Plan

Objectifs du module

1 Les enfants et la technologie

1.1 Les droits des enfants à l'ère numérique

📚 Ressources

1.2 Les avantages de la technologie

🌍 Étude de cas

1.3 Utilisation de la technologie par les enfants

📚 Ressources

💡 Point de réflexion

2 Risques en ligne pour les enfants et les jeunes

2.1 Les risques en ligne

💡 Point de réflexion

(a) Contenu inapproprié

(b) Contacts inappropriés

(c) Comportement inapproprié

(d) Risques relatifs à la santé

📚 Ressource

(e) Questions liées à la consommation

🌍 Étude de cas

2.2 Abus sexuels sur enfants

💡 Point de réflexion

2.3 L'impact de la COVID-19 sur la protection en ligne des enfants

3 Mesures visant à protéger les enfants en ligne

3.1 Mesures législatives

📚 Ressource

3.2 Mesures d'autoréglementation et de réglementation collective

3.3 Mesures techniques

💡 Point de réflexion

📚 Ressources

3.4 Sensibilisation et éducation

🌍 Étude de cas

📚 Ressources

3.5 Élaboration d'une stratégie nationale

📚 Ressources

💡 Point de réflexion

4. Les parties prenantes impliquées dans la protection en ligne des enfants

4.1 Une responsabilité partagée par toutes les parties prenantes

🌍 Étude de cas

Programme Be Internet Awesome de Google

🌍 Étude de cas

4.2 Mode de collaboration des parties prenantes

💡 Point de réflexion

5. Ressources pour les initiatives de protection en ligne des enfants

🌍 Étude de cas

6. Conclusion

7. Questionnaire

Objectifs du module

Bienvenue dans le **module de connaissances sur la protection en ligne des enfants**, dans le cadre du projet GFCE-Afrique.

Quels sont les buts et objectifs de ce module ?

Ce module de connaissances consiste en une série de réponses aux questions clés que les décideurs soulèvent – ou doivent soulever – en ce qui concerne la sécurité des enfants en ligne. Les réponses sont présentées sous forme d'explications, et comprennent des études de cas, des ressources supplémentaires, des points de réflexion et d'autres options permettant l'implication supplémentaire des participants.

Les composants de ce MC peuvent être utilisés pour différents formats d'exécution :

(a) cours en ligne à votre propre rythme : les participants peuvent suivre un cours via une plate-forme d'apprentissage en ligne, étape par étape, à leur propre rythme, avec la possibilité d'échanger des avis avec d'autres personnes qui suivent le cours ; une option de téléchargement de documents est incluse.

(b) formation in situ ou webinaires : les participants peuvent utiliser le contenu comme matériel de référence ou comme base pour les présentations, avec des points de réflexion à utiliser comme exercices.

Que couvre ce module ?

Ce module de connaissances commence par examiner la façon dont les enfants utilisent la technologie et dans quelle mesure ils l'utilisent, avant de présenter les avantages et les menaces que la technologie et l'Internet présentent pour les enfants, selon une approche fondée sur les droits. Il traite ensuite des différentes mesures visant à assurer la protection des enfants en ligne, des cadres législatifs aux mesures techniques et autres initiatives de sensibilisation. Il aborde également les principaux acteurs et leurs responsabilités pour garantir le bien-être des enfants en ligne.

Que pouvez-vous espérer apprendre ?

À la fin du module, vous serez en mesure de répondre aux questions suivantes et de trouver des ressources supplémentaires les concernant :

- Que nous apprennent les dernières études sur la façon dont les enfants utilisent la technologie ? La pandémie de COVID-19 a-t-elle affecté la façon dont les enfants utilisent la technologie ?
- Pourquoi est-il conseillé aux responsables politiques d'envisager la protection des enfants en ligne à travers une approche fondée sur les droits, plutôt que de se concentrer exclusivement sur les risques et les menaces ?
- Quels sont les types de risques associés ? Chaque risque conduit-il à une menace réelle ?
- Quels sont les différents types de mesures que les parties prenantes peuvent utiliser pour protéger les enfants en ligne ?
- Quels sont les principaux domaines à prendre en compte lors de l'élaboration d'une stratégie nationale de protection des enfants en ligne ?
- Quelles voies de collaboration les parties prenantes choisissent-elles, et comment cette collaboration peut-elle être améliorée dans un contexte local ?

1 Les enfants et la technologie

L'accès à l'Internet offre de nombreuses opportunités aux enfants en matière d'éducation, de développement personnel, d'expression de soi et d'interaction avec les autres. Malgré ces nombreux avantages, les enfants et les jeunes sont cependant confrontés à certains risques lorsqu'ils utilisent l'Internet et la technologie. Si les utilisateurs de tous âges peuvent être confrontés à des risques, les enfants sont particulièrement vulnérables car ils sont en plein développement. Cette situation préoccupe depuis un certain temps les gouvernements, les parents et les éducateurs.

Avant d'examiner en profondeur les risques en ligne pour les enfants et les mesures à prendre pour les atténuer, il est important d'aborder l'Internet et la technologie dans une perspective plus large. Il s'agit notamment de comprendre les droits des enfants à l'ère

numérique, les avantages et les opportunités de l'Internet pour les enfants, ainsi que la manière dont les enfants accèdent à la technologie et l'utilisent.

1.1 Les droits des enfants à l'ère numérique

- 🎯 *Comment les questions relatives à la protection en ligne des enfants peuvent-elles être abordées par le biais d'une approche fondée sur les droits, et en quoi est-ce important ?*

Les discussions sur la protection en ligne des enfants se concentrent souvent sur les risques pour les enfants, notamment les tendances inquiétantes liées aux abus sexuels en ligne sur les enfants. Le terme « Protection en ligne de l'enfant » lui-même met l'accent sur les dangers en ligne auxquels les enfants sont confrontés. Toutefois, les politiques qui se concentrent exclusivement sur les risques en ligne peuvent compromettre le potentiel de l'Internet à renforcer l'autonomie des enfants.

Une approche fondée sur les droits, qui place l'enfant au centre, permet de trouver un équilibre entre la nécessité de protéger les enfants contre les dangers et l'appréciation des avantages de la technologie pour les enfants et des droits dont ils disposent à l'ère numérique.

Cela ne veut pas dire que la protection des enfants est mise sur la touche, loin de là. Cette approche prend plutôt comme point de départ la Convention des Nations unies relative aux droits de l'enfant (Vidéo 1) et place les droits de l'enfant au cœur de la discussion. Avec une telle approche, les praticiens peuvent se concentrer sur l'optimisation des opportunités du monde numérique pour les enfants et les jeunes, tout en favorisant un environnement en ligne sûr et sécurisé.

[Intégrer la vidéo : https://www.youtube.com/watch?v=b7_QpJ9Ki5Q

Vidéo 1. La Convention relative aux droits de l'enfant

Source : UNICEF Ghana

📚 **Ressources**

Une règle bien établie est que les droits dont les personnes bénéficient hors ligne doivent également être protégés en ligne. Cela inclut les enfants et leurs droits.

Pourtant, l'une des principales questions que les praticiens se posent est de savoir comment appliquer la Convention des Nations unies relative aux droits de l'enfant (cette convention est entrée en vigueur en 1990, à une époque où l'Internet n'en était qu'à ses prémisses) à l'ère numérique.

En 2021, la 86e session du Comité des droits de l'enfant des Nations unies a adopté quelques instruments juridiques pour expliquer dans quelle mesure la convention s'applique à l'ère numérique :

- Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement général

- Les notes explicatives de l'observation générale

- Un glossaire des principaux termes utilisés en relation avec l'Internet, tels que la signification de « minimisation des données » et de « profilage »

- Une version pour enfants qui présente les droits des enfants d'une manière qu'ils peuvent comprendre.

1.2 Les avantages de la technologie

Pour reprendre les mots de Frank La Rue, ancien rapporteur spécial des Nations unies sur la liberté d'expression, « l'Internet a considérablement amélioré la capacité des enfants et des adultes dans toutes les régions du monde à communiquer rapidement et à moindre

coût. Il est donc un moyen important pour les enfants d'exercer leur droit à la liberté d'expression et il peut servir d'outil pour aider les enfants à revendiquer leurs autres droits, notamment le droit à l'éducation, la liberté d'association et la pleine participation à la vie sociale, culturelle et politique. »

L'Internet offre une multitude d'opportunités aux enfants et aux jeunes, notamment en termes d'apprentissage, de sociabilité, d'expression de soi, de créativité et de participation par le biais de médias en ligne accessibles via des appareils fixes et mobiles.

L'utilisation de la technologie permet aux enfants d'exprimer leurs opinions et leur offre de multiples moyens de se connecter et de communiquer avec leur famille et leurs amis. Les avantages comprennent un accès plus large aux ressources éducatives et aux informations sur les services sociaux et de santé. L'Internet a amélioré l'accès à l'information partout dans le monde. Il offre donc aux enfants et aux jeunes la possibilité de faire des recherches sur la quasi-totalité des sujets d'intérêt, d'accéder aux médias du monde entier, de poursuivre des perspectives professionnelles et d'exploiter des idées pour l'avenir. En outre, l'Internet est un outil important pour les échanges culturels.

La technologie est également utilisée par les prestataires de services de protection de l'enfance, qui recueillent et transmettent des données, afin de faciliter, par exemple, l'enregistrement des naissances, la gestion des dossiers, la recherche des familles, la collecte de données et la cartographie de la violence. Comme les enfants et les familles utilisent l'Internet et les téléphones portables pour rechercher des informations et de l'aide, et pour signaler des incidents de maltraitance, ces technologies peuvent contribuer à protéger les enfants contre la violence et l'exploitation.

🌍 **Étude de cas**

Les technologies mobiles peuvent-elles améliorer l'alphabétisation ?

Une étude réalisée en 2014 par l'UNESCO a interrogé 4 000 personnes dans 7 pays (Éthiopie, Ghana, Inde, Kenya, Nigeria, Pakistan et Zimbabwe) pour savoir comment les personnes utilisent les téléphones portables pour lire, et déterminer l'impact de cette utilisation sur leurs habitudes et leurs attitudes envers la lecture.

Les chercheurs ont conclu que l'accès aux livres (via des appareils mobiles) ne suffit pas à lui seul à promouvoir l'alphabétisation. Cependant, les appareils mobiles facilitent la lecture, en particulier avec un accès à l'Internet via les téléphones portables.

1.3 Utilisation de la technologie par les enfants

- 🎯 *Comment les enfants utilisent-ils la technologie, et dans quelle mesure ?*

L'environnement en ligne évolue rapidement, et de nouvelles technologies sont constamment développées. Ce point a des conséquences importantes sur la vie des enfants.

Les recherches montrent que :

- Sur l'ensemble des utilisateurs en ligne dans le monde, un sur trois est un enfant de moins de 18 ans. Dans le monde du Nord, les enfants représentent 1 utilisateur sur 10, mais dans d'autres pays, ce chiffre atteint pratiquement la moitié de la population en ligne.
- L'appareil le plus populaire que les enfants utilisent pour accéder à l'Internet est le téléphone portable, et dans de nombreux cas, c'est souvent le seul moyen pour les enfants d'accéder à Internet.
- Dans certaines régions, les enfants accèdent à l'Internet au quotidien.
- Les enfants et les jeunes utilisent de plus en plus les messageries instantanées et la technologie portable, tandis que les sites de réseaux sociaux (comme Facebook) cèdent peu à peu la place à YouTube et à des applications plus récentes, comme Instagram et TikTok, qui servent principalement à regarder des vidéos (Figure 1).

Figure 1. Le passé, le présent et l'avenir de la technologie.

Source : Rapport Barnardo's Generation Digital (2019)

📚 **Ressources**

Il existe de multiples études portant sur la façon dont les enfants, à l'échelle du globe et de différentes régions, accèdent à l'Internet et l'utilisent. Par exemple :

- Le rapport comparatif Global Kids Online (2019), publié par l'UNICEF Innocenti, le bureau de la recherche de l'organisation. Global Kids Online est un programme multi-pays coordonné par l'UNICEF Innocenti, qui étudie les opportunités et les risques que les enfants du monde entier peuvent rencontrer en ligne.

- Le rapport EU Kids Online (2020), publié par le projet EU Kids Online, qui étudie comment les jeunes adultes européens âgés de 9 à 16 ans accèdent à l'Internet et l'utilisent.

- Les statistiques collectées par la société de sécurité Kaspersky (2019-2020), qui comprennent des tendances sur les contenus auxquels les enfants accèdent.

💡 **Point de réflexion**

La façon dont les enfants utilisent la technologie et l'Internet éclaire les processus d'élaboration des politiques et mobilise les parties prenantes pour passer à l'action. Existe-t-il des recherches sur la façon dont les enfants de votre pays ou de votre région utilisent l'Internet ? Dans l'affirmative, quelles sont les tendances ? Dans la négative, pourquoi pensez-vous qu'elles font défaut ?

2 Risques en ligne pour les enfants et les jeunes

2.1 Les risques en ligne

- 🎯 *Quels sont les risques auxquels les enfants sont confrontés en ligne ? Existe-t-il un moyen facile de les catégoriser, afin de comprendre les risques et de les combattre plus efficacement ?*

Les experts ont développé plusieurs façons d'identifier les risques en ligne. Nous pouvons résumer les principaux risques en cinq catégories : (a) contenu inapproprié, (b) contact inapproprié, (c) comportement inapproprié, (d) risques relatifs à la santé, et (e) questions liées à la consommation.

💡 **Point de réflexion**

Avant d'entrer dans les détails, il est bon de noter les conclusions de ces diverses études : bien que les enfants et les jeunes soient exposés à des risques, les risques ne conduisent pas toujours à un préjudice réel. Autrement dit, les niveaux de préjudice sont « significativement inférieurs » aux niveaux de risque, dans la mesure où les enfants pourraient prendre des risques sans nécessairement subir de préjudice. Par exemple, le contact en ligne avec des inconnus est peut-être le risque le plus grave ; or bien des enfants établissent de tels contacts. Cependant, peu d'entre eux entrent ensuite en contact hors ligne avec la personne en question, et ces rencontres ne débouchent que rarement sur un préjudice quelconque.

Que pensez-vous de cette découverte ? A-t-elle une incidence sur votre façon d'envisager la protection des enfants en ligne ? Devrait-elle influencer l'approche des parties prenantes en matière de protection des enfants en ligne ?

(a) Contenu inapproprié

Les enfants peuvent être exposés à des contenus inappropriés pour leur âge. Il s'agit notamment de contenus sexuels et adultes, qui affectent les enfants et les jeunes de différentes manières.

Les contenus liés à l'anorexie, à l'automutilation et à la drogue sont particulièrement préjudiciables aux adolescents vulnérables, qui luttent contre des problèmes d'image et d'autres problèmes personnels et sociaux.

Les contenus inappropriés comprennent également les contenus violents. Les jeux violents, par exemple, font intervenir des armes sophistiquées (présentant des caractéristiques d'armes réelles et des caractéristiques fictionnelles) et des effusions de sang. Ces dernières années, plusieurs défis en ligne ont incité de jeunes adultes à commettre des actes dangereux, voire à mettre leur vie en danger.

(b) Contacts inappropriés

Les enfants peuvent être exposés à des contacts préjudiciables et violents, tels que l'intimidation et le harcèlement, lorsqu'ils utilisent des applications et des réseaux sociaux, des salles de conversation (y compris des salles de conversation sur les jeux) et des plateformes de messagerie. Un enfant ou un jeune peut également être l'auteur d'une action inappropriée dans un contexte de pair à pair ou harceler ses pairs (ce qui est également décrit comme un comportement inapproprié).

Les contacts inappropriés peuvent inclure des activités plus graves ou dangereuses telles que la « manipulation » par des auteurs potentiels d'abus sexuels, et d'autres interactions violentes et illégales. Ce type de contact fait de l'enfant un participant à une interaction en ligne initiée par un adulte, éventuellement sans qu'il en ait conscience ou qu'il le souhaite.

(c) Comportement inapproprié

Outre la cyberintimidation et le harcèlement, des comportements tels que le partage de commentaires inappropriés, d'images indécentes générées par l'enfant lui-même (également appelées « matériel explicite généré par l'enfant lui-même ») ou d'informations personnelles sensibles peuvent exposer les enfants à des dommages plus graves. En effet, il est rare que les enfants et les jeunes aient pleinement conscience des conséquences, pour eux-mêmes et pour les autres, de la permanence des contenus publiés en ligne (tatouages numériques) ou de l'effet à long terme de leurs contenus (empreinte numérique).

(d) Risques relatifs à la santé

Les risques liés à la cyberdépendance et aux jeux en ligne sont de plus en plus évidents. Les enfants de moins de cinq ans sont plus sujets à la cyberdépendance, en particulier aux médias sociaux, en raison de leur accès précoce aux appareils électroniques.

📚 **Ressource**

En 2018, l'Organisation mondiale de la santé a reconnu le « trouble du jeu » comme un problème médical (vidéo 2). Cette situation a incité certains pays, comme le Royaume-Uni, à ouvrir des centres spécialisés dans le traitement de la cyberdépendance.

[Intégrer la vidéo : https://www.youtube.com/watch?v=lJ71KAO0mtc]

Vidéo 2. Trouble du jeu : questions et réponses (Q&R)

Source : Organisation mondiale de la santé (OMS)

(e) Questions liées à la consommation

Les risques liés à l'utilisation en ligne (souvent appelés risques liés à la consommation ou risques commerciaux) sont principalement associés à l'utilisation abusive des données et à la vie privée. Ils peuvent être interpersonnels, institutionnels et commerciaux. Ces risques comprennent l'usurpation d'identité, la violation de la vie privée, la réception de publicités inappropriées et de spams, et l'exposition à des coûts cachés (comme les applications ou les jeux invitant les utilisateurs à effectuer des achats in-app). Les données des enfants,

dont la géolocalisation, les données biométriques et d'autres informations sensibles, sont souvent collectées et traitées sans un véritable consentement éclairé, ce qui entraîne une violation de leurs droits, de leur droit à la protection contre les abus et la violence à leur droit à la vie privée.

🌍 **Étude de cas**

Les jeunes au Kenya et leur expérience en ligne

Une étude de 2013, commandée par l'UNICEF auprès de jeunes de 12 à 17 ans ayant accès à des téléphones portables et à l'Internet, était axée sur le comportement et la perception de la sécurité et des risques chez ces jeunes utilisateurs. Cette étude, intitulée Un espace public (privé) : examiner l'utilisation et l'impact des médias numériques et sociaux chez les adolescents au Kenya, a révélé les points suivants :

- Bien des jeunes considèrent que les médias numériques et sociaux font partie intégrante de leur vie et utilisent régulièrement l'Internet. Ils utilisent des plateformes de médias sociaux et des forums de discussion, accèdent à des contenus audio/vidéo, jouent à des jeux et recherchent des informations. Leurs explorations et interactions sociales peuvent occasionnellement entraîner des comportements à risque.

- Ils ont tendance à faire des distinctions floues entre les amis exclusivement en ligne et les autres amis de leur école, de leur quartier ou d'autres domaines de leur vie quotidienne, et considèrent les personnes des deux groupes comme des « amis ». Certains de ces jeunes peuvent essayer de rencontrer en personne des amis exclusivement en ligne.

- Nombre d'entre eux déclarent avoir été confrontés à des contenus sexuellement explicites sur l'Internet, et certains ont partagé ces contenus avec d'autres. Les interactions avec des amis en ligne conduisent parfois à une auto-exposition suggestive et à des conversations sexuellement explicites (Figure 2).

- Ils souhaitent s'informer sur la sécurité numérique mais préfèrent consulter leurs pairs et les informations qu'ils peuvent trouver en ligne. Ils pensent que leurs parents ne disposent peut-être pas des informations ou des compétences nécessaires.

Les parents n'ont que rarement conscience du degré d'engagement numérique de leurs enfants et ont tendance à ne pas superviser l'utilisation de l'Internet. En raison du manque de compréhension des parents à l'égard des médias numériques, les discussions sur

l'Internet et les médias sociaux portent souvent sur les restrictions imposées à l'utilisation par les jeunes.

Figure 2. Réponses des jeunes utilisateurs interrogés.

Source : Étude de l'UNICEF en 2013, A (Private) Public Space: Examining the Use and Impact of Digital and Social Media among Adolescents in Kenya

2.2 Abus sexuels sur enfants

Certains des risques décrits ci-dessus peuvent annoncer un abus sexuel sur enfants. Les enfants peuvent recevoir des contenus illégaux, tels que des images d'abus sexuels sur enfants (CSAM), et être exposés à des prédateurs, ce qui peut conduire à une manipulation et à des abus ou à une exploitation en ligne ou hors ligne.

La technologie a amplifié le problème, puisque les auteurs peuvent capturer l'exploitation par des moyens numériques (images ou vidéos). Une tendance plus récente est la commercialisation de l'abus sexuel sur enfants, notamment par le biais de l'exploitation d'enfants à distance en direct (LDCA), également appelée abus sexuel sur enfants à la demande ou trafic sexuel par Internet, dans laquelle les auteurs peuvent infliger l'exploitation en temps réel.

L'Internet, y compris le darknet, a également amplifié les problèmes, car il offre un moyen relativement facile d'accéder aux CSAM et de les consommer. Les prédateurs peuvent souvent explorer leurs penchants de manière anonyme et trouver des moyens d'échapper aux organismes chargés de l'application de la loi (ce qui fait partie du comportement typique des délinquants, comme le montre la Figure 3). Une autre préoccupation majeure, liée principalement à la retransmission en direct, est la difficulté liée à la détection de l'acte en direct, en raison du défi que représente l'interception des contenus cryptés. En outre, les agresseurs utilisent souvent les espaces en ligne auxquels les enfants ont accès pour entrer en contact avec leurs victimes.

(Il convient de noter que le terme « matériel pédopornographique » est la terminologie privilégiée pour désigner la « pédopornographie »).

Figure 3. Comportements typiques des délinquants dans l'exploitation et les abus sexuels à l'égard des enfants (CSEA)

Source : Rapport mondial d'évaluation des menaces 2019 de WeProtect

💡 **Point de réflexion**

INTERPOL indique que les images d'abus sexuel sur enfants sont « réelles et non virtuelles » :

« Les images d'abus sexuel sur enfants présentes sur le web ne sont pas virtuelles ; il s'agit d'un crime impliquant de vrais enfants et de vraies souffrances ».

2.3 L'impact de la COVID-19 sur la protection en ligne des enfants

- 🎯 *Dans quelle mesure la pandémie affecte-t-elle l'utilisation des technologies par les enfants ?*

En avril 2021, plus de 1,53 milliard d'enfants étaient concernés par la fermeture des écoles dans le monde. Les écoles sont restées ouvertes dans quelques pays seulement ; les autres ont été fermées pendant des semaines, voire, dans certains cas, jusqu'à plus d'une année scolaire complète.

Pour faire face aux fermetures, les écoles se sont souvent tournées vers l'apprentissage en ligne afin de garantir la continuité des cours. Des millions d'enfants et d'éducateurs étaient ainsi en contact par le biais de classes à distance facilitées par des plateformes telles que Microsoft Teams, Zoom et OnlineMeeting. S'il ne pouvait pas remplacer les interactions en face-à-face, l'apprentissage en ligne offrait néanmoins aux élèves une bonne option pour poursuivre leur apprentissage.

Cela signifiait également que les enfants passaient plus de temps en ligne à des fins sociales, éducatives et de divertissement.

- 🎯 *La pandémie augmente-t-elle les risques et les menaces en ligne pour les enfants ?*

Les effets des fermetures et autres confinements ont entraîné des risques accrus pour les enfants, aggravés par le fait que les restrictions limitaient l'accès des enfants aux services de soutien.

- INTERPOL a conclu que cette situation avait conduit à un signalement limité des cas d'abus sexuels sur enfants et à une augmentation de l'échange de matériel d'exploitation d'enfants par le biais de réseaux de pair à pair (voir l'étude complète). Il s'agit d'un contraste saisissant par rapport aux tendances et aux menaces qui prévalaient avant la pandémie.

- Aux États-Unis, le National Center for Missing and Exploited Children (NCMEC) a indiqué avoir reçu 4,2 millions de signalements de matériel d'abus sexuel sur enfants en ligne en avril 2020, soit 2 millions de plus qu'en mars 2020 et près de 3 millions par rapport à avril 2019.

- Au Royaume-Uni, l'Internet Watch Foundation (IWF) a également annoncé que la quantité de matériel d'exploitation avait augmenté de 89 % en seulement quatre semaines de confinement, et qu'il existait également un risque accru que les enfants soient manipulés et contraints en ligne de faire des images et des vidéos explicites d'eux-mêmes.

- L'Australian Federal Police a prévenu que les prédateurs en ligne ciblaient de nouvelles jeunes victimes en ligne. La police soupçonne que les délinquants profitent du confinement pour trouver davantage de victimes potentielles chez les enfants, car les jeunes passent plus de temps en ligne, sous une surveillance limitée des adultes.

- L'Alliance mondiale WeProtect a déclaré que les difficultés économiques et l'incapacité des délinquants à voyager en raison du confinement lié à la

COVID-19 risquaient d'augmenter le potentiel d'exploitation par retransmission en direct dans les environnements domestiques.

📚 **Ressource**

L'analyse de l'Alliance mondiale WeProtect concernant l'Impact de la COVID-19 sur l'exploitation sexuelle d'enfants en ligne (2020) rassemble encore plus de documents disponibles concernant l'impact des restrictions liées à la pandémie de COVID-19 sur les enfants, en particulier dans le cadre de l'exploitation et des abus sexuels.

3 Mesures visant à protéger les enfants en ligne

Il n'existe aucune solution unique capable d'atténuer les risques auxquels les enfants sont confrontés lorsqu'ils utilisent l'Internet. En revanche, une approche combinée permet de s'attaquer globalement aux risques.

Cette approche associe l'aspect politique, notamment la législation, l'autoréglementation et la réglementation collective, ainsi que d'autres mesures politiques visant à créer un environnement numérique approprié, au travail des organismes chargés de l'application de la loi, à l'utilisation d'outils techniques, à l'amélioration de l'éducation et de la sensibilisation, de même que des services de soutien aux enfants qui recherchent des conseils et une assistance, et aux victimes d'abus. Une telle approche est nécessaire tant au niveau national qu'au niveau mondial.

Lorsqu'il s'agit de lutter contre l'exploitation et l'abus sexuels des enfants en ligne, une approche combinée, impliquant une collaboration entre les parties prenantes au niveau mondial, est essentielle (Figure 4).

Figure 4. Une réponse stratégique mondiale à l'exploitation et aux abus sexuels à l'encontre des enfants en ligne

Source : Alliance mondiale WeProtect. La version complète est disponible ici.

3.1 Mesures législatives

- 🎯 *Quels aspects sont traités (ou criminalisés) par les lois, par opposition à d'autres mesures non contraignantes ?*

Vous souvenez-vous des catégories de risques auxquelles les enfants sont confrontés ? Nous avons mentionné cinq catégories (contenus inappropriés, contacts inappropriés, comportements inappropriés, risques relatifs à la santé et questions liées à la consommation), ainsi que le délit plus odieux d'exploitation et d'abus sexuels auquel ces risques peuvent mener.

En matière de législation, des lois spécifiques interdisent certains contenus, contacts ou comportements, avec des degrés d'interprétation variables selon les pays. En fait, certaines activités liées à des contacts ou à des comportements sont punissables en tant qu'infractions pénales dans de nombreux pays. Cela dépend largement du type de risque ou de comportement concerné.

Par exemple, en ce qui concerne l'exploitation et les abus sexuels, il existe différents instruments principaux au niveau international, qui ont inspiré d'autres instruments au niveau régional. Ces instruments internationaux comprennent :

- La Convention des Nations unies relative aux droits de l'enfant, qui, entre autres dispositions, oblige les États à « s'engager à protéger l'enfant contre toutes les formes d'abus et d'exploitation sexuelle » (Article 34).

- Le Deuxième protocole facultatif concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants (et les lignes directrices du Comité des droits de l'enfant de l'ONU), qui impose aux États d'autres obligations concernant les contenus relatifs aux abus sexuels sur les enfants, entre autres sujets.

- La Convention sur la cybercriminalité du Conseil de l'Europe (également appelée Convention de Budapest), qui impose aux États d'ériger en infraction toute forme de pornographie enfantine (Article 9).

- La Convention sur la protection des enfants contre l'exploitation et les abus sexuels (également appelée Convention de Lanzarote), qui oblige les États à prévenir toute forme d'exploitation et d'abus sexuels des enfants et à protéger les enfants (Article 4) ; à encourager le signalement des soupçons d'abus sexuels (Article 12) ; et à soutenir la mise en place de services de communication (Article 13).

- La Convention concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination de l'Organisation internationale du travail, qui demande aux membres de prendre des mesures immédiates et efficaces pour assurer l'interdiction et l'élimination des « pires formes de travail des enfants », y compris la prostitution (Article 3).

📚 Ressource

Le cadre d'évaluation de la législation du Centre international pour enfants disparus et sexuellement exploités (ICMEC) est une ressource importante pour la promulgation, la révision et la mise à jour de la législation. Introduit en 2006, le cadre est régulièrement mis à jour et comprend un « menu de concepts » à prendre en compte lors de la rédaction d'une législation.

Accédez à la dernière version, la 9e édition, publiée en 2018, et consultez l'examen de la législation de votre pays par l'ICMEC. Où en est votre pays ? Qu'est-ce qui devrait être amélioré ?

Exercice

Quelles sont les dispositions légales qui protègent explicitement les enfants en ligne dans la stratégie ou la législation de votre pays en matière de cybersécurité ?

3.2 Mesures d'autoréglementation et de réglementation collective

- 🎯 *Les mesures non contraignantes sont-elles aussi efficaces que les lois ?*

L'industrie privilégie l'autoréglementation (accord volontaire de la part de l'industrie) et la réglementation collective (combinaison de la réglementation gouvernementale et privée), qui est considérée comme une approche efficace. Bien qu'elles soient souvent non contraignantes, ces mesures ont donné de bons résultats en matière de protection des enfants contre les menaces en ligne.

Par exemple, les fournisseurs d'accès à Internet (FAI) peuvent prévoir volontairement des mesures de notification et de retrait et peuvent également filtrer certains types de contenus illégaux, tandis que les plateformes de médias sociaux peuvent fixer un âge minimum pour les enfants.

Une bonne relation de travail entre le secteur et les services répressifs, y compris des processus et des protocoles clairement définis pour travailler ensemble, est également importante. En 2008, le Conseil de l'Europe a publié ses Lignes directrices pour la coopération entre les services répressifs et les fournisseurs d'accès à Internet contre la cybercriminalité, qui sont toujours d'actualité.

En 2020, les gouvernements des cinq pays (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis), en consultation avec six entreprises de technologie (Google, Microsoft, Twitter, TikTok, Facebook et Roblox) et d'autres experts, ont lancé un document intitulé Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes volontaires pour contrer l'exploitation et l'abus sexuels des enfants en ligne) que les entreprises doivent mettre en œuvre.

3.3 Mesures techniques

- 🎯 *Quels sont des exemples de mesures techniques ? Peuvent-elles être utilisées indépendamment, à la place d'autres types de mesures ?*

Les politiques nationales s'appuient, à des degrés divers, sur des mesures techniques qui ne doivent être utilisées qu'en conjonction avec d'autres mesures. En outre, les mesures techniques peuvent être soit volontaires, comme dans de nombreux pays, soit une obligation légale. Par exemple, le filtrage des FAI s'inscrit dans les mesures d'autoréglementation de certains pays, tandis qu'il est une exigence obligatoire dans d'autres.

Diverses mesures techniques et procédurales permettent de lutter contre les abus sexuels sur les enfants. Les mécanismes de signalement par ligne directe ainsi que les demandes de notification et de retrait vont souvent de pair et constituent généralement la première ligne de défense des acteurs de l'industrie qui cherchent à éradiquer les contenus illicites dans leurs services.

Les mesures techniques consistent également à gérer des bases de données d'identification des victimes et à empêcher l'accès à des sites spécifiques, tels que les bases de données d'Europol et d'INTERPOL, qui aident à identifier les victimes d'abus sexuels sur des enfants. La technologie de hachage, qui attribue une empreinte digitale unique (ou valeur de hachage) pour identifier les images d'abus sexuels sur enfants, est devenue un outil important dans la lutte contre le CSAM. D'autres mesures techniques font appel au data mining et à l'analyse des données pour faciliter les enquêtes.

💡 **Point de réflexion**

Les lignes directes constituent généralement une première ligne de défense pour le public et l'industrie afin de signaler et de supprimer les contenus illégaux. Votre pays dispose-t-il d'une ligne d'assistance nationale pour signaler les contenus présentant des abus sexuels sur des enfants ou les cas d'exploitation d'enfants ?

📚 **Ressources**

Le guide GSMA INHOPE *Hotlines: Responding to Reports of Illegal Online Content* (2014) est une ressource utile pour la mise en place d'une ligne d'assistance.

3.4 Sensibilisation et éducation

- 🎯 *Quelle est la valeur ajoutée associée à la fourniture d'un soutien et de ressources en matière de sensibilisation et d'éducation aux parents, aux éducateurs et aux enfants eux-mêmes ?*

L'éducation et la sensibilisation des enfants, ainsi que des parents et des éducateurs, sont généralement considérées comme la première ligne de défense, d'où leur importance constante. Au niveau national, de nombreuses campagnes ont ciblé les enfants et les jeunes, les parents et les tuteurs, ainsi que les éducateurs. Une multitude de ressources de sensibilisation, en ligne notamment, est également disponible et se développe. Ces ressources fournissent généralement des conseils sur l'utilisation en toute sécurité de la technologie et de l'Internet.

Par exemple, l'initiative COP sur la protection en ligne des enfants de l'Union internationale des télécommunications (UIT) fournit des lignes directrices à l'intention des enfants, des parents et des tuteurs, ainsi que des éducateurs, de l'industrie et des décideurs (publiées en 2020). Il est également important de fournir des ressources dans différentes langues. La Journée pour un Internet plus sûr (Safer Internet Day) est organisée chaque année, en

février, par le réseau INSAFE en vue de promouvoir l'utilisation sûre de l'Internet et des technologies mobiles, en particulier chez les enfants et les jeunes du monde entier. Ce ne sont là que quelques exemples.

🌍 **Étude de cas**

Une étude menée au Kenya fournit plusieurs recommandations axées sur l'éducation

L'étude de l'UNICEF que nous avons mentionnée précédemment, A (Private) Public Space: Examining the Use and Impact of Digital and Social Media among Adolescents in Kenya (2013), a formulé plusieurs recommandations. Notamment :

- Commencer par comprendre l'utilisation et la sécurité numériques du point de vue des jeunes, avant de concevoir le contenu des programmes d'information sur la sécurité numérique…
- Impliquer les parents et les autorités scolaires dans les programmes de sécurité numérique destinés aux jeunes.
- Équilibrer les messages de sécurité numérique en mettant l'accent sur l'utilité de l'Internet dans des domaines tels que l'éducation, la recherche et le commerce.
- Encourager les jeunes à utiliser également l'Internet comme ressource pour signaler les abus en ligne ou hors ligne ou tout autre comportement inapproprié.
- Créer des campagnes de sécurité numérique en ligne et hors ligne destinées à l'ensemble des médias traditionnels et numériques […] que les jeunes ont l'habitude de consulter et d'utiliser.
- Encourager les jeunes champions de la sécurité numérique qui peuvent s'adresser à leurs pairs par le biais des médias numériques, des spots audio et vidéo sur les médias de masse, et des espaces hors ligne comme les écoles et les universités.

📚 Ressources

Le Centre international pour les enfants disparus et exploités (ICMEC) est l'une des nombreuses organisations qui ont fourni des ressources éducatives sur la protection en ligne des enfants pendant la pandémie de COVID-19. Par exemple, ces courtes vidéos, destinées aux professionnels des services à la jeunesse, abordent des questions spécifiques.

[Intégrer

Introduction à la protection des enfants pendant la pandémie

Question 1 - Que devons-nous surveiller ?

Question 2 - Qui est vulnérable en ce moment ?

Question 3 - Comment puis-je soutenir les collègues et les parents ?

Question 4 - Quelles sont les options de signalement et de réponse disponibles ?

Question 5 - Quelles ressources sont utiles en ce moment ?]

La page de ressources COVID-19 de l'ICMEC propose de nombreuses autres ressources pour traiter d'autres questions relatives à la protection de l'enfance, notamment du contenu multilingue, des webinaires (enregistrements) pour les parents et les éducateurs, et des ressources pour les enfants.

Campagnes de sensibilisation (communauté ACE à partager)

Dans le cadre de la Journée pour un Internet plus sûr en 2021, le régulateur Communications Authority of Kenya, GSMA et les opérateurs mobiles Safaricom PLC, Airtel Kenya, Telkom Kenya et Jamii Telecommunications Ltd ont lancé un microsite doté d'un guide interactif sur la protection en ligne des enfants, sous l'égide de l'initiative GSMA #WeCare. Le site offre des conseils de sécurité pour les enfants et les parents/tuteurs dans quatre domaines clés : Conseils intelligents Cyberharcèlement Fraude en ligne Cyberdépendance.

3.5 Élaboration d'une stratégie nationale

- *🎯 Pourquoi une stratégie nationale de protection en ligne des enfants est-elle essentielle ?*

Afin de protéger les enfants contre les risques en ligne tout en favorisant l'accès à l'information et l'utilisation sûre de la technologie et de l'Internet, il est nécessaire d'élaborer, d'exécuter et d'évaluer une stratégie de protection en ligne des enfants inclusive et à multiples facettes. Cette stratégie peut garantir une action coordonnée et une coopération à tous les niveaux. Pour être efficace, une stratégie doit comporter des mesures et des activités ciblées, notamment les ressources financières et humaines nécessaires à sa mise en œuvre.

L'Union internationale des télécommunications (UIT), en collaboration avec des partenaires experts, a élaboré différentes lignes directrices sur la sécurité en ligne des enfants dans le cadre de son initiative COP de protection en ligne des enfants (au sein de son Programme mondial de cybersécurité, cadre de collaboration internationale sur le cyberespace). Ces lignes directrices ont la particularité d'avoir été rédigées à l'intention de groupes de parties prenantes spécifiques et de répondre aux rôles et aux besoins particuliers de ces derniers.

En particulier, les lignes directrices à l'intention des décideurs offrent aux gouvernements et aux responsables politiques « un cadre convivial et flexible qui soutient l'élaboration de mesures ciblées et efficaces garantissant la protection en ligne des enfants au niveau national ».

📚 Ressources

Les lignes directrices de l'UIT sur la protection en ligne des enfants constituent un ensemble complet de recommandations, destinées à toutes les parties prenantes concernées,

concernant la manière de contribuer au développement d'un environnement en ligne sûr et responsabilisant pour les enfants et les jeunes.

Il existe quatre séries de lignes directrices sur la protection en lignes des enfants (COP) pour 2020 :

- Lignes directrices à l'intention des décideurs ;

- Lignes directrices à l'intention des entreprises ;

- Lignes directrices à l'intention des parents et des éducateurs ; et

- Lignes directrices à l'intention des enfants.

- 🎯 *Quelles sont les étapes, les exigences et les mesures à prendre en compte pour formuler une stratégie nationale sur la sécurité des enfants en ligne ?*

D'un point de vue pratique, les Lignes directrices de l'UIT sur la protection en ligne des enfants à l'intention des décideurs fournissent une « liste de contrôle nationale » des exigences et des mesures susceptibles de gérer les risques, pour aider les décideurs à planifier une stratégie nationale.

La liste de contrôle repose sur plusieurs domaines clés. Le Tableau 1, extrait des lignes directrices, présente divers paramètres que les décideurs doivent prendre en considération.

	#	**Principaux paramètres à prendre en considération**
Cadre juridique	1	Analyser le cadre juridique existant pour déterminer s'il prévoit tous les mécanismes juridiques nécessaires pour permettre aux organismes d'application de la loi et aux autres organismes

		compétents de protéger les personnes de moins de 18 ans sur toutes les plateformes connectées à l'Internet.
	2	Établir, mutatis mutandis, que tout acte commis sur un enfant qui est illégal dans le monde réel est illégal dans le monde virtuel et que les règles sur la protection des données et de la vie privée dans le cyberespace s'appliquent également aux enfants.
Cadre réglementaire	3	Envisager d'élaborer des politiques de réglementation, par exemple des politiques d'autoréglementation ou de réglementation collective, ou un cadre réglementaire complet. Le modèle d'autoréglementation ou de réglementation collective pourrait inclure l'élaboration et la publication de codes de bonnes pratiques ou d'exigences de base en matière de sécurité en ligne, tant pour contribuer à stimuler, à coordonner ou à organiser et à soutenir la participation de toutes les parties prenantes pertinentes, que pour formuler et appliquer plus rapidement les mesures idoines en réponse aux évolutions technologiques. Un modèle réglementaire pourrait définir les attentes et les obligations à l'échelle des parties prenantes et les consacrer dans un cadre juridique. Des sanctions en cas de violation des lois peuvent aussi être envisagées.
Signalement − Contenus illicites	4	Veiller à l'établissement et à la promotion à grande échelle d'un mécanisme permettant de fournir des moyens simples et compréhensibles de signalement des contenus illicites trouvés sur l'Internet (par exemple, une ligne d'assistance téléphonique nationale capable de fournir une réponse rapide, d'obtenir le retrait des contenus illicites ou de les rendre inaccessibles). Les entreprises devraient disposer de mécanismes pour identifier, bloquer et retirer les contenus relatifs aux abus

		sexuels commis à l'encontre d'enfants en ligne, en mobilisant tous les services pertinents pour leurs organisations.
Signalement − Préoccupations des utilisateurs	5	Les entreprises devraient donner aux utilisateurs la possibilité de signaler des éléments préoccupants et des problèmes et y répondre en conséquence.
Acteurs et parties prenantes	6	Mobiliser toutes les parties prenantes concernées par la protection en ligne des enfants, en particulier : - les organismes gouvernementaux ; - les organismes d'application de la loi ; - les organismes de services sociaux ; - les fournisseurs de services Internet et d'autres fournisseurs de services électroniques ; - les fournisseurs de réseau de téléphonie mobile ; - les fournisseurs de réseaux Wi-Fi publics ; - d'autres sociétés de haute technologie pertinentes ; - les organisations d'enseignement ; - les organisations de parents ; - les enfants et les jeunes ; - les agences de protection de l'enfance et d'autres ONG compétentes ; - le monde de l'enseignement et de la recherche ; - les propriétaires de cybercafés et les autres fournisseurs d'accès public (bibliothèques, télécentres, PC Bangs, salles de jeux en réseau, etc.).
Recherche	7	Entreprendre des travaux de recherche concernant les divers acteurs et les diverses parties prenantes au niveau national afin de connaître leurs points de vue, leurs données d'expérience, leurs préoccupations et leurs initiatives en matière de protection

		en ligne des enfants. Ces travaux devraient aussi permettre de connaître la portée des responsabilités et les activités existantes et celles qu'il est prévu de mener pour assurer la protection en ligne des enfants.
Éducation, maîtrise des outils numériques et compétences numériques	8	Développer des volets consacrés à la maîtrise des outils numériques dans le cadre des programmes scolaires nationaux adaptés à l'âge des enfants et destinés à tous les enfants.
Ressources pédagogiques	9	Renforcer le savoir et l'expérience de toutes les parties prenantes et élaborer des messages et des contenus sur la sécurité sur l'Internet qui soient conformes aux lois et aux normes culturelles locales et qui présentent la garantie d'une distribution efficace et d'une diffusion appropriée auprès du public cible visé. Envisager de faire appel aux médias de masse pour promouvoir les messages de sensibilisation. Mettre au point une documentation qui met en avant les aspects positifs et stimulants de l'Internet pour les enfants et les jeunes et proscrit tout message alarmant. Encourager un comportement en ligne positif et responsable. Envisager d'élaborer des ressources pour aider les parents à évaluer la sécurité en ligne de leurs propres enfants et à apprendre comment réduire autant que possible les risques et optimiser les possibilités qui s'offrent à leur propre famille, grâce à une formation ciblée.
Protection de l'enfance	10	Veiller à la mise en place de mécanismes de protection des enfants universels et systématiques en vertu desquels toutes les personnes qui travaillent avec les enfants (protection sociale, santé, écoles, etc.) sont dans l'obligation d'identifier les cas d'abus et de préjudice qui se produisent en ligne, d'intervenir à cet égard, et de signaler ces cas.

Sensibilisation au niveau national	11	Organiser des campagnes de sensibilisation au niveau national afin de mettre en avant les questions liées à la protection en ligne des enfants auprès du plus grand nombre. Il peut être utile de s'inspirer de campagnes mondiales telles que la Journée pour un Internet plus sûr, en vue d'organiser une campagne.
Outils, services et paramètres	12	Envisager le rôle que peuvent jouer les paramètres des dispositifs, les outils techniques (tels que les programmes de filtrage) et les applications et fonctionnalités de protection des enfants. Encourager les utilisateurs à être responsables lorsqu'ils utilisent leurs dispositifs, en les incitant à effectuer des mises à jour du système d'exploitation et à utiliser des logiciels et des applications de sécurité appropriés.

Tableau 1. Élaboration d'une stratégie nationale de protection en ligne des enfants : Liste de vérification nationale - Principaux paramètres à prendre en considération

Source : Ce tableau est extrait des Lignes directrices de l'UIT sur la protection en ligne des enfants à l'intention des décideurs 2020

💡 **Point de réflexion**

Votre pays dispose-t-il d'une stratégie nationale sur la protection en ligne des enfants ? Ou est-il en train d'en élaborer une, ou de mettre à jour une stratégie existante ? Dans l'affirmative, quelle partie prenante a été le moteur de cette stratégie ? Et quels sont les domaines clés les plus difficiles à aborder ?

Dans la négative, quel a été le principal obstacle à l'élaboration d'une stratégie nationale ? Qui serait/pourrait être la force motrice d'une telle initiative ?

4. Les parties prenantes impliquées dans la protection en ligne des enfants

Comme nous l'avons vu dans la section précédente, il n'existe pas de solution unique pour atténuer les risques auxquels les enfants sont confrontés lorsqu'ils utilisent l'Internet. En revanche, une approche combinée peut être utilisée pour s'attaquer globalement aux risques.

L'approche combinée nécessite l'implication de toutes les parties prenantes, notamment les parents, les éducateurs, les gouvernements et l'industrie (Figure 6).

Figure 6. Un écosystème Internet plus sûr

Source : Rapport de la Commission sur le haut débit UIT/UNESCO concernant la sécurité en ligne des enfants (2019)

4.1 Une responsabilité partagée par toutes les parties prenantes

- 🎯 *Quels sont les rôles et les responsabilités de chaque partie prenante ?*

Les parties prenantes impliquées dans la protection en ligne des enfants comprennent :

- Les gouvernements nationaux sont tenus de protéger les enfants et les jeunes en ligne et hors ligne. Certaines des principales exigences en matière de protection en ligne consistent à garantir que la législation nationale est adaptée à cet objectif, que les organismes d'application de la loi disposent des compétences adéquates et que des lignes d'assistance téléphonique sont en place.

- Au niveau national, les organismes chargés de l'application de la loi doivent disposer des capacités et des compétences nécessaires pour lutter contre les abus sexuels en ligne sur les enfants. Sur la base de preuves, fournies en partie par les contenus relatifs aux abus sexuels sur les enfants, les organismes chargés de l'application de la loi s'efforcent de localiser les victimes et de les mettre à l'abri, ainsi que de localiser les auteurs. Les organismes chargés de l'application de la loi travaillent également aux niveaux régional et international pour lutter contre les abus sexuels sur les enfants en ligne. Les capacités, les compétences et les autres ressources nécessaires à l'application de la loi sont cruciales : si les lois ne sont pas réellement appliquées, les enfants ne peuvent pas être protégés comme ils le devraient.

- L'industrie a également la responsabilité de veiller à garantir un environnement en ligne sûr et sécurisé. Les fournisseurs de services peuvent jouer un rôle clé dans la création d'un tel environnement, et de nombreux outils, tels que les filtres et les mécanismes de signalement, peuvent être utilisés à cet effet. L'industrie est favorable à l'autoréglementation et à la réglementation collective, qui ont été reconnues comme une approche efficace. En outre, l'industrie a été particulièrement active dans le domaine de la lutte contre les abus sexuels sur les enfants en ligne. Outre les acteurs individuels du secteur des TIC, différentes coalitions industrielles ont également été formées (nous y reviendrons dans la suite de ce document).

- Les ONG dédiées aux enfants ainsi que les lignes d'assistance et d'aide aux enfants sont des parties prenantes clés dans la lutte contre l'exploitation et l'abus sexuels des enfants, en ligne et hors ligne. Elles sont des partenaires précieux pour comprendre l'ampleur et la nature du problème, mais aussi pour fournir des conseils et un soutien aux victimes d'abus. Les ONG nationales peuvent également coopérer par le biais de réseaux internationaux.

- Les parents et les éducateurs ont la responsabilité de guider et d'aider les enfants, en particulier les plus jeunes, à utiliser les services qui favorisent les comportements positifs. Ils jouent un rôle important dans l'éducation et la sensibilisation, qui sont considérées comme une première ligne de défense importante pour atténuer les risques.

🌍 **Étude de cas**

Programme Be Internet Awesome de Google

En 2020, Google a lancé son programme de sécurité en ligne pour les enfants, Be Internet Awesome, en Afrique du Sud et au Nigeria. Grâce à ce programme, les enfants acquièrent les qualités, telles que l'intelligence, la vigilance, la force, la gentillesse et le courage, qui leur permettent d'explorer le monde en ligne en toute confiance. Le programme Be Internet Awesome offre des ressources aux éducateurs et aux enfants dans cinq domaines fondamentaux :

- Partagez avec prudence : empreinte numérique et communication responsable
- Ne tombez pas dans le panneau : hameçonnage, escroqueries et sources crédibles
- Sécurisez vos secrets : sécurité en ligne et mots de passe
- C'est cool d'être gentil : combattre les comportements négatifs en ligne
- En cas de doute, exprimez-vous : contenu douteux et scénarios

🌍 **Étude de cas**

Comment des parties prenantes au Kenya se sont associées en vue de mener une campagne nationale sur la sécurité des enfants

En septembre 2021, l'Autorité des communications du Kenya a lancé une campagne de sensibilisation de trois mois pour protéger les enfants et leur empreinte numérique, alors qu'elle intensifie ses efforts en faveur d'une utilisation responsable de l'Internet.

Les parties prenantes impliquées, avec l'Autorité des communications, sont les suivantes :

- Le ministère de l'éducation
- Le ministère des TIC, de l'innovation et de la jeunesse
- Le secteur de la justice, sous l'égide du Conseil national de l'administration de la justice
- Le secteur privé, qui étudie les moyens de déployer la technologie pour faciliter l'enseignement et l'apprentissage des enfants pendant la fermeture des écoles.

4.2 Mode de collaboration des parties prenantes

- 🎯 *Comment les parties prenantes collaborent-elles aux niveaux national, régional et mondial ? Quels sont les principaux exemples ?*

La protection des enfants en ligne nécessite l'implication de toutes les parties prenantes, qui doivent agir ensemble de manière efficace et coordonnée pour protéger les enfants en ligne,

et pour lutter contre les abus sexuels d'enfants en ligne. Les efforts en cours, qui sont particulièrement pertinents dans la lutte contre les abus sexuels à l'égard des enfants, comprennent :

- Les partenariats public-privé, tels que l'Alliance mondiale WePROTECT, le Partenariat mondial pour mettre fin à la violence envers les enfants et l'Alliance pour une meilleure protection des mineurs en ligne.
- Des coalitions financières, telles que la Coalition financière américaine contre l'exploitation sexuelle des enfants et la Coalition financière Asie-Pacifique contre l'exploitation sexuelle des enfants.
- Des alliances industrielles, telles que la Coalition de la technologie, et l'Alliance des opérateurs mobiles contre les contenus pédophiles de la GSMA.
- Les agences des Nations unies, telles que l'UNICEF, l'UNESCO, l'Office des Nations unies contre la drogue et le crime (ONUDC), l'UIT et la Commission sur le haut débit UIT/UNESCO, dont son Groupe de travail sur la sécurité des enfants en ligne.
- Les ONG nationales, qui peuvent coopérer par le biais de réseaux internationaux, comme ECPAT International et l'ICMEC.
- Les lignes d'assistance téléphonique pour enfants et les ONG, telles que Child Helpline International et Childnet International.
- D'autres initiatives et organisations régionales et mondiales axées sur la sécurité en ligne des enfants, telles que Better Internet for Kids, EU Kids Online et Global Kids Online.

💡 **Point de réflexion**

L'implication de toutes les parties prenantes est essentielle. Dans votre pays, comment les différentes parties prenantes sont-elles impliquées dans la sécurité en ligne des enfants ?

5. Ressources pour les initiatives de protection en ligne des enfants

Les initiatives de protection en ligne des enfants nécessitent des ressources : des personnes (champions) et des fonds. Dans la plupart des cas, les ressources destinées à soutenir ces initiatives proviennent du gouvernement, des organisations internationales et de la société civile.

🌍 **Étude de cas**

Africa Online Safety Fund

En partenariat avec la société sud-africaine de conseil en impact social Impact Amplifier et l'Institute of Strategic Dialogue, Google a annoncé à l'occasion de la Journée pour un Internet plus sûr la création d'un fonds panafricain d'un million de dollars US pour soutenir des idées innovantes autour de la vie privée, la confiance et la sécurité des familles en ligne dans toute l'Afrique subsaharienne, en 2020.

L'Africa Online Safety Fund avait pour but de soutenir des solutions transformatrices et catalytiques s'attaquant au vol d'identité, à l'intimidation et au harcèlement, au trafic sexuel, aux crimes haineux, au recrutement de terroristes et à la propagande terroriste, à la désinformation et aux escroqueries financières, en particulier pour les femmes et les enfants au Nigeria, en Afrique du Sud, au Kenya, au Sénégal, en Éthiopie et en Côte d'Ivoire.

Le programme a honoré 8 organisations, qui ont reçu une subvention de 100 000 dollars US pour des solutions transformatrices, et 18 lauréats, qui ont reçu une subvention de 10 000 dollars US pour des projets catalytiques.

6. Conclusion

Ce module a examiné les opportunités et les risques auxquels sont confrontés les enfants lorsqu'ils utilisent la technologie. Ce module contient quelques points importants à retenir, que nous allons maintenant résumer.

Premièrement, les discussions sur la protection en ligne des enfants ont tout à gagner d'une approche basée sur les droits, qui place les droits des enfants au cœur de la discussion. Avec une telle approche, les praticiens peuvent se concentrer sur l'optimisation des opportunités du monde numérique pour les enfants et les jeunes, tout en favorisant un environnement en ligne sûr et sécurisé.

Deuxièmement, il ne fait aucun doute que les enfants sont exposés à de nombreux risques en ligne, que nous avons identifiés comme suit : (a) contenus inappropriés, (b) contacts inappropriés, (c) comportements inappropriés, (d) risques relatifs à la santé, et (e) questions liées à la consommation. Sans minimiser ces risques, il est bon de retenir les conclusions de diverses études : si les enfants et les jeunes sont exposés à des risques et peuvent prendre des risques en ligne, ils ne subissent pas nécessairement un préjudice réel.

Troisièmement, aucune solution unique ne peut atténuer les risques auxquels les enfants sont confrontés lorsqu'ils utilisent l'Internet. En revanche, une approche combinée permet de s'attaquer globalement aux risques. Cette approche associe l'aspect politique au travail des organismes chargés de l'application de la loi, à l'utilisation d'outils techniques, à l'amélioration de l'éducation et de la sensibilisation, de même que des services de soutien aux enfants qui recherchent des conseils et une assistance, et aux victimes d'abus. Une telle approche est nécessaire tant au niveau national qu'au niveau mondial.

Quatrièmement, en ce qui concerne les abus et l'exploitation des enfants, la technologie a amplifié le problème puisque les auteurs peuvent capturer ces abus par des moyens numériques (images ou vidéos). L'Internet, y compris le darknet, a également amplifié les problèmes, car il offre un moyen relativement facile d'accéder au matériel pédopornographique et de le consommer. Cette situation soulève des problèmes importants pour toutes les parties prenantes.

Cinquièmement, la lutte contre l'exploitation et l'abus sexuels des enfants en ligne nécessite également une approche combinée, impliquant une collaboration entre les parties prenantes aux niveaux national, régional et mondial.