United Nations
Educational, Scientific and
Cultural Organization

UNESCO Chair in
ICT for Development
Royal Holloway, University of London

Note d'orientation 13 Garantir la sécurité des enfants lorsqu'ils apprennent en utilisant des technologies numériques

À partir du rapport: Éduquer les personnes les plus défavorisées après la COVID-19 : orientations destinées aux gouvernements sur l'utilisation des technologies numériques

ACTE TROIS (SUR TROIS) : NOTES D'ORIENTATION

EdTech Hub
Clear evidence, better decisions, more learning.

Date November 2020

Authors Tim Unwin
Azra Naseem
Alicja Pawluczuk
Mohamed Shareef
Paul Spiesberger
Paul West
Christopher Yoo

Traduction Française Karen Ferreira-Meyers

Report homepage https://edtechhub.org/education-for-the-most-marginalised-post-covid-19/

Note d'orientation : Garantir la sécurité des enfants lorsqu'ils apprennent en utilisant des technologies numériques[1]

Contexte

L'on pense trop souvent que les technologies numériques n'apportent que des avantages. Comme ce rapport l'a souligné tout au long, il s'agit cependant d'un mythe dangereux et, pour que l'utilisation des technologies numériques soit avantageux, il est essentiel que les gouvernements mettent en place des mesures visant à atténuer les préjudices qu'elles peuvent causer. Ces dommages sont à la fois intentionnels et non intentionnels. En outre, ce qui est considéré dans une culture comme un avantage peut ne pas l'être dans une autre. Il n'y a guère d'accord international sur ce que l'on autorise ou pas sur l'internet, sur la manière de le gérer ou de le contrôler, et sur les personnes qui en sont responsables. Cependant, la plupart des juridictions et des gouvernements s'accordent sur le fait qu'il ne faut pas que les enfants subissent des préjudices du fait de leur utilisation des technologies numériques en général, et de l'Internet en particulier. Il s'agit donc d'un domaine où il faut encourager et mettre à profit la collaboration internationale.

Les enfants et les jeunes sont touchés de manière disproportionnée par les menaces du monde numérique. Les préjudices potentiels, notamment les discours de haine, la pornographie en ligne, les abus et le harcèlement sexuels, les brimades et autres formes de comportements non désirés sont bien plus importants qu'on ne l'imagine généralement. En 2019, par exemple, l'Internet Watch Foundation, basée au Royaume-Uni, a enregistré une augmentation de 28% par rapport à l'année précédente du nombre de rapports d'images et de vidéos d'abus sexuels sur des enfants.[2] Près d'un tiers de toutes les pages web actionnées par leurs analystes contenaient des images auto-générées et les trois quarts d'entre elles montraient une fille âgée de 11 à 13 ans ; 89% des sites d'hébergement se trouvaient en Europe (y compris en Russie et en Turquie). Pourtant, selon INHOPE, seuls 42 pays disposent actuellement d'une ligne d'assistance téléphonique au sein de leur réseau pour le signalement des abus sexuels sur des enfants (CSAM) ; les pays africains et asiatiques se distinguent par leur absence de ce réseau. Parmi les risques supplémentaires figurent ceux liés au manque d'intimité des enfants, à la désinformation, à la collecte de données injustifiées et à l'analyse algorithmique de leurs comportements numériques. Il existe peu d'indications sur la manière dont il faut traiter et protéger les données des enfants contre toute utilisation future non autorisée ou contraire à l'éthique. Il faut que les gouvernements s'efforcent d'établir et de suivre un code de conduite éthique localisé, adapté et à l'épreuve du temps, axé sur les enfants, et il faut que les entreprises coopèrent avec les gouvernements afin de protéger la vie privée et la sécurité des enfants.

1 Auteurs principaux Azra Naseem, Alicja Pawlucsuk et Tim Unwin.

2 Internet Watch Foundation https://www.iwf.org.uk/sites/default/files/inline-files/Briefing%20-%20IWF%20Annual%20Report%202019.pdf.

L'accès aux technologies numériques au sein des systèmes éducatifs est l'un des principaux moyens par lesquels les enfants accèdent et se rendent vulnérables à ceux qui cherchent à les exploiter par le biais des technologies numériques. Il faut que les gouvernements veillent donc à faire tout ce qui est en leur pouvoir pour limiter ces risques, former les jeunes à l'utilisation sûre des technologies numériques et poursuivre ceux qui cherchent à leur nuire. Heureusement, il existe aujourd'hui un nombre croissant de conseils judicieux à l'intention des gouvernements sur la manière de traiter ces questions. Le rapport de l'UNICEF de 2017 souligne ainsi qu'il existe trois grandes formes de risques (contenu, contact et comportement) et que ceux-ci se recoupent avec trois grands types de préjudices (agression et violence, abus sexuel et exploitation commerciale). Ils notent également que les enfants les plus vulnérables sont généralement ceux qui sont déjà les plus marginalisés, les filles, les enfants issus de ménages pauvres, ceux qui vivent dans des communautés ayant une compréhension limitée des différentes formes d'abus sexuels et d'exploitation des enfants, ceux qui sont handicapés, ceux qui ne sont pas scolarisés, ceux qui ont des problèmes de santé mentale et ceux qui appartiennent à d'autres groupes marginalisés.

En outre, la Commission sur le haut débit est parvenue en 2019 à un consensus entre ses partenaires du secteur privé et des gouvernements sur cinq éléments clés d'une déclaration universelle qui affirme leur engagement à protéger les enfants lorsqu'ils accèdent à l'internet. Pour atteindre cet objectif et pour souligner leur responsabilité dans l'éducation de tous les enfants à l'avenir numérique qui les attend, ils ont affirmé de :

- « Utiliser de manière *PROACTIVE* les technologies disponibles et développer de nouvelles technologies innovantes pour bloquer le matériel pédopornographique et empêcher que les réseaux et les services, ainsi que l'environnement informatique interne, ne soient utilisés par les délinquants pour commettre des infractions contre les enfants.

- *CONCEVOIR* des services numériques adaptés à l'âge des enfants qui répondent au mieux à leurs besoins tout en les équipant pour se protéger en ligne.

- *TRAVAILLER* collectivement, dans les milieux politiques, réglementaires, du secteur privé, des forces de l'ordre et de la sécurité nationale, pour minimiser les risques de violence, d'abus et d'exploitation des enfants en ligne.

- *PROTÉGER* la vie privée, la sécurité et la sûreté des enfants.

- *DÉFIER* les politiques, les approches, les mentalités, les outils technologiques et tout média qui, sciemment ou non, entravent la cause de la protection des enfants, en s'appuyant sur des recommandations juridiques reconnues au niveau international ».[3]

3 Broadband Commission/ITU (2019) *Child online safety universal declaration*, Geneva: ITU, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf.

Orientation

Ce guide identifie les mesures les plus importantes qu'il faut que les gouvernements prennent afin de garantir que les enfants puissent utiliser les technologies numériques en toute sécurité :

1. **Il faut que les gouvernements donnent la première priorité à ce que tous les enfants reçoivent une formation appropriée et continue à l'utilisation sûre et acceptable des technologies numériques** avant qu'ils ne soient initiés à leur utilisation dans l'enseignement et l'apprentissage.
2. Il faut que les gouvernements **promulguent une législation appropriée pour empêcher l'utilisation des technologies numériques** à des fins d'exploitation des enfants et veillent à ce que les services de police et d'autres organismes identifient les auteurs de ces actes et les traduisent en justice.
3. **Il faut que les gouvernements s'assurent qu'ils disposent de mécanismes pour faciliter la collaboration internationale en matière de sécurité des enfants en ligne**, à la fois pour garantir le partage des bonnes pratiques et afin de traduire en justice les auteurs de crimes.
4. Il faut que les gouvernements s'assurent qu'il existe **une ligne téléphonique nationale permettant de signaler tout matériel pédopornographique (CSAM)** et que celle-ci est intégrée au réseau international INHOPE.
5. **Il faut que les politiques nationales éducatives donnent mandat aux ministères et aux écoles de fournir une formation en matière de sécurité numérique à tous les acteurs du système éducatif national** (fonctionnaires, administrateurs, chefs d'établissement, enseignants, autres animateurs pédagogiques, apprenants et parents) sur la manière d'identifier les abus sexuels sur les enfants en ligne, de les signaler rapidement et en toute confiance, et de soutenir ceux qui en sont victimes.
6. **Il faut créer des espaces sûrs dans toutes les écoles et institutions éducatives** où ceux qui souffrent d'abus en ligne peuvent s'échapper des technologies numériques, apprendre en toute sécurité par d'autres moyens et acquérir les compétences nécessaires pour participer activement en tant que survivants dans les environnements numériques.
7. **Il faut que les gouvernements financent des campagnes médiatiques (télévision, radio, médias sociaux) dans les langues locales pour mettre en évidence les problèmes liés à la sécurité des enfants en ligne et la manière de les protéger.** Il convient que ces campagnes visent à créer une culture de soutien aux enfants et à leurs familles, et à supprimer la stigmatisation liée au signalement de l'exploitation et des brimades en ligne.

Exemples

Les exemples suivants illustrent des initiatives intéressantes en matière de sécurité numérique des enfants, notamment de la part des gouvernements :

- Australia, eSafety Commissioner (2019) *Safety by design overview*, Canberra: eSafety Commissioner, https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf.
- Broadband Commission/ITU (2019) *Child online safety universal declaration*, Geneva: ITU, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf.

- INHOPE hotlines, https://www.inhope.org.
- ITU (2020) *Guidelines on child online protection*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP-2020-Guidelines.aspx, including specific guidance for policy makers in multiple languages https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-E.pdf.
- UK Council for Child Internet Safety (UKCCIS), https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.
- WeProtect Global Alliance (2018) *Working examples of model national response Capabiliti4es and implementation*, https://www.end-violence.org/sites/default/files/paragraphs/download/WePROTECT%20Global%20Alliance.pdf.

Suggestions de lectures complémentaires

- Alder, R. (2015) 20 tips for creating a safe learning environment, *Edutopia*, https://www.edutopia.org/blog/20-tips-create-safe-learning-environment-rebecca-alber.
- DQ Institute (2020) *Child online safety index*, https://www.dqinstitute.org/child-online-safety-index/.
- ECPAT International and Religions for Peace (2016) *Protecting children from online sexual exploitation: A guide to action for religious leaders and communities*, New York: ECPAT International, Religions for Peace, UNICEF, https://www.unicef.org/protection/files/FBO_Guide_for_Religious_Leaders_and_Communities_ENG.pdf.
- Internet Watch Foundation (2019) *Annual report*, https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance.
- The Children's Society and Young Minds (2018) *Safety net: Cyberbullying's impact on young people's mental health: Inquiry report,* London: The Children's Society and Young Minds, https://www.alexchalk.com/sites/www.alexchalk.com/files/2018-04/pcr144b_social_media_cyberbullying_inquiry_full_report.pdf.
- UNICEF (2017) *The state of the world's children 2017: Children in a digital world*, New York: UNICEF, https://www.unicef.org/publications/index_101992.html.

Cette note d'orientation est basée sur les bonnes pratiques existantes et les conseils reçus des participants à nos consultations. N'hésitez pas à utiliser et à partager ces informations, mais veuillez respecter les droits d'auteur de toutes les œuvres incluses et partager également toute version adaptée de ces œuvres.

United Nations
Educational, Scientific and
Cultural Organization

UNESCO Chair in
ICT for Development
Royal Holloway, University of London

EdTech Hub

Clear evidence, better decisions, more learning.

Publication typesetting by User Design,
Illustration and Typesetting
www.userdesignillustrationandtypesetting.com