfants jouent le rôle de modèles de comportement en ligne.
7) Faire en sorte que les enfants aient une utilisation équilibrée des outils numériques, de sorte que leur temps en ligne soit bien réparti entre des activités telles que l'apprentissage, la création et l'établissement de liens positifs. Utiliser des outils intégrés pour analyser les habitudes d'utilisation à partir du temps passé sur chaque application et service.
8) S'assurer que vous et vos enfants êtes des utilisateurs compétents des outils numériques. Il existe de nombreux outils qui peuvent aider les parents à "gérer" la technologie connectée, à l'intérieur et à l'extérieur de la maison.

    a) Tenir compte de tous les appareils connectés, et non seulement des plus évidents (smartphones, tablettes et ordinateurs), y compris les consoles de jeu, les assistants personnels, les télévisions connectées et tout autre dispositif qui se connecte à l'Internet.
    b) Prendre les classifications par âge en considération pour déterminer à quels contenus, jeux, applications et services les enfants et les jeunes ont accès. Garder à l'esprit que la classification par âge peut varier selon les boutiques d'applications et les plates-formes elles-mêmes. Envisager de régler les paramètres pour définir les applications et les jeux qui peuvent être téléchargés et utilisés.
    c) Songer à employer des outils de filtrage du réseau, souvent appelé outils de contrôle parental, et des commandes ou moteurs de recherche sûrs pour filtrer les contenus auxquels les enfants et les jeunes ont accès en ligne.
    d) Au niveau de la famille, savoir quand et comment signaler des contenus qui suscitent une gêne, des inquiétudes ou des préoccupations, ou qui sont jugés contraires aux conditions d'utilisation. Connaître les procédés permettant de bloquer les contacts indésirables ou non sollicités.
    e) Examiner les tenants et les aboutissants de l'utilisation des applications et technologies de surveillance qui permettent de suivre l'utilisation de l'Internet par un enfant. Celles-ci peuvent avoir des conséquences involontaires en suscitant un comportement plus dissimulé en ligne et peuvent également causer des dommages dans des contextes de violence domestique et familiale. Si vous les utilisez, expliquez à votre enfant ce que vous surveillez et pour quelles raisons.
    f) Il est important, à mesure que les enfants et les jeunes grandissent et mûrissent, de réévaluer les contrôles et les restrictions imposées pour s'assurer que ceux-ci sont adaptés à leur âge; il est primordial de favoriser la capacité de discernement des enfants pour qu'ils puissent s'épanouir en ligne.

9) Apprendre aux enfants à ne pas partager leurs mots de passe avec des amis ou leurs frères et sœurs. Songer à la façon dont ils partagent des informations personnelles; par exemple, il pourrait être judicieux d'utiliser une photo de profil impersonnelle et de limiter la publication de renseignements personnels (âge, école, emplacement, etc.) sur un profil visible dans le monde entier.
10) Ne pas supposer que tout le monde sur l'Internet représente une menace pour votre enfant. En général, les sites web pour enfants sont sécurisés et peuvent leur offrir une expérience sociale et éducative très enrichissante et créative, mais il convient de rester présent et vigilant.
11) Rester calme et ne pas tirer de conclusions hâtives si vous entendez ou voyez des choses inquiétantes à propos du comportement de votre enfant ou de l'un de ses amis en ligne. Éviter de menacer de retirer ou de confisquer les appareils, car ceux-ci peuvent constituer pour certains jeunes un moyen essentiel de maintenir le lien social. Si vos enfants craignent

que vous ne les leur retiriez, il se peut qu'ils deviennent encore plus réticents à partager les problèmes ou les préoccupations qu'ils pourraient avoir.

12) Reprendre confiance après certaines expériences et en tirer des leçons est essentiel pour renforcer la résilience numérique. Si les enfants courent des risques ou subissent des préjudices en ligne, les parents peuvent les aider à trouver des moyens de reprendre confiance, afin de profiter en toute sécurité des aspects positifs le moment venu et d'échapper autant que faire se peut à l'exclusion.

Où chercher de l'aide?

De nombreux pays disposent de services d'assistance téléphonique auxquels les enfants et les jeunes peuvent s'adresser pour signaler un problème. Ces numéros sont largement diffusés et selon les pays, les approches sont différentes pour faire passer ce message. Il est important que les enfants et les jeunes sachent qu'il n'est jamais trop tard pour signaler un problème et qu'en le faisant, ils peuvent venir en aide à d'autres personnes.

Alors que les enfants et les jeunes reconnaissent qu'ils adoptent parfois des comportements risqués, ils ne se montrent pas excessivement préoccupés par les risques inhérents à ce type de comportements et préfèrent tenter de résoudre les problèmes par eux-mêmes ou au sein de leur groupe de pairs. On peut donc supposer qu'ils ne font appel à leurs parents ou à d'autres adultes qu'en cas de problèmes potentiellement graves. Cela représente un problème, en particulier chez les garçons plus âgés, qui ont tendance à privilégier l'emploi de la fonction "Signaler un abus"[60] (telle que définie par l'équipe Virtual Global Task Force), sans pour autant en informer leurs parents ou d'autres adultes. Mais ce n'est pas le cas de tous les enfants et jeunes. On peut constater que les enfants et les jeunes qui sont conscients des risques se régulent eux-mêmes dans leurs activités, mais au sujet des nouvelles technologies, ils estiment généralement que les adultes ne devraient pas être responsables de juger et de contrôler leur comportement[61]. Il convient d'être prudent lorsqu'on opère une distinction simpliste entre les mondes virtuel et réel, car elle ne reflète plus nos vies quotidiennes actuelles, qui intègrent de plus en plus les technologies en ligne. Pour de nombreux enfants et adolescents, cela suppose de parvenir à démêler soigneusement les opportunités offertes par les technologies (possibilité d'explorer leur identité, d'établir des relations intimes et d'accroître leur réseau social) des risques que la communication via Internet peut induire (atteinte à la vie privée, défaut de compréhension et pratiques abusives)[62].

Les parents et les éducateurs doivent savoir qu'en cas de suspicion d'abus sexuel en ligne, il convient de bloquer l'agresseur et de conserver la communication entretenue à des fins de preuve. Les parents ne doivent jamais visionner d'images à caractère sexuel créées par leur enfant ou d'autres enfants. Ce matériel doit être remis aux autorités policières et les abus ou l'exploitation d'enfants en ligne doivent être signalés aux autorités compétentes. Les parents ne doivent jamais se faire passer pour leur enfant en vue de "prouver" les abus.

De plus amples informations sur les modalités de signalement des images d'enfants à caractère sexuel sont disponibles sur les pages suivantes:

---

60 Europol (2019), *2019 Virtual Global Taskforce Releases Environmental Scan*, https://www.europol.europa.eu/newsroom/news/2019-virtual-global-taskforce-releases-environmental-scan.

61 Manida Naebklang (2019), *Report of the World Congress III against Sexual Exploitation of Children & Adolescents*, https://www.ecpat.org/wp-content/uploads/legacy/ECPATWCIIIReport_FINAL.pdf.

62 Livingstone (2008), Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression, http://journals.sagepub.com/doi/10.1177/1461444808089415 (last visited 16 January 2020].

Internet Watch Foundation – https://www.iwf.org.uk/

NCMEC – https://report.cybertip.org/

Europol – https://www.europol.europa.eu/report-a-crime/law-enforcement-reporting-channels-child-sexual-coercion-and-extortion

8 Lignes directrices à l'intention des parents, des tuteurs et des personnes s'occupant d'enfants

Les conseils en matière de sécurité ont été établis à partir de l'analyse des données recueillies et des recherches disponibles. Cette section du rapport vise à fournir des lignes directrices aux parents, tuteurs et personnes s'occupant d'enfants (ainsi qu'aux éducateurs, dans une liste séparée) pour les aider à apprendre aux enfants et aux jeunes comment vivre une expérience en ligne positive et enrichissante, en toute sécurité.

Les parents, tuteurs et personnes s'occupant d'enfants doivent tenir compte de la nature exacte des différents sites, de la compréhension que leurs enfants ont des dangers et de la mesure dans laquelle ils peuvent contribuer à réduire les risques, avant de décider quel environnement convient à leur enfant.

L'Internet recèle un grand potentiel pour donner les moyens aux enfants et aux jeunes de trouver des informations par eux-mêmes. Leur apprendre à avoir une attitude en ligne positive et responsable est un objectif essentiel. Le Tableau 1 divise les questions en domaines principaux, que les parents et les personnes responsables d'enfants doivent prendre en considération.

Tableau 1: Principaux domaines à considérer par les parents, les tuteurs et les personnes s'occupant d'enfants

Parents, tuteurs	#	Principaux domaines à considérer	Description
Sûreté et sécurité de la technologie utilisée	1	Dialoguez avec vos enfants. Essayez d'effectuer certaines activités en ligne avec eux.	Intéressez-vous à ce qu'ils font en ligne, échangez avec eux. Il est important que les enfants et les jeunes n'aient pas l'impression que leurs parents ne leur font pas confiance. Le filtrage, la surveillance et la restriction de l'accès ont leur place, mais ils doivent s'accompagnés de dialogue et de discussion. Lorsque les enfants et les jeunes passent du temps avec d'autres personnes en dehors de leur foyer, ils ont accès à d'autres appareils (parfois sans restriction), d'où la nécessité d'une bonne communication – votre enfant vous parlerait-il une mauvaise expérience? Il convient de ne pas réagir de manière excessive lorsque des enfants ou des jeunes vous racontent un événement survenu en ligne. Ce qui est important, c'est qu'ils vous l'aient dit, et un bon accueil de votre part les incitera à avoir confiance dans le fait que vous pouvez les aider et à revenir vers vous à l'avenir. Il peut être utile pour les enfants et les jeunes de comprendre ce qu'est l'Internet, afin qu'ils aient une meilleure connaissance de l'"espace Internet", sur lequel ils accèdent à leurs plates-formes préférées telles qu'Instagram, Snapchat ou YouTube. L'Internet peut parfois apparaître comme un lieu abstrait aux yeux des enfants et des jeunes et, s'ils n'en comprennent pas bien le fonctionnement, ils peuvent avoir plus de mal à évaluer les risques, à les reconnaître ou à les identifier. On pourrait, par exemple, le comparer à une grande ville regorgeant d'endroits agréables et de gens charmants, mais qui comporte aussi des zones dans lesquelles vous ne vous rendriez pas car elles pourraient être dangereuses. Cette analogie aidera les enfants et les jeunes à réfléchir aux différents "publics" qu'ils peuvent rencontrer en ligne, et par exemple, à la manière dont l'information peut circuler. Les parents doivent s'intéresser à ce que font leurs enfants en ligne et être prêts à partager des expériences numériques avec eux, afin de favoriser la confiance et d'ouvrir le dialogue.

Parents, tuteurs	#	Domaines essentiels à considérer	Description
	2	Identifiez les technologies, appareils et services utilisés par les membres de votre famille/ au sein de votre foyer.	Pour ce qui est des appareils: identifiez tous les appareils qui sont connectés chez vous, y compris les téléphones portables, les ordinateurs portables, les tablettes ainsi que les télévisions intelligentes, les consoles de jeu, les dispositifs de suivi de la condition physique, et tout autre appareil utilisé par un membre de la famille. Identifiez les services et applications en ligne qu'utilisent tous les membres de la famille sur tous ces appareils.
	3	Installez un pare-feu et un logiciel antivirus sur tous les appareils. Déterminez si les logiciels de filtrage et de blocage ou de contrôle peuvent être utiles et adaptés à votre famille.	Assurez-vous que vos appareils sont équipés de systèmes anti-virus et de protection contre des logiciels malveillants et que ceux-ci sont à jour. Apprenez à vos enfants les bases de la sécurité sur Internet. Par exemple, votre système d'exploitation est-il à jour? Utilisez-vous la version la plus récente d'une application? Les derniers correctifs de sécurité sont-ils installés? Les outils de filtrage et de surveillance sont utiles, mais les aspects liés à la confiance et au respect de la vie privée doivent également être pris en considération. Les parents devraient discuter avec leurs enfants des raisons pour lesquelles ils utilisent de tels outils, dans le but de préserver la sécurité de la famille.
Règles	4	Convenez avec les membres de la famille des directions à suivre concernant l'usage de l'Internet et des terminaux personnels, en accordant une attention particulière aux problèmes liés à la vie privée, aux sites web inappropriés selon l'âge, aux applications et aux jeux, au harcèlement, au temps passé à l'écran et aux dangers que représentent les inconnus. Veillez également à entretenir un climat favorable au sein du foyer, afin que les enfants et les jeunes se sentent en mesure de vous demander de l'aide.	Dès que les enfants et les jeunes commencent à utiliser les technologies, discutez des règles et établissez une liste ensemble. Ces règles doivent inclure les horaires pendant lesquels les enfants et les jeunes peuvent utiliser l'Internet et les modalités d'utilisation, ainsi que les limites en matière de temps passé à l'écran. Modèle numérique – Il est important que les parents donnent le bon exemple à leurs enfants, car ces derniers sont plus susceptibles d'adopter des comportements appropriés lorsqu'ils imitent leurs parents/tuteurs. Il conviendrait que ces mesures s'étendent à la prise et au partage de photos: la mise en ligne de toute image devrait être précédée d'une demande d'autorisation à la personne intéressée. Évaluez votre propre utilisation de l'Internet et des réseaux sociaux par rapport à votre enfant, par exemple le partage d'anecdotes ou de photos concernant l'enfant. Tenez compte de la vie privée de l'enfant, actuelle mais aussi future. Les enfants et les jeunes doivent pouvoir évoquer toute pression ou difficulté à laquelle ils sont confrontés en ligne (et hors ligne). Pour favoriser la discussion, une possibilité consiste à tirer parti des occasions où les médias publient des articles sur le comportement sur Internet/en ligne. Cela dépersonnalisera la question, mais permettra aux enfants et aux jeunes d'exprimer leur opinion.
Éducation des parents et des tuteurs	5	Savoir quels sont les services en ligne et mobiles qu'utilisent vos enfants (réseaux sociaux, sites web, applications, jeux, etc.) et bien comprendre comment les enfants passent leur temps en ligne.	Sachez comment faire en sorte que les enfants et les jeunes utilisent les applications et les plates-formes de la manière la plus sûre possible, notamment en réglant les paramètres de confidentialité des comptes, en suivant les restrictions d'âge, etc. Utilisez les outils fournis avec les appareils mobiles, tels que Family Link ou d'autres outils de contrôle parental. Vérifiez si les sites vendent des produits ou si les applications utilisées comprennent des achats intégrés. Essayez de comprendre les motivations des enfants et des jeunes lorsqu'ils sont en ligne. Pourquoi utilisent-ils certains sites web ou services? Quelle est la particularité des différents sites web et services en termes de groupes d'amis, de sentiment d'identité et d'appartenance? Comprendre ces différents aspects vous permettra également de mieux saisir les difficultés sociales et émotionnelles auxquelles les enfants et les jeunes peuvent être confrontés (ce qui peut parfois se traduire par des comportements à risque) et de leur donner des indications pour les aider à renforcer leur capacité de discernement.

Parents, tuteurs	#	Domaines essentiels à considérer	Description
Examen des fonctionnalités des sites web	6	Tenez compte de l'âge défini pour le consentement numérique.	Dans certains pays, des lois spécifient l'âge minimum à partir duquel une entreprise ou un site web peut demander à un jeune de donner des renseignements personnels le concernant sans avoir à fournir au préalable une preuve de l'accord parental. Ce que l'on appelle l'"âge du consentement numérique" se situe généralement entre 13 et 16 ans. On estime dans certains pays que le fait d'exiger l'accord des parents avant de demander à des personnes plus jeunes de fournir des données personnelles constitue une bonne pratique, tandis que dans d'autres, cette pratique est inscrite dans la loi (voir l'Article 8 du Règlement général sur la protection des données pour les États membres de l'UE). De nombreux sites web destinés aux enfants plus jeunes demandent l'accord parental avant d'inscrire un nouvel utilisateur. Vérifiez les prescriptions relatives à l'âge minimum d'utilisation pour chaque service.
	7	Utilisation contrôlée des cartes bancaires et autres moyens de paiement	De nombreux appareils, applications et services peuvent être utilisés pour effectuer des achats et gérer attentivement l'accès aux comptes des parents sur lesquels les moyens de paiement et les cartes de crédit sont enregistrés. Il est important de protéger vos cartes bancaires et de crédit, et de ne pas divulguer vos codes PIN afin d'empêcher tout accès non autorisé.
	8	Signalements	Sachez comment signaler des problèmes sur les plates-formes que vos enfants utilisent et comment supprimer ou modifier des profils; veillez à ce que les enfants apprennent à le faire en grandissant. Renseignez-vous également sur les lignes d'assistance téléphonique locales dédiées aux signalements.
	9	Publicité, fausses informations et informations trompeuses	Gardez à l'esprit que les publicités peuvent être inappropriées ou trompeuses. Expliquez à vos enfants comment ils peuvent signaler des publicités et maîtriser davantage ce qu'ils voient en ligne. Il est important de savoir que les contenus auxquels accèdent les enfants et les jeunes en ligne peuvent influencer leurs opinions. Communiquez avec eux pour les aider à renforcer leur maîtrise des outils en ligne.

Parents et tuteurs	#	Domaines essentiels à considérer	Description
Éducation des enfants	10	Instaurer un climat favorable	Les enfants et les jeunes doivent comprendre que le monde en ligne est le reflet du monde hors ligne, avec ses bonnes et ses mauvaises expériences. Il est important qu'ils se sentent suffisamment en confiance pour vous demander de l'aide et du soutien en cas de problème, et suffisamment sûrs d'eux pour apporter de l'aide aux autres en ligne. Selon l'âge de vos enfants, il peut être utile de comprendre les contenus qu'ils publient et de connaître leur profil en ligne. Les enfants et les jeunes doivent être capables de reconnaître les risques en ligne; certains sont évidents, mais ce n'est pas le cas de tous (par exemple, la coercition, le chantage ou l'humiliation). Ces mécanismes sont tous utilisés par les agresseurs et les criminels. Les enfants et les jeunes doivent également comprendre que l'accès à des contenus en ligne va de pair avec des responsabilités. Ils doivent être conscients du fait que les lois s'appliquent tout autant en ligne que hors ligne, et qu'ils sont censés avoir un comportement acceptable.
	11	À mesure que les enfants et les jeunes en apprennent davantage sur l'environnement numérique, ils peuvent vouloir rencontrer des personnes qu'ils ne connaissent pas physiquement, mais avec lesquelles ils ont entretenu une relation en ligne. Il est important que vous adoptiez une bonne démarche pour les sensibiliser aux dangers que peut comporter la rencontre d'un inconnu avec qui ils ont échangé en ligne.	Les enfants et les jeunes peuvent courir un réel danger s'ils rencontrent en personne un inconnu avec lequel ils ont été en contact uniquement sur l'Internet. Les personnes rencontrées en ligne peuvent s'avérer avoir une autre identité dans la vie réelle. Toutefois si votre enfant se lie d'une forte amitié avec une personne en ligne et qu'il souhaite organiser une rencontre, évitez de le laisser se rendre seul ou sans surveillance au rendez-vous, précisez clairement que vous préférez l'accompagner, ou faites-en sorte qu'un autre adulte de confiance le fasse. Il est évident que cette situation variera en fonction de l'âge de l'enfant. Il est également important de noter que l'on constate une augmentation des agressions à distance: dans ces cas, les criminels ou les agresseurs ne cherchent pas à rencontrer un enfant, mais à obtenir de celui-ci un contenu sexuellement explicite.
	12	Importance des informations personnelles	Aidez vos enfants à comprendre ce que sont les informations personnelles et à les gérer. Expliquez que les enfants et les jeunes devraient publier uniquement des informations dont le partage avec d'autres personnes ne vous gêne pas, et ne les gêne pas. Ils ne devraient pas partager des informations d'identification personnelle. Rappelez aux enfants et aux jeunes qu'ils doivent gérer leur réputation en ligne. Une fois que le contenu a été partagé, il peut être difficile de le modifier ou l'adapter.
Éducation des enfants	13	Assurez-vous que les enfants et les jeunes comprennent les répercussions que peut avoir la mise en ligne de photographies, y compris des photos d'eux-mêmes et de leurs amis.	Expliquez à vos enfants que les photographies peuvent révéler beaucoup d'informations personnelles. Les enfants et les jeunes doivent comprendre les risques liés à l'utilisation d'appareils photo et au téléchargement de contenus. En principe, les images d'autres personnes ne devraient pas être mises en ligne sans leur consentement. Cela concerne également les parents, lorsqu'ils prennent et téléchargent des images de leurs enfants. De même, il est important que les enfants et les jeunes sachent que ce sont parfois d'autres personnes de leur entourage qui peuvent diffuser des informations; ils doivent donc dialoguer avec leurs amis et les membres de leur famille, et les sensibiliser à la notion de partage excessif. Encouragez vos enfants à ne pas mettre en ligne de photographies d'eux-mêmes ou de leurs amis révélant des détails clairement identifiables tels que des plaques de rue, des plaques d'immatriculation ou le nom de leur école inscrit sur leurs vêtements.

9 Le rôle des éducateurs

Il est très important que les éducateurs n'émettent aucune hypothèse quant à la question de savoir ce que les enfants et les jeunes savent ou ne savent pas sur les questions de sécurité en ligne. Par exemple, il est important que les éducateurs enseignent aux enfants et aux jeunes l'importance des mots de passe, comment les protéger et comment créer un mot de passe fort: de nombreux adolescents partagent leurs mots de passe avec leurs amis, ce qui est souvent considéré comme un signe de grande amitié.

La protection de la vie privée des enfants et des jeunes en ligne fait l'objet de nombreux débats, et une étude menée par la London School of Economics a montré que les enfants et les jeunes accordent de l'importance à leur vie privée et adoptent des stratégies de protection, mais qu'ils apprécient également la possibilité de communiquer en ligne. De même, l'étude a révélé que la *médiation parentale* était importante pour donner aux enfants et aux jeunes les moyens de devenir autonomes, car elle leur permettait de prendre des risques tout en apprenant des comportements protecteurs autonomes. Elle a également indiqué que "*l'éducation aux médias destinée aux parents, aux éducateurs et aux travailleurs sociaux doit être envisagée, car les faits suggèrent que les adultes connaissent très mal les risques et les stratégies de protection des données et de la vie privée des enfants et des jeunes en ligne*"[63].

Les écoles ont la possibilité de transformer l'enseignement et d'aider les élèves à réaliser leur potentiel et à améliorer leur niveau grâce aux TIC. Mais il est tout aussi important que les enfants et les jeunes apprennent à se protéger lorsqu'ils utilisent ces nouvelles technologies, en particulier les technologies plus collaboratives telles que les plates-formes et les services de réseaux sociaux, qui sont un aspect essentiel d'un apprentissage social productif et créatif. Les enfants et les jeunes peuvent désormais facilement créer leurs propres contenus et les partager largement grâce aux réseaux sociaux, dont la plupart permettent également le streaming en direct.

Les éducateurs peuvent aider les enfants et les jeunes à utiliser la technologie de manière judicieuse et sûre, notamment en prenant les mesures suivantes:

- S'assurer que l'école dispose d'un ensemble de politiques et de pratiques cohérentes et que leur efficacité est examinée et évaluée régulièrement.
- Contribuer au développement des compétences et de la maîtrise du numérique en incluant l'éducation à la citoyenneté numérique dans leurs programmes. Il est important d'inclure les concepts d'apprentissage social et émotionnel dans l'éducation à la sécurité en ligne, car ces concepts aideront les élèves à comprendre et à gérer leurs émotions en vue d'établir des relations saines et respectueuses, en ligne et hors ligne.
- S'assurer que tout le monde connait la Politique d'utilisation acceptable (PUA) et sait s'en servir. Il est important d'avoir une PUA, qui de plus doit être adaptée en fonction de l'âge.
- Vérifier que la politique de l'école visant à lutter contre le harcèlement comprend des références au harcèlement en ligne et via téléphone mobile ou tout autre équipement, et que des sanctions effectives sont prévues pour les contrevenants.
- Nommer un coordinateur de la sécurité en ligne.
- S'assurer que le réseau de l'école est sûr et sécurisé.
- S'assurer que le fournisseur d'accès à l'Internet est agréé.
- Utiliser un outil de filtrage/contrôle.

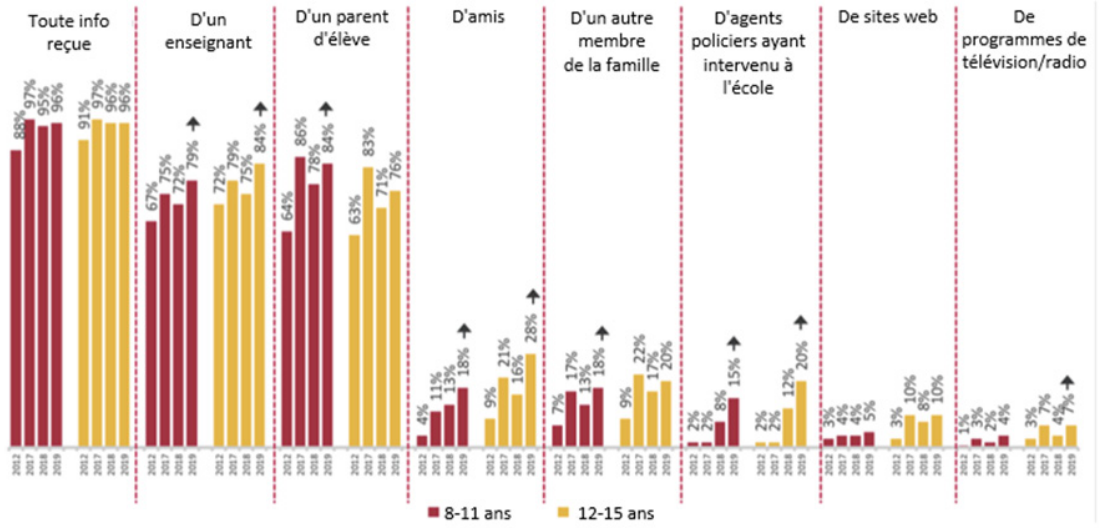
[63] Sonia Livingstone, Mariya Stoilova et Rishita Nandagiri (2018), Children's Data and Privacy Online: *Growing up in a Digital Age*, http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.

- Dispenser des cours de formation à la sécurité en ligne à tous les enfants et les jeunes et préciser où, comment et quand ils seront proposés.
- S'assurer que tout le personnel (y compris le personnel auxiliaire) a été correctement formé et que leur formation est régulièrement mise à jour.
- Avoir un seul référent au sein de l'école et être capable de recenser et d'enregistrer les incidents relatifs à la sécurité en ligne, ce qui permettra aux responsables de l'école de se faire une meilleure idée des problèmes à résoudre ou des tendances à examiner.
- S'assurer que l'équipe de direction et les responsables de l'école sont suffisamment sensibilisés à la question de la sécurité en ligne à l'école.
- Mettre en place une évaluation régulière de toutes les mesures liées à la sécurité en ligne.
- Évaluer les conséquences pédagogiques et psychologiques que l'Internet et les technologies en ligne peuvent avoir sur les enfants et les jeunes.
- L'utilisation de l'Internet par les enfants et les jeunes a connu un essor considérable ces dernières années, et s'est accompagnée d'une préoccupation croissante quant à la sécurité en ligne. Pendant longtemps, le danger potentiel des technologies de la communication a suscité une panique morale récurrente, particulièrement en ce qui concerne les jeunes femmes. Toutefois, il a été avancé que l'étude effective de ces dangers montre que, très souvent, ce n'est pas tant la technologie en elle-même qui est en cause, mais plutôt l'augmentation de l'activité en ligne des enfants et des jeunes, ainsi que les angoisses liées à la perte de contrôle parental. Les éducateurs sont perçus comme ayant un rôle vital dans la promotion et la préservation de la sécurité sur Internet. Les parents du monde entier semblent croire que les écoles devraient jouer un rôle central dans l'éducation des enfants et des jeunes à l'utilisation en toute sécurité des nouvelles technologies, mais il ressort aussi clairement des recherches que les principales sources d'information sur les questions en ligne pour les enfants et les jeunes sont l'école et des parents[64]. Des recommandations supplémentaires sur les compétences qui doivent être incluses dans ce type de formation ont été identifiées dans le cadre du projet "Éducation à la citoyenneté numérique" du Conseil de l'Europe[65].

[64] Ofcom (2020), Children and Parents: Media Use and Attitudes Report 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/190518/children-media-use-attitudes-2019-chart-pack.pdf.

[65] Conseil de l'Europe (2018), Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique – Recommandation CM/Rec(2018)7 du Comité des Ministres (2018), Construire une Europe pour et avec les enfants, https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.

Figure 8: Enfants déclarant avoir reçu des informations ou des conseils sur la manière d'utiliser l'Internet en toute sécurité, parmi ceux qui se connectent à l'Internet chez eux (2012) ou ailleurs (2017, 2018, 2019), par âge[66]



Origine: Ofcom

- Les premières approches concernant la sécurité en ligne se sont largement concentrées sur les solutions techniques, telles que l'utilisation de logiciels de filtrage, mais ces dernières années, avec l'augmentation de la mobilité des technologies de l'information, les ordinateurs de bureau plus traditionnels ont cessé d'être le seul point d'accès à l'Internet. De plus en plus de téléphones mobiles, de tablettes, d'assistants numériques personnels et de consoles de jeux offrent une connexion haut débit qui permet aux enfants et aux jeunes d'accéder à l'Internet alors qu'ils sont à l'école, à la maison, dans une bibliothèque, un café Internet, une enseigne de restauration rapide, un club de jeunes ou même dans les transports en commun, sur le chemin de l'école. À l'école, les enfants et les jeunes peuvent travailler sur l'Internet, de manière collaborative au sein d'un réseau fermé, ou simplement en étant entourés d'autres enfants. Les mesures les plus évidentes comprennent la sécurisation efficace du réseau. Les enfants et les jeunes peuvent posséder des appareils personnels dont la sécurité n'est pas assurée par la protection du réseau, d'où l'importance de l'éducation, de la discussion et du dialogue.
- Les politiques de sécurité en ligne doivent être conçues et mises en œuvre de manière à impliquer un large éventail de groupes d'intérêt et de parties prenantes, notamment:
  - les professeurs principaux;
  - les administrateurs;
  - l'équipe de direction;
  - les enseignants;
  - le personnel auxiliaire;
  - les parents ou personnes s'occupant des enfants;
  - les agents des autorités locales;
  - si possible, les fournisseurs d'accès à l'Internet et ceux qui fournissent l'Internet et des services haut débit aux écoles.

[66] Ofcom (2020), Children and Parents: Media Use and Attitudes Report 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/190518/children-media-use-attitudes-2019-chart-pack.pdf.

Étant donné que chacun de ces groupes a un point de vue qui peut être utile pour définir les politiques des écoles, il est important de tous les consulter. Toutefois, le simple fait d'avoir des politiques ne suffit pas, et toutes les personnes qui s'occupent d'enfants et de jeunes devraient participer activement à aider le personnel à identifier et à adopter un comportement sûr. En donnant une voix à tous ces groupes depuis le début, tout le monde devrait convenir de la pertinence de ces politiques et endosser la responsabilité qui leur revient pour les appliquer.

La création d'un environnement sûr pour l'apprentissage des TIC dépend de plusieurs éléments importants, parmi lesquels on peut citer:

- une infrastructure permettant la prise de conscience de l'ensemble;
- les responsabilités, politiques et procédures;
- un éventail d'outils technologiques efficaces;
- une formation complète sur la sécurité en ligne;
- l'existence de programmes personnalisés au sein de l'établissement;
- un processus d'évaluation qui contrôle en continu l'efficacité de l'environnement d'apprentissage des TIC.

Ces éléments devraient tous être intégrés dans les politiques existantes sur la sécurité des enfants au sein de l'école, plutôt que d'être considérés comme des aspects dont la gestion relève uniquement d'une équipe chargée des TIC. Il est peu pertinent de faire la distinction entre le harcèlement sur l'Internet ou via un téléphone mobile et ces mêmes pratiques hors ligne. La technologie peut, néanmoins, représenter une part importante de la solution, avec des moyens tels que:

- la prévention et la protection contre les virus;
- des systèmes de contrôle permettant de savoir qui a téléchargé quoi, à quel moment et sur quel ordinateur;
- un filtrage et un contrôle des contenus visant à limiter les contenus inappropriés accessibles sur le réseau de l'école.

Les problèmes liés aux nouvelles technologies ne concernent pas tous les enfants et les jeunes, et lorsque des problèmes surviennent, ils dépendent de l'âge des enfants et des jeunes qui utilisent ces technologies. Fin 2008, le groupe de travail sur la sécurité de l'Internet aux États-Unis (Internet Safety Technical Taskforce) a produit un rapport sur l'amélioration de la sécurité des enfants et des technologies en ligne, qui fournit une analyse bibliographique utile des recherches originales et publiées sur la sollicitation sexuelle en ligne, le harcèlement et l'intimidation en ligne et l'exposition à des contenus problématiques[67]. Il est noté dans ce rapport "qu'il est à craindre que les médias grand public n'amplifient ces peurs, les rendant disproportionnées par rapport aux risques auxquels sont confrontés les jeunes". Plus de dix ans plus tard, et encore aujourd'hui, les parents et les éducateurs sont bombardés d'articles qui tendent davantage à encourager les adultes à restreindre l'accès aux services en ligne qu'à éduquer et donner aux enfants les moyens de les utiliser en toute sécurité.

Cela pourrait risquer d'occulter les risques connus et réduit la probabilité que la société s'intéresse aux facteurs qui sont à l'origine de ces risques, lesquels peuvent malencontreusement devenir préjudiciables. La couverture médiatique des délits commis sur l'Internet contre des enfants et des jeunes reflète souvent les positions polarisées des professionnels et des universitaires qui

[67] ISTTF (2008), Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

travaillent dans ce domaine, avec, d'un côté, ceux qui estiment qu'il est dangereux de déformer la menace qui pèse sur les enfants et les jeunes, et de l'autre, ceux pour qui la menace aurait été sous-estimée.

Les différents modes d'agression dont les enfants et les jeunes peuvent être victimes en ligne comprennent notamment:

- la sollicitation d'enfants ou *grooming*;
- l'exposition à du matériel problématique ou illicite;
- l'exposition à un milieu qui pourrait encourager les comportements destructeurs chez les jeunes;
- le harcèlement en ligne.

Une méthode utile de classification des risques encourus par les enfants en ligne a été présentée dans la Figure 7.

Cadres éducatifs informels

Outre l'école et la maison, c'est dans un cadre non formel, par exemple dans des clubs de jeunes ou des groupes religieux, que les enfants peuvent avoir accès à l'Internet et à ses services. En raison de l'imbrication de la vie en ligne et hors ligne des enfants et des jeunes, les personnes travaillant avec les enfants dans de tels cadres peuvent avoir une influence sur la compréhension qu'ont les enfants de l'environnement numérique et de leur sécurité en ligne, même si ce n'est pas leur principal objectif. Par conséquent, toutes les personnes intervenant dans des cadres plus informels devraient comprendre les risques et les possibilités offertes, et être en mesure de soutenir les enfants de manière appropriée ou d'accéder à l'aide et à la formation nécessaires.

Les principaux éléments et principes des lignes directrices destinées aux éducateurs s'appliquent également dans ces cadres informels, mais le contexte peut être différent et d'autres facteurs peuvent entrer en ligne de compte.

Gestion des dispositifs, du filtrage et des communications

Le personnel auxiliaire, les bénévoles et les enfants sont plus enclins à accéder aux services depuis leurs propres appareils dans des cadres ou systèmes de gestion des dispositifs informels, et le filtrage du contenu peut être moins accessible ou moins performant qu'au sein des écoles. Par conséquent, il peut être nécessaire de s'assurer que les éducateurs et les enfants savent comment protéger et gérer leur propre appareil, ce qui nécessite une plus grande attention dans les cadres informels. De même, les éducateurs et les enfants ne doivent pas trop se fier aux options de filtrage moins sophistiquées pour leur protection.

Les cadres informels devraient quoiqu'il en soit disposer de politiques et de lignes directrices solides et bien étayées en matière de protection des enfants. Cependant, dans certains cas, les éducateurs ou les bénévoles peuvent ne pas avoir accès à un dispositif au niveau de l'organisation ou à une adresse e-mail. Il convient donc d'accorder une attention particulière à l'utilisation des dispositifs personnels et à la question de savoir si/comment cette utilisation est contrôlée/gérée en toute sécurité dans les politiques et dans la pratique.

De même, sans accès aux technologies, aux équipements et au soutien en matière d'éducation, les réseaux sociaux et les services de messagerie traditionnels sont plus susceptibles d'être utilisés plus fréquemment dans des cadres informels qu'au sein des écoles. Il peut donc être

nécessaire d'accorder une attention particulière aux politiques, pratiques et formations au niveau de l'organisation afin de déterminer si/comment celles-ci sont utilisées et gérées en toute sécurité.

Formation et soutien

Les éducateurs et les bénévoles qui travaillent dans un cadre informel ont parfois moins les moyens de suivre une formation, d'actualiser leurs compétences ou d'accéder au soutien proposé aux éducateurs dans un cadre formel. Il peut être nécessaire de se demander comment les organisations informelles trouvent, dispensent et financent des formations et un soutien de ce type.

Le Tableau 2 identifie certains des principaux points dont les éducateurs doivent tenir compte.

10 Lignes directrices à l'intention des éducateurs

Il est admis que les enseignants/éducateurs n'ont pas individuellement le contrôle sur certains des points envisagés dans le Tableau 2 ci-dessous, tels que le filtrage et le contrôle. Ces mesures devraient être prises par l'école ou l'établissement scolaire.

Tableau 2: Principaux points dont les éducateurs doivent tenir compte

	#	Domaines essentiels à considérer	Description
Sûreté et sécurité des dispositifs	1	Assurez-vous que tous les dispositifs sont sécurisés et protégés par un mot de passe.	Comme tout un chacun, les enseignants sont vulnérables aux cyberattaques, aux logiciels malveillants, aux virus et aux piratages. Il est important que les enseignants veillent à ce que les dispositifs qu'ils utilisent soient correctement protégés (avec des mots de passe forts) et verrouillés lorsqu'ils ne sont pas utilisés (par exemple, si un enseignant doit quitter la salle, l'enseignant doit verrouiller son dispositif ou se déconnecter).
	2	Installez des logiciels antivirus et des pare-feu.	Veillez à ce que tous les dispositifs soient équipés d'un pare-feu et d'un logiciel antivirus et à ce qu'ils soient mis à jour.
Politiques	3	Toutes les écoles devraient adopter une politique qui détermine où et comment la technologie peut être utilisée au sein de l'établissement par les différentes parties prenantes et comment les incidents liés à la protection des enfants sont gérés, y compris en ligne.	Les enseignants doivent veiller à respecter la politique relative à l'utilisation des technologies mobiles et autres appareils électroniques. Il est important que les enseignants adoptent un comportement adéquat lors de l'utilisation des appareils. Les écoles doivent préciser où et quand les appareils mobiles peuvent être utilisés.
	4	Photos des élèves	Les écoles devraient adopter une politique qui précise si les photos des élèves sont autorisées ou non. Le personnel peut-il prendre des photos à des fins pédagogiques? L'autorisation correspondante a-t-elle été accordée par les parents/tuteurs/élèves eux-mêmes? Idéalement, la politique devrait prévoir qu'aucun dispositif personnel ne soit utilisé à cette fin en vue de protéger à la fois les élèves et le personnel.
Filtrage et contrôle	5	Veillez à ce que les services Internet fournis par l'école soient filtrés et contrôlés.	Les élèves ne doivent pas pouvoir accéder à des contenus préjudiciables ou inappropriés depuis le système informatique de l'école. Aucun système de filtrage ne peut être efficace à 100% et il est important d'associer ces solutions techniques à un bon enseignement et un bon apprentissage, ainsi qu'à une supervision efficace. Au minimum, le filtrage doit empêcher l'accès à des contenus illicites ainsi qu'à des contenus jugés inappropriés ou préjudiciables. À titre d'exemple, les catégories suivantes de contenus préjudiciables devraient être prises en considération: • Discrimination • Propos haineux • Consommation de drogues • Extrémisme • Pornographie • Piratage et vol de droits d'auteur • Contenu relatif à l'automutilation ou au suicide • Violence extrême

	#	Domaines essentiels à considérer	Description
Réputation en ligne/ empreinte numérique	6	Évaluez l'importance de l'empreinte numérique et de la réputation en ligne.	Les enseignants doivent être conscients du fait que ce qu'ils disent et font en ligne peut avoir une incidence sur leur réputation et celle de l'école/université. Les enseignants doivent toujours agir de manière professionnelle en ligne. Les enfants doivent également être sensibilisés à l'importance de la réputation en ligne et à la manière de la gérer efficacement.
Comment communiquer de manière professionnelle en toute sécurité	7	Gardez à l'esprit l'importance d'une communication professionnelle en ligne avec les élèves, les parents et d'autres parties prenantes.	La frontière entre la vie personnelle et la vie professionnelle d'un enseignant doit toujours être claire, y compris en ce qui concerne les activités en ligne. L'adresse e-mail de l'école doit toujours être utilisée pour toute communication entre le personnel et les élèves ou les parents. Les écoles souhaiteront peut-être s'assurer que les politiques relatives à la communication ou les codes de conduite interdisent les communications individuelles et extra pédagogiques ou sur des plates-formes autres que scolaires. Idéalement, les dispositifs personnels ne devraient pas être utilisés pour communiquer avec les élèves ou les parents/tuteurs. Les communications numériques individuelles doivent être évitées. En cas de visioconférence ou d'apprentissage à distance, les écoles doivent être claires quant aux attentes du personnel et des élèves (par exemple, penser à l'endroit où se déroule l'apprentissage/la communication numérique – en évitant la chambre à coucher, tenir compte des autres personnes qui peuvent être présentes dans la maison/salle de classe).
Comportement et vulnérabilité des élèves en ligne et impact sur leur protection et leur bien-être	8	Comprenez les risques et les avantages que peut comporter l'Internet pour les élèves.	Les enseignants doivent comprendre ce que font les enfants et les jeunes lorsqu'ils se connectent à l'Internet, ainsi que les risques et les avantages que son utilisation peut comporter.

11 Conclusion

Les technologies de l'information et de la communication (TIC) ont transformé les habitudes de vie modernes. Elles nous ont apporté les communications en temps réel et sans frontières et un accès quasiment illimité aux informations ainsi qu'à une large gamme de services innovants. En même temps, elles ont également créé de nouveaux risques d'exploitation et d'abus. Sans protection adéquate, les enfants et les jeunes – qui sont les utilisateurs les plus assidus de l'Internet – peuvent faire l'objet de sollicitations sexuelles indésirables, de harcèlement et d'exposition involontaire à des contenus violents, à caractère sexuel ou dérangeants.

Sans mécanismes appropriés pour créer un environnement numérique sûr, les enfants et les jeunes resteront vulnérables. Malgré une sensibilisation croissante au sujet des risques liés à l'utilisation non sécurisée des TIC, il reste encore beaucoup à faire. Il est donc crucial que les parents et les éducateurs discutent et décident avec les enfants et les jeunes de ce qui constitue une utilisation sûre et appropriée des TIC, ainsi qu'un comportement responsable en ligne.

En travaillant ensemble, les parents, les éducateurs, les enfants et les jeunes peuvent bénéficier des avantages des TIC, tout en minimisant les dangers qui peuvent menacer les enfants et les jeunes.

Terminologie

Les définitions ci-dessous sont principalement tirées de la terminologie existante, telle qu'élaborée dans la Convention relative aux droits de l'enfant de 1989, ainsi que par le Groupe de Travail Interinstitutionnel sur l'exploitation sexuelle des enfants dans les Principes directeurs concernant la protection des enfants contre l'exploitation et l'abus sexuels, 2016[68] (Guide de terminologie du Luxembourg), par la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, 2012[69], ainsi que par le rapport Global Kids Online, 2019[70].

Adolescent

Les adolescents sont des personnes âgées de 10 à 19 ans. Il est important de noter que le terme *adolescent* n'est pas un terme contraignant en droit international, et que les personnes de moins de 18 ans sont considérées comme des enfants, tandis que les personnes de 19 ans sont considérées comme des adultes, sauf si la majorité est atteinte plus tôt en vertu du droit national[71].

Intelligence artificielle (IA)

Au sens large, le terme désigne indistinctement des systèmes qui sont du domaine de la pure science-fiction (les IA dites "fortes", dotées d'une forme de conscience d'elles-mêmes) et des systèmes qui sont déjà opérationnels et capables d'exécuter des tâches très complexes (reconnaissance faciale ou vocale, conduite d'un véhicule – ces systèmes sont qualifiés d'IA "faibles" ou "modérées")[72].

Systèmes d'IA

Un système d'IA est un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations ou de prendre des décisions influant sur des environnements réels ou virtuels, et qui est conçu pour fonctionner à des degrés d'autonomie divers[73].

Alexa

Amazon Alexa, connu sous le nom d'**Alexa**, est un assistant virtuel optimisé par l'IA développé par Amazon. Il est capable d'interagir vocalement, de lire de la musique, de faire des listes de tâches, de programmer des alarmes, de diffuser des podcasts, de lire des livres audio et de fournir des informations en temps réel sur la météo, le trafic, les sports et autres domaines, telles que les actualités. Alexa peut également contrôler plusieurs appareils intelligents en

---

68 Terminology and Semantics (2016), Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-FR.pdf.

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

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

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

72 Conseil de l'Europe (2020), *L'IA, c'est quoi?*, https://www.coe.int/fr/web/artificial-intelligence/what-is-ai.

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

faisant office de système domotique. Les utilisateurs peuvent étendre les capacités d'Alexa en installant des "compétences" (fonctionnalités supplémentaires développées par des fournisseurs tiers et appelées plus communément "applications" dans d'autres cadres, telles que les bulletins météo et les fonctions audio)[74].

Intérêt supérieur de l'enfant

Décrit tous les éléments nécessaires pour prendre une décision dans une situation spécifique, pour un enfant ou un groupe d'enfants spécifique[75].

Enfant

Conformément à l'article 1 de la Convention relative aux droits de l'enfant, on entend par enfant toute personne âgée de moins de 18 ans, sauf si la majorité est atteinte plus tôt en vertu du droit national[76].

Exploitation et abus sexuels à l'encontre des enfants

Décrit toutes les formes d'exploitation et d'abus sexuels (Convention des Nations Unies relative aux droits de l'enfant, 1989, art. 34), par exemple "a) que des enfants [soient] incités ou contraints à se livrer à une activité sexuelle illégale; b) que des enfants [soient] exploités à des fins de prostitution ou autres pratiques sexuelles illégales; c) que des enfants [soient] exploités aux fins de la production de spectacles ou de matériel de caractère pornographique", ainsi que tout "contact sexuel qui implique généralement l'usage de la force sur une personne sans son consentement"[77]. 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[78].

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[79]. Bien que de nombreuses juridictions continuent de qualifier les images et les vidéos d'abus sexuels sur des enfants de "pédopornographie" ou d'"images indécentes d'enfants", les présentes lignes directrices désignent collectivement ces sujets sous le terme "matériel montrant des abus sexuels sur des enfants". Cette dénomination est conforme aux lignes directrices de la Commission sur

---

74 Amazon (2019), Site officiel *Alexa Skills Kit: Build Skills for Voice*, https://developer.amazon.com/en-US/alexa/alexa-skills-kit.

75 HCDH (1990) (Haut-Commissariat des Nations Unies aux droits de l'homme), *Convention relative aux droits de l'enfant,* https://www.ohchr.org/fr/professionalinterest/pages/crc.aspx.

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

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

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

79 Terminology and Semantics (2016), *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels,* http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-FR.pdf; UNICEF et Global Kids Online (2019), *Global Kids Online Comparative Report*, https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf.

le large bande et au modèle de réponse nationale de l'Alliance mondiale WePROTECT[80]. Ce terme décrit plus précisément le contenu. La pornographie se réfère à une industrie légitime et commercialisée et, comme le précise le Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels, l'utilisation de ce terme:

"peut contribuer (volontairement ou non) à diminuer la gravité, à rendre trivial, voire à légitimer ce qui constitue en réalité un abus sexuel ou une exploitation sexuelle d'enfants […]; le terme 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"[81].

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

Enfants et jeunes

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

Jouets connectés

Les jouets connectés se connectent à l'Internet grâce à des technologies telles que la WiFi et le Bluetooth, et fonctionnent généralement en association avec des applications pour permettre aux enfants de jouer de manière interactive. Selon Juniper Research, le marché des jouets connectés a atteint 2,8 milliards USD en 2015 et devrait passer à 11 milliards USD d'ici 2020. Ces jouets collectent et stockent des informations personnelles sur les enfants, notamment leur nom, leur géolocalisation, leur adresse, des photographies, ainsi que des enregistrements audio et vidéo[82].

Cyberharcèlement, également appelé harcèlement en ligne

Le cyberharcèlement décrit un acte agressif intentionnel perpétré de manière répétée par un groupe ou une personne utilisant les technologies numériques et visant une victime qui ne peut pas se défendre facilement[83]. Il consiste généralement à "utiliser les technologies numériques et l'Internet pour publier des informations blessantes sur quelqu'un, à partager délibérément des informations privées, des photos ou des vidéos de manière blessante, à envoyer des messages menaçants ou insultants (par e-mail, messagerie instantanée, chat, SMS),

---

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

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

82 Jeremy Greenberg (2017), *Dangerous Games: Connected Toys, COPPA, and Bad Security*, https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

83 Anna Costanza Baldry, Anna Sorrentino et David P. Farrington (2019), *Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities*, https://doi.org/10.1016/j.childyouth.2018.11.0058.

à répandre des rumeurs et de fausses informations sur la victime ou à l'exclure délibérément des communications en ligne"[84]. Il peut s'agir de communications directes (par chat ou SMS), semi-publiques (comme l'envoi d'un message intimidant à une liste d'adresses e-mail) ou publiques (comme la création d'un site Web visant à se moquer de la victime).

Cyberhaine, discrimination et extrémisme violent

"La cyberhaine, la discrimination et l'extrémisme violent sont une forme distincte de cyberviolence car ils visent une identité collective, plutôt que des individus [...] et sont souvent liés à la race, l'orientation sexuelle, la religion, la nationalité ou le statut migratoire, le sexe/genre et la politique"[85].

Citoyenneté numérique

La citoyenneté numérique désigne la capacité à participer de manière positive, critique et compétente à l'environnement numérique, en s'appuyant sur des compétences efficaces en matière de communication et de création, à pratiquer des formes de participation sociale respectueuses des droits de l'Homme et de la dignité humaine grâce à une utilisation responsable des technologies[86].

[84] Terminology and Semantics (2016), *Guide de terminologie du Luxembourg pour la protection des enfants contre l'exploitation et l'abus sexuels,* http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf; UNICEF et Global Kids Online (2019), *Global Kids Online Comparative Report* (Rapport comparatif de Global Kids Online), https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf.

[85] UNICEF et Global Kids Online (2019), *Global Kids Online Comparative Report* (Rapport comparatif de Global Kids Online), https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf.

[86] Conseil de l'Europe (date?), *Citoyenneté numérique et éducation à la citoyenneté numérique,* https://www.coe.int/en/web/digital-citizenship-education/home.

Maîtrise du numérique

La maîtrise du numérique consiste à posséder les compétences nécessaires pour vivre, apprendre et travailler dans une société où la communication et l'accès à l'information se font de plus en plus par le biais de technologies numériques comme les plates-formes Internet, les réseaux sociaux et les appareils mobiles[87]. Elle comprend la capacité à communiquer clairement et le fait de posséder des compétences techniques et un esprit critique.

Résilience numérique

Ce terme décrit la capacité d'un enfant à faire face émotionnellement aux préjudices causés en ligne. La résilience numérique implique, pour l'enfant, de disposer des ressources émotionnelles nécessaires pour comprendre quand il est en danger en ligne, savoir comment demander de l'aide, mettre à profit son expérience et se remettre d'une mauvaise expérience[88].

Éducateurs

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

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

Administrateurs

Ce terme décrit toute personne exerçant une fonction dans la gestion/direction de l'école.

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

Le terme *grooming* en ligne ou hors ligne, tel que défini par le Guide de terminologie du Luxembourg, désigne le processus consistant à établir ou à construire une relation avec un enfant, soit en personne, soit par le biais de l'Internet ou d'autres technologies numériques, afin de faciliter les contacts (sexuels) en ligne avec cette personne et de persuader l'enfant de s'engager dans une relation sexuelle[89]. Il s'agit d'un processus visant à inciter les enfants à avoir un comportement ou des conversations à caractère sexuel, à leur insu ou non, ou d'un processus qui implique une communication et une socialisation entre l'agresseur et l'enfant afin de le rendre plus vulnérable aux abus sexuels. Le terme "*grooming*" n'a pas été défini dans le droit international; certaines juridictions, dont le Canada, utilisent le terme "leurre d'enfants" (*luring*).

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

---

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

88 Andrew K. Przybylski et autres (2014), *A Shared Responsibility. Building Children's' Online Resilience Report*, https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.

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

Les technologies de l'information et de la communication décrivent toutes les technologies informatiques axées sur la communication. Elles comprennent tous les services et dispositifs de connexion à l'Internet tels que les ordinateurs, les ordinateurs portables, les tablettes, les smartphones, les consoles de jeu, les télévisions et les montres connectées[90]. Elles comprennent également des services tels que la radio et, entre autres, le haut débit, le matériel réseau et les systèmes par satellite.

Jeux en ligne

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

La notion d'"écosystème des jeux vidéo" comprend le fait de regarder d'autres personnes jouer à des jeux vidéo sur des plates-formes de sport électronique, de streaming ou de partage de vidéos, qui permettent généralement aux spectateurs de commenter ou d'interagir avec les joueurs et d'autres personnes du public[91].

Outils de contrôle parental

Logiciel qui permet aux utilisateurs, le plus souvent un parent, de contrôler certaines ou toutes les fonctions d'un ordinateur ou d'un autre appareil pouvant se connecter à l'Internet. Généralement, ces programmes peuvent limiter l'accès à certains types ou catégories de sites web ou de services en ligne. Certains permettent également de gérer le temps d'écran, c'est-à-dire que l'appareil peut être réglé pour que l'accès à l'Internet ne soit possible qu'à certaines plages horaires. Des versions plus avancées peuvent enregistrer tous les SMS envoyés ou reçus par un appareil. Les programmes sont normalement protégés par un mot de passe[92].

Parents, tuteurs et personnes s'occupant d'enfants

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

---

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

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

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

Informations personnelles

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

Vie privée

Le respect de la vie privée dépend souvent de facteurs tels que le partage d'informations personnelles en ligne, le fait d'avoir un profil public sur les réseaux sociaux, le partage d'informations avec des personnes qu'on a connues en ligne, le réglage des paramètres de confidentialité, le partage des mots de passe avec des amis et le souci du respect de la vie privée[93].

Sexting

Le terme "sexting" désigne couramment le fait d'envoyer, de recevoir ou d'échanger des contenus à caractère sexuels et autoproduits, y compris des images, des messages ou des vidéos, par le biais de téléphones portables et/ou de l'Internet[94]. La création, la distribution et la possession d'images d'enfants à caractère sexuel sont illégales dans la plupart des pays. Si des images d'enfants à caractère sexuel sont divulguées, les adultes ne doivent pas les regarder. La diffusion d'images à caractère sexuel par un adulte auprès d'un enfant constitue toujours un acte criminel, et lorsque cela se produit entre des enfants, elle peut causer un préjudice aux enfants; il peut alors être nécessaire de procéder à un signalement et de prendre des mesures pour supprimer les images partagées.

Sextorsion ou chantage sexuel d'enfants

La sextorsion 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)"[95].

L'Internet des objets

L'Internet des objets représente la prochaine étape vers la numérisation de la société et de l'économie, au sein de laquelle les objets et les personnes sont interconnectés par des réseaux de communication et rendent compte de leur état et/ou de l'environnement qui les entoure[96].

---

93 US Federal Trade Commission (1998), *Children's Online Privacy Protection Act*, https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.

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

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

96 Ntantko (2013), *The Internet of Things, Digital Single Market*, https://ec.europa.eu/digital-single-market/en/internet-of-things.

URL

L'abréviation signifie "Uniform Resource Locator" (identificateur uniforme de ressources) et désigne l'adresse d'une page Internet[97].

Réalité virtuelle

La réalité virtuelle est l'utilisation de l'informatique pour créer l'effet d'un monde tridimensionnel interactif dans lequel les objets semblent présents dans l'espace[98].

WiFi

La WiFi (Wireless Fidelity) est l'ensemble des normes techniques qui permettent la transmission de données sur les réseaux sans fil[99].

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

[98] NASA (date?), *Virtual Reality*, à l'adresse: https://www.nas.nasa.gov/Software/VWT/vr.html.

[99] US Federal Trade Commission (1998),*Children's Online Privacy Protection Act*, https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.

Avec·le·soutien·de:¶

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

ISBN: 978-92-61-30472-0

Publié en Suisse
Genève, 2020
Crédits photos: Shutterstock