BOÎTE À OUTILS POUR LA PROTECTION EN LIGNE DES ENFANTS

FAIRE DE LA SÉCURITÉ EN LIGNE DES ENFANTS UNE RÉALITÉ

5RIGHTS FOUNDATION

End Violence Against Children

À propos de 5Rights Foundation

Construire le monde numérique que les jeunes méritent

5Rights développe de nouvelles politiques, crée des cadres innovants, élabore des normes techniques, publie des recherches, prend en compte les récits reçus et veille à ce que les droits et les besoins des enfants soient reconnus et priorisés dans le monde numérique.

Nous mettons l'accent sur les changements réalisables et notre travail est pris pour exemple et largement utilisé dans le monde entier. Nous travaillons avec les gouvernements, les institutions intergouvernementales, les associations professionnelles, les universitaires, les entreprises, les ONG et les enfants afin que les produits et services numériques puissent avoir un impact positif sur les expériences vécues par les jeunes. La Convention des Nations Unies relative aux droits de l'enfant définit un enfant ou un adolescent comme toute personne âgée de moins de 18 ans.

La présente publication a été produite avec le soutien financier du Partenariat mondial End Violence Fund [Partenariat mondial pour l'élimination de la violence envers les enfants], dans le cadre de son initiative Safe Online. Le Fonds End Violence apporte un soutien financier aux programmes qui fournissent des solutions pratiques et innovantes pour protéger les enfants contre l'exploitation et les abus en ligne.

Les opinions, constatations, conclusions et recommandations qui y sont exprimées sont celles de 5Rights Foundation et ne reflètent pas nécessairement celles du Partenariat mondial End Violence Fund.

5RIGHTS FOUNDATION

End Violence Against Children

Table des matières

= Rendez-vous ici pour accéder à des informations clés

01 Introduction 6

02 Comment l'utiliser 9

03 Pourquoi les droits de l'enfant sont-ils importants 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 Dix domaines d'action politique 37

06 Documents clés 169

07 Glossaire 174

08 Politique modèle 180

PRÉFACE

« En cette période sans précédent, la puissance, la promesse et le danger de la technologie numérique ne peuvent être sous-estimés. En œuvrant ensemble, les entités composant la communauté internationale pourront veiller à ce que la technologie soit exploitée à bon escient, saisir l'occasion de gérer son impact et veiller à ce qu'elle offre des conditions d'accès équitables pour tous.

Les générations futures jugeront si la génération actuelle a su ou non saisir les opportunités offertes par l'ère de l'interdépendance numérique. Le temps est venu d'agir. »

António Guterres
Secrétaire Général des Nations Unies
Feuille de route du Secrétaire général pour la coopération numérique, juin 2020

PRÉFACE

« Nous ne pourrons pas construire un avenir durable si nous ne sommes pas en mesure de faire en sorte que les enfants puissent grandir en sécurité et à l'abri de la violence et des préjudices, y compris dans les environnements numériques. Même si, en principe, nous avons tous une vision de ce à quoi un monde numérique sûr et habilitant pour les enfants devrait ressembler, cela se complique grandement dès lors qu'il s'agit de la traduire en politiques, en réglementations, en actions, en produits et en services réels.

Notre espoir est que cette boîte à outils pour la protection en ligne des enfants constitue une partie de la solution à ce problème, un guide pratique pour les responsables politiques, qui simplifie les questions clés que nous devons aborder si nous voulons rendre Internet sûr pour les enfants. »

Dr. Howard Taylor
Directeur exécutif
Partenariat mondial End Violence Fund

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 1

01 **Introduction** 6

02 Comment l'utiliser 9

03 Pourquoi les droits de l'enfant sont-ils importants 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 Dix domaines d'action politique 37

06 Documents clés 169

07 Glossaire 174

08 Politique modèle 180

SECTION SUIVANTE >

Introduction

Dans un monde de plus en plus connecté, la nécessité d'un environnement numérique sûr et habilitant pour les enfants n'a jamais été aussi grande. Les responsables politiques du monde entier s'efforcent de définir les règles d'engagement entre les enfants et le monde numérique. La publication de la feuille de route pour la coopération numérique du Secrétaire général des Nations unies ne saurait d'ailleurs être plus claire à cet égard.[1] Cette boîte à outils est conçue pour aider les responsables politiques et les praticiens, en offrant une approche accessible et pratique pour construire un monde numérique qui aide les enfants, en leur permettant de s'épanouir à la fois en ligne et hors ligne.

La boîte à outils décrit la feuille de route à mettre en application pour garantir que le monde numérique soit sûr et respectueux des droits des enfants. Elle divise ses obligations en dix domaines pour soutenir la mise en œuvre des principaux accords et cadres internationaux suivants : les objectifs de développement durable (ODD) ; l'observation générale n° 25 de la CIDE (2021) sur les droits des enfants dans l'environnement numérique ; le modèle de réponse nationale de WeProtectGlobal Alliance ; les directives de l'Union internationale des télécommunications sur la protection en ligne des enfants.

Cette boîte à outils ne vise pas à remplacer les accords et cadres régionaux, nationaux ou internationaux existants, mais fournit plutôt des exemples de meilleures pratiques du monde entier, décrit des approches détaillées dans chaque domaine politique et définit les mesures que les individus et les équipes chargés de la protection des enfants en ligne doivent prendre. En tant que tel, c'est un outil permettant aux responsables politiques du monde entier d'accepter les obligations qui sont déjà les leurs.

Garantir la protection en ligne ne consiste pas seulement à répondre aux risques et aux préjudices : cela suppose de concevoir activement un environnement numérique sûr pour chaque enfant. Lorsqu'on sait qu'une personne sur trois en ligne a moins de 18 ans, on comprend que l'importance cruciale de la technologie numérique dans la vie des enfants signifie que celle-ci doit être pensée, dès la conception et par défaut, en incluant leur confidentialité, leur sécurité et leurs droits. Cette approche préventive et holistique est reflétée dans la boîte à outils, qui fournit une feuille de route aux gouvernements, aux États-nations et aux organisations, pour construire, revoir ou améliorer leurs politiques et pratiques en matière de droits de l'enfant. Elle permettra à tous les acteurs de la chaîne de responsabilité de jouer leur rôle dans l'élaboration d'une approche globale de la protection des enfants en ligne, qui évoluera au fil du temps. La boîte à outils est conçue pour être utilisée par les responsables politiques du monde entier, y compris ceux des pays nouvellement connectés, et pour être accessible et transférable dans différents contextes et situations.

Au nom de 5Rights et de notre communauté, je tiens à remercier le Secrétaire général *António Guterres* pour son leadership visionnaire à l'heure de fournir une feuille de route pour un monde connecté et pour avoir compris et reconnu que si le monde connecté n'était pas sûr pour les enfants et ne respectait pas leurs droits, alors ce monde ne tiendrait pas sa promesse d'offrir un monde meilleur à chacun. Je tiens également à souligner que le travail initial sur lequel se fonde cette boîte à outils a été entrepris au nom du Gouvernement rwandais et que nous lui sommes reconnaissants de son soutien et de son autorisation de l'utiliser ici. Nous tenons également à remercier le Professeur Julia Davidson OBE et le Dr Susie Alegre pour leurs contributions à ce document. Nous souhaitons aussi saluer le soutien généreux du Partenariat mondial End Violence Fund, qui nous a permis d'élaborer la politique de protection en ligne des enfants pour le Gouvernement rwandais, et qui a par la suite vu le potentiel de la transformer en quelque chose dont tous les pays pourraient bénéficier.

La boîte à outils doit sa sagesse et sa structure au travail de nombreux autres. Il s'agit, entre autres, du Comité des droits de l'enfant des Nations Unies, de WeProtect Global Alliance, du Partenariat mondial End Violence Fund, de l'University of East London, de l'Université du Rwanda, de la Fondation 5Rights et des nombreux États, organisations intergouvernementales mondiales et communautés académiques, de protection de l'enfance et d'application de la loi sur les travaux desquels elle s'appuie. Nous saluons leur travail et les remercions pour leur travail, leur engagement et leurs contributions. Et puis, plus que tout, la boîte à outils doit son approche aux centaines d'enfants et de jeunes qui nous ont dit vouloir s'engager dans le monde numérique, de manière créative, sûre et sans peur : cette boîte à outils est la leur.

Baronne Beeban Kidron OBE
Fondatrice et présidente, 5Rights Foundation

1. Feuille de route du Secrétaire général des Nations Unies pour la coopération numérique, Nations Unies, 2020.

SECTION SUIVANTE >

« En écrivant des articles, je partage mon point de vue sur le féminisme, et un plus grand nombre de gens le liront, comme tout le monde est sur les réseaux sociaux. »

– Enfant vivant au Pakistan, 16 ans

« Le monde réel peut restreindre la façon dont les gens peuvent s'exprimer, mais le monde numérique ne devrait jamais restreindre l'expression. »

– Enfant vivant en Nouvelle-Zélande, 17 ans

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 2

01 Introduction 6

02 **Comment l'utiliser** 9

03 Pourquoi les droits de l'enfant sont-ils importants 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 Dix domaines d'action politique 37

06 Documents clés 169

07 Glossaire 174

08 Politique modèle 180

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Comment l'utiliser

La boîte à outils pour la protection en ligne des enfants fournit des outils pratiques visant à aider les responsables politiques du monde entier à remplir leurs obligations internationales en matière de droits des enfants et de protection en ligne des enfants.

Pour certains, ce document servira de point de départ, pour d'autres, il sera l'occasion de comparer leur politique et leur mise en œuvre actuelles par rapport aux meilleures pratiques internationales. Elle est conçue pour « ne pas être spécifique à un pays » afin que les responsables politiques, qui travaillent en s'appuyant sur une analyse de leur propre contexte national, puissent l'utiliser pour évaluer et éclairer leur propre cheminement vers l'intégration des droits de l'enfant à l'environnement numérique.

La boîte à outil contient :

- Une politique « modèle » complète et solide sur la protection en ligne des enfants, comme une approche que les responsables politiques peuvent mettre en œuvre ou sur laquelle ils peuvent s'appuyer pour assurer une coordination efficace entre les juridictions
- Dix domaines d'action politique à utiliser par les responsables politiques pour élaborer leur propre politique de protection en ligne pour les enfants
- Listes de contrôle et autres outils d'audit que les responsables politiques peuvent utiliser pour évaluer et améliorer les actions actuelles et prévues de leur pays pour la protection en ligne des enfants
- Résumés et lignes directrices pour les documents fondamentaux mondiaux
- Un glossaire des termes clés utilisés dans la politique de protection en ligne et la politique de protection en ligne des enfants
- Panneaux d'orientation vers des exemples de meilleures pratiques et des informations provenant de différents pays
- Diagrammes et autres documents explicatifs pour aider à communiquer des idées politiques à d'autres publics, y compris les fonctionnaires et la société civile.

Elle répond à l'appel à l'action lancé par le Secrétaire général de l'ONU dans sa Feuille de route pour la coopération numérique (2020) en rassemblant les ressources fondamentales : l'Observation générale n° 25 de la Convention des Nations Unies relative aux droits de l'enfant (2021) ; les directives de l'Union internationale des télécommunications sur la protection en ligne des enfants ; le modèle de réponse nationale de WeProtect Global Alliance, afin de fournir une ressource pratique aux responsables politiques désireux d'assurer la protection en ligne des enfants.

La boîte à outils et ses ressources sont disponibles en ligne sur childonlinesafetytoolkit.org et en nous contactant à l'adresse suivante : info@5rightsfoundation.com.

Les paroles sont importantes. Les mots que nous utilisons affectent la façon dont nous pensons les droits de l'enfant et la protection en ligne des enfants. Les mots que nous utilisons affectent la façon dont nous hiérarchisons les questions, la façon dont nous réagissons et, surtout, notre capacité à collaborer efficacement et à faire respecter ou à honorer les droits des enfants par-delà les frontières. Bien que les contextes nationaux soient nécessairement différents, il est essentiel que les lois et règlements utilisent, autant que possible, des concepts, des termes et des définitions qui soient alignés et permettent une coopération entre les organismes d'application de la loi, ainsi qu'une plus large coopération et compréhension transfrontalières.[2] La boîte à outils comprend des glossaires internationalement reconnus du Comité des droits de l'enfant de l'ONU et des Luxembourg Guidelines (lignes directrices de Luxembourg), qui contribuent à fournir un modèle pour la langue utilisée.[3]

La boîte à outils complète et met en évidence des modèles déjà bien développés pour soutenir des aspects spécifiques de la protection en ligne des enfants.

On trouve parmi les ressources fondamentales :

- L'observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, qui est un outil essentiel pour comprendre les droits de l'enfant dans le contexte de la protection en ligne des enfants. Dans ce document, le Comité des droits de l'enfant des Nations Unies explique comment les États doivent mettre en œuvre la Convention relative aux droits de l'enfant en ce qui concerne l'environnement numérique et fournit des orientations sur les mesures législatives, politiques et autres, pertinentes pour assurer le plein respect de leurs obligations en vertu de la Convention et des Protocoles facultatifs.[4]

- Le modèle de réponse nationale (MNR, de l'anglais *Model National Response*) de WeProtect Global Alliance est particulièrement important en ce qui concerne l'exploitation et les abus sexuels sur mineur. Le MRN est un élément clé de toute boîte à outils nationale pour la protection en ligne des enfants.[5] Le MRN cherche à aider les pays à renforcer leur réponse à l'exploitation en ligne des enfants et aux abus sexuels sur ces derniers, mais il indique que ce problème ne peut pas être traité de manière isolée : un ensemble plus large de capacités pour prévenir et combattre l'exploitation sexuelle des enfants et la violence exercée sur eux doit être mis en place pour assurer une réponse nationale complète. Cette boîte à outils fournit des ressources qui soutiennent la mise en œuvre du MNR. La Boîte à outils pour la protection en ligne des enfants peut aider les signataires du MNR de WeProtect Global Alliance à s'assurer qu'ils disposent de la capacité institutionnelle nécessaire pour atteindre les objectifs fixés, et que les obligations prévues par l'Observation générale n° 25 (2021) sont respectées.

- Les *lignes directrices de l'Union internationale des télécommunications (UIT) sur la protection en ligne des enfants* 2020 constituent un ensemble complet de recommandations et d'outils à l'attention de toutes les parties prenantes concernées qui souhaitent comprendre comment contribuer au développement d'un environnement en ligne sûr et responsabilisant pour les enfants et les jeunes. Elles sont adaptées à quatre publics clés : les enfants, les parents/aidants et éducateurs, le secteur industriel

2. « Le Comité recommande aux États parties, lorsqu'ils établissent leurs cadres juridiques, de tenir compte des progrès technologiques afin de veiller à ce que leur applicabilité ne soit pas compromise par l'évolution de la situation et afin d'éviter les failles liées aux nouvelles préoccupations, notamment les nouvelles formes de vente en ligne et d'exploitation sexuelle. Compte tenu de la nature évolutive de la question, les États parties devraient évaluer régulièrement et, le cas échéant, réviser leur législation et leurs politiques afin de garantir que leurs cadres juridiques et politiques restent adaptés à l'évolution rapide des réalités. » Directives concernant la mise en œuvre du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, Comité des droits de l'enfant, 2019.
3. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016.
4. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect Global Alliance, 2016.
5. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE 2021.

et les responsables politiques. Pour chacun de ces publics, les lignes directrices sont destinées à agir comme un plan détaillé qui peut être adapté et utilisé d'une manière qui est compatible avec les coutumes et les lois nationales ou locales et aborde les questions qui pourraient affecter tous les enfants et les jeunes de moins de 18 ans.[6]

D'autres ressources et cadres importants sont pertinents pour les responsables politiques qui s'intéressent à la protection en ligne des enfants, notamment :

- **Les objectifs de *développement durable des Nations Unies*.** Les 17 objectifs de développement durable (ODD) des Nations unies sont au cœur du programme de développement durable à l'horizon 2030, dont les [7] adoptés par tous les États membres des Nations unies en 2015.
- **Les principes directeurs des Nations Unies *relatifs aux entreprises et aux droits de l'homme.*** Ces principes énoncent l'obligation qu'ont les États parties et les entreprises de protéger et de respecter les droits de l'homme, y compris les droits de l'enfant.
- **INSPIRE de l'Organisation mondiale de la santé *: sept stratégies pour mettre fin à la violence à l'encontre des enfants.***[9] INSPIRE un ensemble de mesures techniques fondées sur des données probantes visant à épauler les pays dans leurs efforts pour prévenir et combattre la violence à l'encontre des enfants.
- **Projet de directives de l'UNICEF *sur l'IA pour les enfants.***[10] La Directive est conçue pour promouvoir les droits de l'enfant dans les politiques et pratiques d'IA des gouvernements et du secteur privé, et sensibiliser à la manière dont les systèmes d'IA peuvent respecter ou compromettre ces droits.

Il en existe beaucoup d'autres aux niveaux régional, national et international, qui peuvent être pertinentes pour des contextes nationaux spécifiques ou fournir des modèles pertinents au niveau mondial, dont beaucoup sont citées dans les sections pertinentes de cette boîte à outils.

La prévalence de l'exploitation et des abus sexuels d'enfants constitue également une préoccupation majeure. En 2020, 65 millions de pièces de contenu pédopornographique ont été signalées au National Center for Missing and Exploited Children des États-Unis, et bien d'autres sont passées inaperçues.[11] La communauté internationale est depuis longtemps unie dans sa détermination commune à protéger les enfants. Sur la base de cette volonté, la coopération entre les organismes nationaux d'application de la loi et les grandes entreprises technologiques s'est intensifiée, mais il reste encore beaucoup à faire.

Les entreprises doivent adopter des pratiques de numérisation plus solides et accélérer les méthodes de détection axées sur la prévention. Cette approche doit également être étayée par des mesures législatives importantes. À cet égard, les partenariats multipartites, tels que We Protect Global Alliance et le Partenariat mondial End Violence, sont très utiles.

Source : Feuille de route du Secrétaire général des Nations Unies pour la coopération numérique, juin 2020[12]

6. Guidelines on Child Online Protection (Lignes directrices sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.
7. Transforming our world: the 2030 Agenda for Sustainable Development (Transformer notre monde : l'Agenda 2030 pour le développement durable), Nations Unies, 2021.
8. Principes directeurs relatifs aux entreprises et aux droits de l'homme, Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2011.
9. INSPIRE: Seven Strategies for Ending Violence Against Children (INSPIRE : sept stratégies pour mettre fin à la violence contre les enfants), Organisation mondiale de la santé, 2021.
10. Directives politiques sur l'IA pour les enfants, Fonds des Nations Unies pour l'enfance, 2020.
11. Rapport CyberTipline, National Center for Missing and Exploited Children (Centre national des enfants disparus et exploités), 2020.
12. Feuille de route du Secrétaire général des Nations Unies pour la coopération numérique, Nations Unies, 2020.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Comment nous y sommes parvenus

Le monde numérique change sans cesse. La politique de protection en ligne des enfants doit être ancrée dans une approche fondée sur les droits de l'enfant et doit être suffisamment souple pour répondre à l'évolution des risques et des opportunités au fur et à mesure qu'ils se présentent. La boîte à outils pour la protection en ligne des enfants vise à répondre à ce besoin en fournissant un ensemble complet d'actions pour une politique adoptable, des exemples de meilleures pratiques et des ressources qui peuvent être partagées.

La boîte à outils est le fruit de consultations menées à travers le monde, en tenant compte des idées de tous les continents, et de lieux variés, des petits États insulaires en développement jusqu'aux grands pays industrialisés.[13] Nous avons consulté des experts internationaux de divers horizons, y compris de l'industrie, des responsables politiques et des universitaires. La rédaction a été entreprise par 5Rights, dont le siège est au Royaume-Uni, et a été soutenue par des collègues en Europe, en Amérique du Nord et en Australie et par des partenaires[14] qui ont animé des groupes de discussion en Amérique latine, en Afrique et en Asie, pour s'assurer que la boîte à outils est à la fois pratique et pertinente dans une variété de contextes locaux. Le texte est ancré dans des normes mondiales, en particulier la Convention des Nations Unies relative aux droits de l'enfant, mais la boîte à outils peut également être adaptée pour refléter les cultures et les valeurs que l'on trouve dans les constitutions nationales du monde entier.

Il s'agit d'une boîte à outils holistique, pratique et accessible pour les responsables politiques, contribuant à ouvrir la voie d'un monde où tous les enfants se sentent en sécurité et épanouis : un monde qui respecte pleinement leurs droits en ligne et hors ligne.

Au cours des consultations, les enfants ont indiqué que d'après eux, l'environnement numérique devrait soutenir, promouvoir et protéger leur engagement sûr et équitable :

« Nous aimerions que le gouvernement, les entreprises technologiques et les enseignants nous aident à savoir quoi faire des informations non fiables que l'on trouve en ligne. »
- Enfant vivant au Ghana, âge inconnu

« J'aimerais obtenir des éclaircissements sur ce qui se passe réellement avec mes données ... Pourquoi les recueillir ? Comment sont-elles recueillies ? »
- Enfant vivant en Allemagne, 16 ans

« Je crains que mes données ne soient partagées. »
- Enfant vivant au Canada, 15 ans

13. Incluant des consultations de groupes de discussion au Brésil, au Cambodge, en Colombie, au Ghana, au Sri Lanka et au Zimbabwe, afin de s'assurer de la pertinence de ce travail à l'échelle mondiale.
14. Les partenaires locaux comprenaient RedPapaz en Colombie, Alana Foundation au Brésil, African Digital Rights Hub au Ghana, UNICEF Zimbabwe, UNICEF Cambodge et Save the Children International au Sri Lanka.

« Les enfants ont besoin de confidentialité pour pouvoir utiliser la technologie en toute tranquillité. »

– Enfant vivant aux Philippines, 16 ans

« Même si vos paramètres de confidentialité et de sécurité sont activés, les entreprises/personnes disposent de techniques avancées pour obtenir les informations qu'elles veulent connaître. Elles en savent probablement plus que nous et ont accès à plus d'informations en ligne que ce que l'on imagine. »

– Enfant vivant au Canada, 13 ans

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 3

01 Introduction 6

02 Comment l'utiliser 9

03 **Pourquoi les droits de l'enfant sont-ils importants** 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 Dix domaines d'action politique 37

06 Documents clés 169

07 Glossaire 174

08 Politique modèle 180

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Pourquoi les droits de l'enfant sont importants

Les droits de l'enfant constituent le fil conducteur de toutes les politiques qui affectent la vie des enfants, tant en ligne qu'hors ligne. L'objectif d'une politique de protection en ligne des enfants est, fondamentalement, de faire en sorte que les droits des enfants à la protection et à la participation soient réels et effectifs lorsqu'ils s'engagent dans le monde numérique.

Les enfants et leurs familles ont des droits fondamentaux en vertu de la Charte internationale des droits, notamment la Déclaration universelle des droits de l'homme de 1948, le Pacte international relatif aux droits civils et politiques de 1966 et le Pacte international relatif aux droits économiques, sociaux et culturels de 1966, ainsi que des structures régionales et nationales de défense des droits de l'homme.

En ce qui concerne les enfants, la *Convention des Nations Unies relative aux droits de l'enfant de 1989* (« la Convention » ou CDE)[15] et ses *protocoles facultatifs relatifs à la vente d'enfants*[16] et *aux enfants dans les conflits armés*[17] fournissent un cadre pratique pour comprendre comment les droits de l'homme s'appliquent aux enfants. La Convention est le traité sur les droits de l'homme le plus largement ratifié de l'histoire et son protocole additionnel relatif à une procédure de communication contribue à la rendre exécutoire afin que les droits des enfants soient réels et effectifs.

Tous les droits contenus dans la CDE sont utiles pour assurer la protection en ligne des enfants, et il est essentiel de consulter les enfants pour comprendre ce que ces droits signifient dans la pratique. Par exemple, les droits des enfants au jeu, à la participation et à la vie de famille dans l'espace en ligne doivent être pris en compte. Toutes les personnes impliquées dans la réalisation des consultations doivent être correctement formées aux droits de l'enfant et aux implications pratiques de la voix et de l'inclusion des enfants.

Le Comité des droits de l'enfant des Nations Unies[18] fournit des orientations, dans l'Observation générale n° 25 (2021), sur les mesures législatives, politiques et autres mesures appropriées pour assurer le plein respect des obligations découlant de la Convention et de ses Protocoles facultatifs à la lumière des opportunités, des risques et des défis en lien avec les droits de l'enfant dans l'environnement numérique. L'Observation générale n° 25 (2021) sera un outil clé à prendre en considération lors de l'élaboration d'une politique de protection en ligne des enfants.

> **Les droits de chaque enfant doivent être respectés, protégés et reconnus dans l'environnement numérique. Les innovations dans le domaine des technologies numériques ont un impact sur la vie des enfants et sur leurs droits, d'une manière large et interdépendante, même lorsque les enfants n'ont pas eux-mêmes accès à Internet. Un accès éclairé aux technologies numériques peut aider les enfants à réaliser l'ensemble de leurs droits civils, politiques, culturels, économiques et sociaux. Toutefois, si l'on ne parvient pas à l'inclusion numérique, les inégalités existantes risquent de s'accroître et de nouvelles inégalités pourraient survenir.**
>
> Source : Observation générale n° 25 (2021), par. 4[19]

15. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
16. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
17. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
18. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, Comité des droits de l'enfant des Nations Unies, 2021.
19. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, Comité des droits de l'enfant des Nations Unies, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

La CDE énonce quatre principes directeurs pour la protection des droits de l'enfant, et l'Observation générale n° 25 (2021) décrit comment ces principes s'appliquent dans le monde numérique :

1. Le droit à la non-discrimination (article 2) :

L'article 2 de la Convention relative aux droits de l'enfant[20] dispose que tout enfant a le droit de jouir de ses droits dans des conditions d'égalité, « sans discrimination aucune, sans distinction de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale, ethnique ou sociale, de propriété, de handicap, de naissance ou de tout autre statut de l'enfant, de ses parents ou tuteurs légaux ». Les paragraphes 10 et 11 de l'Observation générale n° 25 (2021) décrivent comment cette disposition s'applique dans le monde numérique.

Les enfants peuvent être victimes de discrimination en étant exclus de l'utilisation des technologies et services numériques ou en faisant l'objet de communications haineuses ou d'un traitement injuste via l'utilisation de ces technologies. D'autres formes de discrimination peuvent survenir lorsque les processus automatisés qui aboutissent au filtrage, au profilage ou à la prise de décision sont fondés sur des données biaisées, partiales ou obtenues injustement concernant un enfant.

Le Comité demande aux États parties de prendre des mesures proactives pour prévenir la discrimination fondée sur le sexe, le handicap, l'origine socioéconomique, l'origine ethnique ou nationale, la langue ou tout autre motif, ainsi que la discrimination à l'égard des enfants appartenant à des minorités et des enfants autochtones, des enfants demandeurs d'asile, réfugiés et migrants, des enfants lesbiennes, homosexuels, bisexuels, transgenres et intersexués, des enfants victimes et survivants de la traite ou de l'exploitation sexuelle, des enfants bénéficiant d'une protection de remplacement, des enfants privés de liberté et des enfants se trouvant dans d'autres situations de vulnérabilité. Il conviendra de mettre en place des mesures spécifiques pour combler la fracture numérique liée au genre, pour les filles, et de veiller à ce qu'une attention particulière soit accordée à l'accès, à l'habileté numérique, à la confidentialité et à la protection en ligne.

Source : Observation générale n° 25 (2021), par. 10-11[21]

20. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, Nations Unies, 1989.
21. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2. L'intérêt supérieur de l'enfant (art. 3, par. 1) :

L'article 3 de la Convention relative aux droits de l'enfant[22] dispose que « dans toutes les actions concernant les enfants, qu'elles soient entreprises par des institutions publiques ou privées de protection sociale, par des tribunaux, par des autorités administratives ou par des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale ». Les paragraphes 12 et 13 de l'Observation générale n° 25 (2021) décrivent comment cette disposition s'applique dans le monde numérique.

L'intérêt supérieur de l'enfant est un concept dynamique qui nécessite une évaluation adaptée au contexte spécifique. L'environnement numérique n'a pas été conçu, à l'origine, pour les enfants, mais il joue toutefois un rôle important dans leur vie. Les États parties doivent veiller à ce que, dans toutes les mesures relatives à la fourniture, la réglementation, la conception, la gestion et l'utilisation de l'environnement numérique, l'intérêt supérieur de chaque enfant soit une considération primordiale.

Les États parties doivent associer à ces actions les organes nationaux et locaux qui veillent à la réalisation des droits de l'enfant. En prenant en considération l'intérêt supérieur de l'enfant, ils doivent tenir compte de tous les droits de l'enfant, y compris le droit de rechercher, de recevoir et de communiquer des informations, d'être protégé contre tout préjudice et de voir ses opinions dûment prises en considération, et veiller à la transparence dans l'évaluation de l'intérêt supérieur de l'enfant et des critères qui ont été appliqués.

Source : Observation générale n° 25 (2021), par. 12-13[23]

3. Droit à la vie, à la survie et au développement (article 6) :

L'article 6 de la Convention relative aux droits de l'enfant[24] dispose que les États parties « reconnaissent que tout enfant a un droit inhérent à la vie » et qu'ils doivent « assurer dans toute la mesure possible la survie et le développement de l'enfant ». Le paragraphe 15 de l'Observation générale n° 25 (2021) décrit comment cette disposition s'applique dans le monde numérique.

L'utilisation d'appareils numériques ne doit pas être nocive, ni se substituer aux interactions en personne entre les enfants ou entre les enfants et les parents ou aidants. Les États parties doivent accorder une attention particulière aux effets de la technologie au cours des premières années de la vie, lorsque la plasticité cérébrale est maximale et que l'environnement social, en particulier les relations avec les parents et les aidants, est crucial pour façonner le développement cognitif, émotionnel et social des enfants. Au cours des premières années de vie, des précautions peuvent être nécessaires, en fonction de la conception, de l'objectif et des utilisations des technologies. Une formation et des conseils sur l'utilisation appropriée des appareils numériques doivent être dispensés aux parents, aux aidants, aux éducateurs et aux autres acteurs concernés, en tenant compte de la recherche sur les effets des technologies numériques sur le développement des enfants, en particulier pendant les poussées de croissance neurologique critiques de la petite enfance et de l'adolescence.

Source : Observation générale n° 25 (2021), par. 15[25]

22. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, Nations Unies, 1989.
23. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
24. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, Nations Unies, 1989.
25. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4. Le droit d'être entendu (art. 12) :

Aux termes de l'article 12 de la Convention relative aux droits de l'enfant[26], les États parties doivent veiller à ce que, lorsque les enfants sont « capables de former leur propre opinion », ils jouissent « du droit d'exprimer librement leur opinion sur toutes les questions qui les concernent » et veiller à ce que cette opinion soit « dûment prise en considération en fonction de l'âge et du degré de maturité de l'enfant ». Le paragraphe 17 de l'Observation générale n° 25 (2021) décrit comment cette disposition s'applique dans le monde numérique, et de plus amples informations sur la manière de mettre en œuvre ce droit sont disponibles dans les Ressources 1 ci-dessous.

> **Lors de l'élaboration de la législation, des politiques, des programmes, des services et de la formation sur les droits de l'enfant en relation avec l'environnement numérique, les États parties doivent travailler avec tous les enfants, écouter leurs besoins et tenir dûment compte de leurs opinions. Ils doivent veiller à ce que les fournisseurs de services numériques s'engagent activement auprès des enfants, en appliquant des garanties appropriées, et tiennent dûment compte de leurs points de vue lors de la mise au point de produits et de services.**
>
> Source : Observation générale n° 25 (2021), par. 17[27]

Ces principes sont indivisibles et doivent tous être pris en compte lors de l'élaboration d'une politique de protection en ligne des enfants. Ils fournissent une perspective utile pour examiner ce que les cinq autres thèmes transversaux signifient dans la pratique et comment les dix domaines d'action politique décrits dans la boîte à outils devraient être mis en œuvre.

Les droits de l'enfant ne se retrouvent pas seulement dans le droit international. La plupart des constitutions ou cadres juridiques nationaux contiennent des dispositions générales relatives aux droits de l'homme qui protègent les enfants. Ces lois nationales sur les droits de l'homme devraient également être utilisées pour l'élaboration d'une politique de protection en ligne des enfants qui fait figurer en son cœur la protection et la promotion des droits de l'enfant.

Le Comité des droits de l'enfant des Nations unies appelle les États à veiller à ce que les politiques nationales relatives aux droits de l'enfant abordent spécifiquement l'environnement numérique et à ce que la protection en ligne des enfants soit intégrée aux politiques nationales de protection de l'enfance. Cette boîte à outils est conçue pour les aider à le faire.

26. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, Nations Unies, 1989.
27. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

Les États parties doivent veiller à ce que les politiques nationales relatives aux droits de l'enfant traitent spécifiquement de l'environnement numérique, et doivent mettre en œuvre des règlements, des codes industriels, des normes de conception et des plans d'action en conséquence, qui doivent tous être régulièrement évalués et mis à jour. Ces politiques nationales doivent avoir pour but de donner aux enfants la possibilité de tirer parti de l'environnement numérique et de leur garantir un accès sûr à cet environnement.

La protection en ligne des enfants doit être intégrée aux politiques nationales de protection de l'enfance. Les États parties doivent mettre en œuvre des mesures visant à protéger les enfants contre les risques, y compris ceux de cyberagression et d'exploitation et abus sexuels en ligne et facilités par la technologie numérique, veiller à ce que ces crimes fassent l'objet d'enquêtes et offrir réparation et soutien aux enfants qui en sont victimes. Ils doivent également répondre aux besoins des enfants défavorisés ou vulnérables, notamment en leur fournissant des informations adaptées qui soient, le cas échéant, traduites dans les langues minoritaires pertinentes.

Les États parties doivent veiller à la mise en place de mécanismes efficaces de protection de l'enfance en ligne et de politiques de protection de l'enfance, tout en respectant les autres droits de l'enfant, dans tous les contextes où les enfants accèdent à l'environnement numérique, y compris à la maison, dans les établissements d'enseignement, dans les cybercafés, dans les centres de jeunesse, dans les bibliothèques et dans les structures de soins de santé et de protection de remplacement.

Source : Observation générale n° 25 (2021), par. 24-26 [28]

Ressources pour les droits de l'enfant :

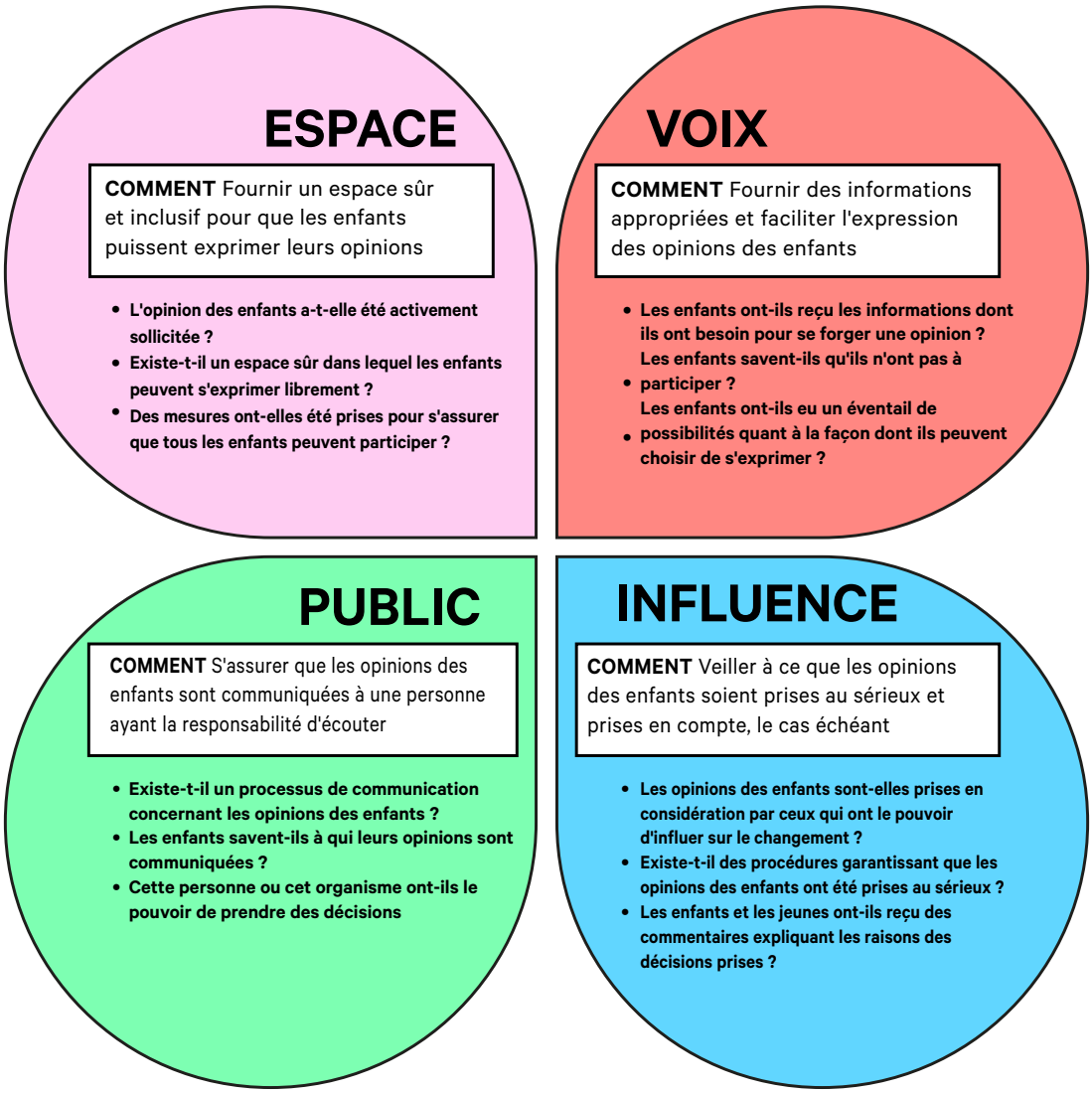
1. Mise en œuvre du droit d'être entendu dans l'élaboration de votre politique de protection en ligne des enfants :

Le droit d'être entendu doit être au cœur de l'élaboration des politiques pratiques de protection en ligne des enfants. Les enfants et les jeunes expriment des opinions marquées sur l'environnement numérique[29], et ils ont le droit d'être entendus sur les questions qui les concernent.[30] Pour que la politique de protection en ligne réponde aux besoins des enfants, les responsables politiques doivent entendre la voix des enfants et inclure leurs points de vue à l'élaboration des politiques. Les points de vue des enfants sur les risques et les préjudices, les avantages et les opportunités dans l'environnement en ligne peuvent être différents de ceux des adultes qui les entourent. Une consultation efficace avec participation des enfants[31] tout au long de l'élaboration, de la mise en œuvre, du suivi et de l'évaluation des politiques de protection en ligne des enfants est donc essentielle pour garantir que leurs besoins sont correctement satisfaits et que la politique est réellement adaptée aux enfants.[32]

28. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021
29. In Our Own Words – Children's Rights in the Digital World (Dans nos propres mots : les droits de l'enfant dans le monde numérique), 5Rights Foundation, 2021.
30. Le droit d'être entendu est contenu dans l'article 13 de la Convention.
31. Celui-ci devra prendre en compte les quatre éléments du modèle Lundy : l'espace, la voix, le public, l'influence. Voir : The Lundy model of child participation (Le modèle Lundy de participation des enfants).
32. The Digital Futures Commission (Commission sur l'avenir du numérique).

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

Le modèle de Lundy présente une méthode visant à comprendre « comment » permettre la participation des enfants, via quatre domaines d'intérêt :



Source : Le modèle Lundy de participation des enfants[33]

L'importance d'intégrer les voix et les expériences des enfants à l'élaboration d'une politique de protection en ligne des enfants est réitérée par les lignes directrices de l'Union internationale des télécommunications sur la protection en ligne des enfants. Le fait de veiller à ce que la voix des enfants soit prise en compte dans toute considération de protection en ligne des enfants permet de créer une politique plus robuste, plus diversifiée et plus inclusive.

> **Les enfants et les jeunes veulent participer à la conversation et ont une expertise précieuse à partager en tant que « natifs du numérique ». Les responsables politiques et les praticiens doivent s'engager avec les enfants et les jeunes dans un débat permanent sur l'environnement en ligne, pour défendre leurs droits.**
>
> Source : ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[34]

33. The Lundy model of child participation (Le modèle Lundy de participation des enfants), Commission européenne, 2007.
34. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

2. Aider les gens à comprendre la Convention relative aux droits de l'enfant :

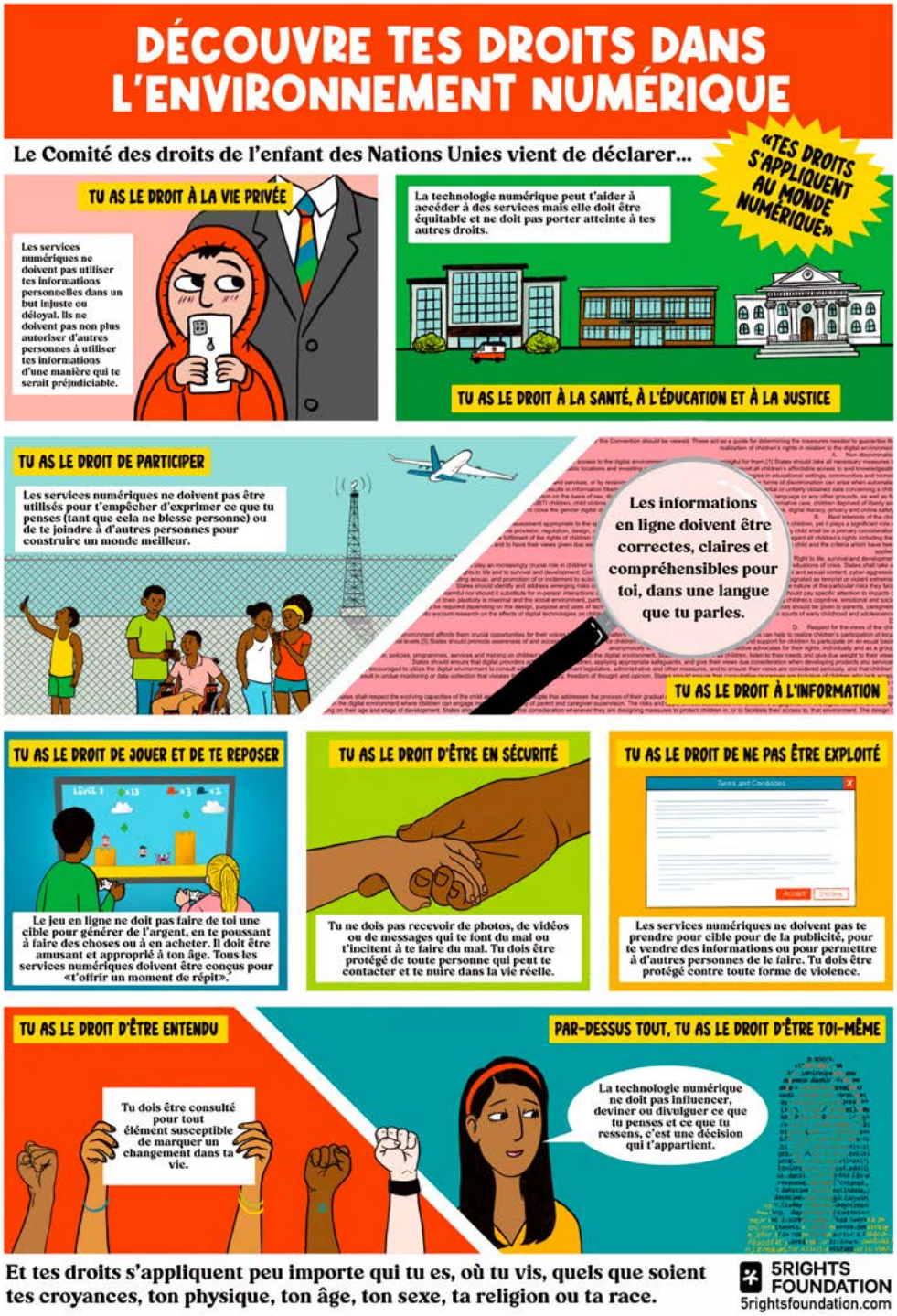
The United Nations Convention on the Rights of the Child: The Children's Version (la Convention des Nations Unies relative aux droits de l'enfant - La version pour les enfants)[35]

35. The United Nations Convention on the Rights of the Child: The Children's Version (la Convention des Nations Unies relative aux droits de l'enfant : la version pour les enfants), Save the Children, 2019.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

3. Aider les enfants à comprendre l'observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique :

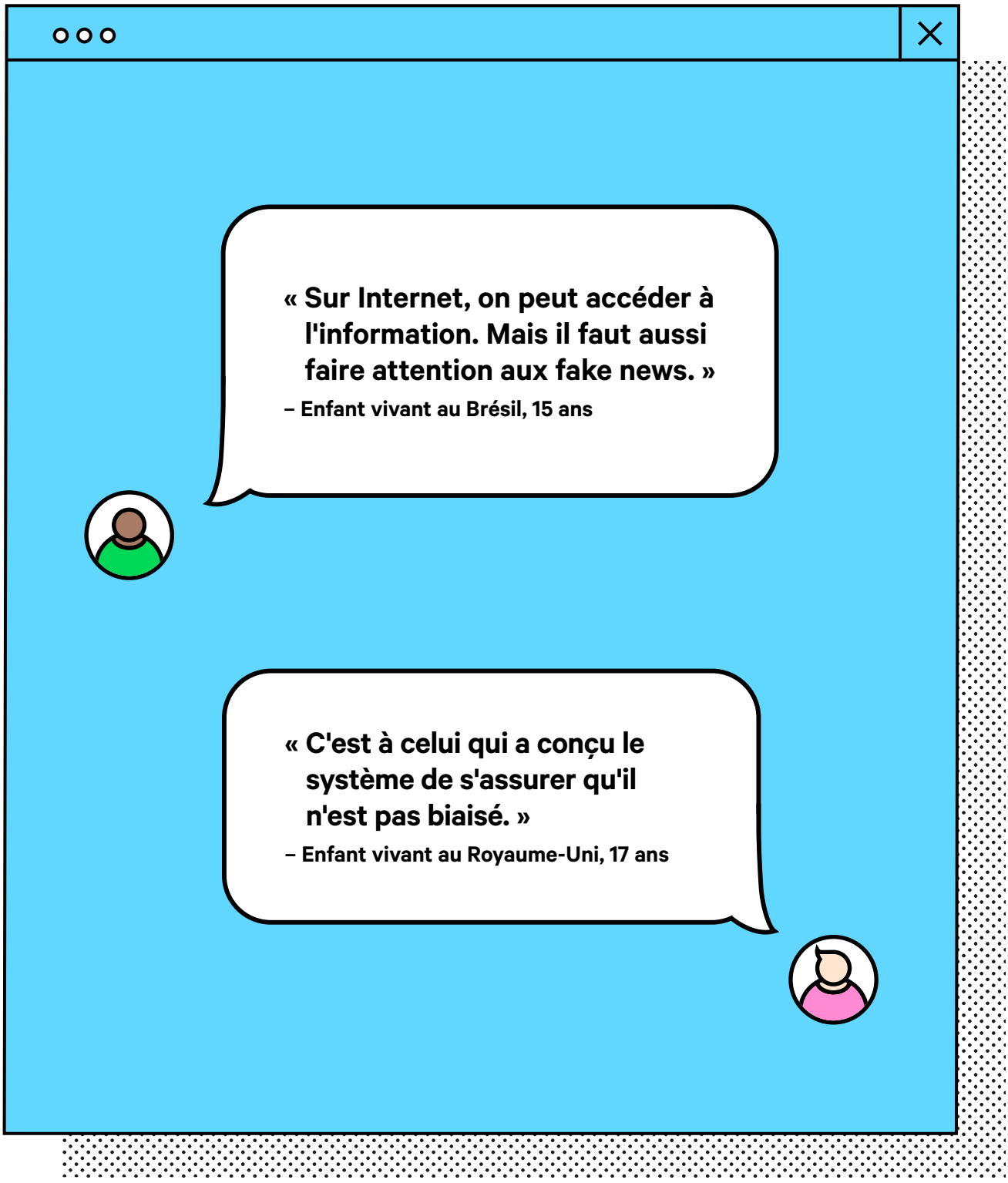


Source : Know Your Rights! Affiche Observation générale n° 25 (2021)[36]

36. Know Your Rights! Affiches Observation générale n° 25 (2021), 5Rights Foundation, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >



« Sur Internet, on peut accéder à l'information. Mais il faut aussi faire attention aux fake news. »

– Enfant vivant au Brésil, 15 ans

« C'est à celui qui a conçu le système de s'assurer qu'il n'est pas biaisé. »

– Enfant vivant au Royaume-Uni, 17 ans

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 4

01 Introduction 6

02 Comment l'utiliser 9

03 Pourquoi les droits de l'enfant sont-ils importants 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 Dix domaines d'action politique 37

06 Documents clés 169

07 Glossaire 174

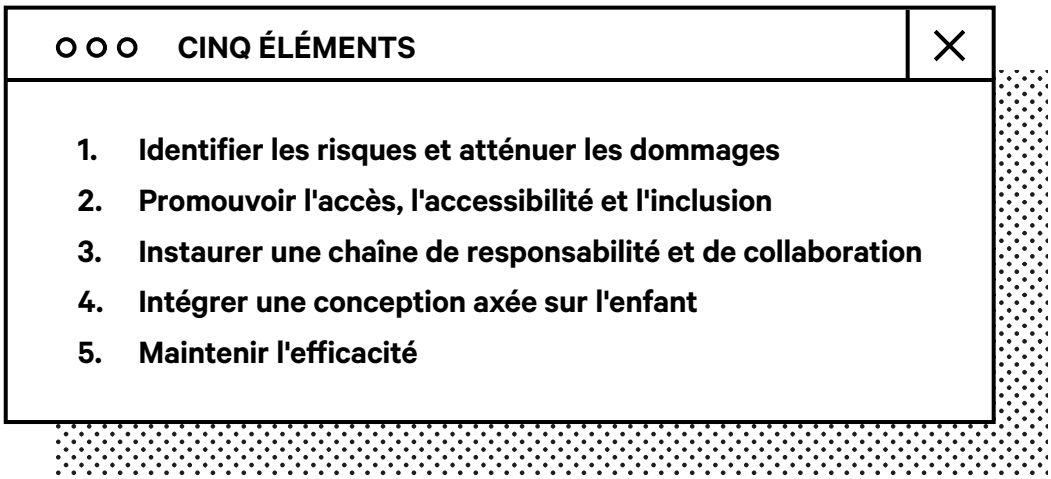
08 Politique modèle 180

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Les éléments que chaque responsable politique doit prendre en considération

Cette section explore cinq thèmes transversaux auxquels les responsables politiques doivent réfléchir lorsqu'ils conçoivent, élaborent et mettent en œuvre des politiques de protection en ligne des enfants.



Chacun de ces points doit être pris en considération lors de la mise en œuvre des dix domaines d'action politique de la page n° 38.

1. Identifier les risques et atténuer les dommages :

> **Les possibilités offertes par l'environnement numérique jouent un rôle de plus en plus crucial dans le développement des enfants et peuvent être vitales pour leur vie et pour leur survie, en particulier dans les situations de crise. Les États parties doivent prendre toutes les mesures appropriées pour protéger les enfants contre les risques qui menacent leur droit à la vie, à la survie et au développement. Les risques liés au contenu, aux contacts, à la conduite et au contrat englobent, entre autres, les contenus violents et à caractère sexuel, la cyberagression et le harcèlement, les jeux de hasard, l'exploitation et les abus, y compris l'exploitation et les abus sexuels, et la promotion de conduites suicidaires ou l'incitation au suicide ou à des activités mettant la vie en danger, y compris par des criminels ou des groupes armés désignés comme terroristes ou extrémistes violents. Les États parties doivent recenser les risques émergents auxquels les enfants sont confrontés dans divers contextes et s'y attaquer, notamment en écoutant leurs points de vue sur la nature des risques particuliers auxquels ils sont exposés.**
>
> Source : Observation générale n° 25 (2021), par. 14[37]

Les stratégies de protection en ligne des enfants doivent être élaborées avant tout pour maximiser les avantages que les enfants peuvent tirer des technologies numériques. Cela implique nécessairement la responsabilité première d'atténuer les risques, de limiter au maximum la probabilité qu'un dommage se produise, de remédier aux dommages lorsqu'ils se sont produits et de prendre en compte l'impact que les produits et services peuvent avoir sur l'utilisateur final, si cet utilisateur est (ou est susceptible d'être) un enfant. Il est essentiel de concevoir des produits et des services qui anticipent la participation des enfants en toute sécurité.

37. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

Si certains enfants subissent un préjudice grave, des millions d'autres sont victimes d'un préjudice en ligne sous une forme ou une autre. Par exemple, il existe un large éventail de risques liés à la surveillance ou à l'exploitation commerciale, à l'exposition à de fausses informations ou à des arnaques, à des prédateurs ou à du harcèlement, tandis qu'un nombre moins important d'entre eux subissent le préjudice extrême d'un abus sexuel. De nombreux risques sont cumulatifs. Ils affectent les enfants de différentes manières et une forme de préjudice peut ouvrir la voie à d'autres formes de préjudice.[38]

La nature internationale du monde en ligne implique que les enfants sont confrontés aux mêmes risques en ligne, quelle que soit leur situation géographique. Mais des contextes différents peuvent également soulever des préoccupations spécifiques. Dans certains cas, un enfant peut être désavantagé par un manque d'accès à l'environnement en ligne ; dans d'autres cas, il peut y avoir un lien entre le préjudice subi en ligne et l'expérience hors ligne d'un enfant. Les risques et les préjudices spécifiques se chevauchent souvent les uns les autres. Il existe très peu de grandes lignes ou de divisions nettes.

Des facteurs tels que le sexe, l'âge, les circonstances familiales, le statut socio-économique, le lieu, les expériences et la disponibilité de la technologie numérique peuvent modifier les risques et les façons dont les enfants subissent des préjudices. Certains risques et préjudices affectent des communautés et des catégories d'enfants entières : par exemple, les filles sont plus exposées aux abus, tandis que les garçons ont tendance à être davantage maltraités.[39] Les normes culturelles entourant la masculinité aggravent également le problème de la sous-détection et du sous-signalement des abus sexuels sur les enfants de sexe masculin.[40] Les risques et les préjudices peuvent également être amplifiés par des plateformes conçues de manière à encourager le partage de contenus choquants et sensationnels, ou encore par le profilage ou la promotion de certains types de comportements d'utilisateurs parce qu'ils suscitent un engagement rentable.

Les responsables politiques doivent prendre en compte tous les risques auxquels sont exposés les enfants et prendre des mesures pour les atténuer. Un outil clé pour identifier les risques est le cadre des 4C.

La classification des 4C de CO:RE reconnaît que les risques en ligne apparaissent lorsqu'un enfant :

- Accède à ou est exposé à des **contenus** potentiellement dangereux
- Subit ou est visé par des **contacts** potentiellement dangereux
- Est témoin, participe ou est victime d'un **comportement** potentiellement dangereux
- Est partie à ou exploité par un **contrat potentiellement nuisible**.

CO:RE	CONTENU Enfant destinataire	CONTACT Enfant participant	CONDUITE Enfant acteur	CONTRAT Enfant consommateur
Contenu agressif	Contenu violent, gore, graphique, raciste, haineux et extrémiste	Harcèlement, traque, comportement haineux, surveillance indésirable	Intimidation, activités haineuses ou hostiles de la part de pairs, par exemple trolling, exclusion, shaming	Vol d'identité, fraude, hameçonnage, escroqueries, jeux de hasard, chantage, risques de sécurité
Contenu à caractère sexuel	Pornographie (légale et illégale), sexualisation de la culture, normes d'image corporelle	Harcèlement sexuel, sollicitation sexuelle, génération et partage de matériel concernant un abus sexuel sur mineur	Harcèlement sexuel, messages sexuels non consentis, pressions sexuelles	Sextorsion, traite à des fins d'exploitation sexuelle, exploitation sexuelle des enfants en streaming
Valeurs	Contenu généré par l'utilisateur ou contenu marketing non adapté à l'âge, information erronée/ désinformation	Persuasion idéologique, radicalisation et recrutement extrémiste	Communautés d'utilisateurs potentiellement nuisibles, par exemple automutilation, anti-vaccinations, pressions des pairs	Filtrage des informations, biais de profilage, polarisation, conception persuasive
Contenus transversaux	Violations de la confidentialité et de la protection des données, risques pour la santé physique et mentale, formes de discrimination			

Source : CO:RE Content, Contact, Conduct, Contract – Updating the 4Cs of online risk, 2021 [41]

38. Building the digital world that young people deserve (Construire le monde numérique que les jeunes méritent), 5Rights Foundation, 2020.
39. Safe Online Investment Portfolio Results 2020 (Résultats du portefeuille d'investissement en ligne sécurisé 2020), Global Partnership to End Violence against Children (Partenariat mondial pour mettre fin à la violence à l'encontre des enfants), 2020. p. 2.
40. Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse (Rompre avec le mal au Kenya : données sur l'exploitation et l'abus sexuels des enfants en ligne), Global Partnership to End Violence against Children (Partenariat mondial pour mettre fin à la violence à l'encontre des enfants), 2021. p. 68.
41. Content, Contact, Conduct, Contract - Updating the 4Cs of Online Risk, CO:RE 2021.

> **Avec l'expansion du haut débit abordable dans les pays en développement, il est urgent de mettre en place des mesures pour réduire les risques et les menaces à l'encontre de ces enfants, tout en leur permettant de tirer parti de tous les avantages du monde numérique.**
>
> Source : ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[41]

> **Les États parties doivent tenir compte de l'évolution de la situation des enfants et de leur représentation dans le monde moderne, de la compétence et de la compréhension des enfants, qui évoluent de manière inégale selon les domaines de compétence et d'activité, et de la diversité des risques encourus. Ces considérations doivent être mises en balance avec l'importance de l'exercice de leurs droits dans des environnements soutenus et la diversité des expériences et des circonstances individuelles. Les États parties doivent veiller à ce que les fournisseurs de services numériques offrent des services adaptés à l'évolution des capacités des enfants.**
>
> Source : Observation générale n° 25 (2021), par. 20[42]

2. Promouvoir l'accès, l'accessibilité et l'inclusion :

> **Les droits de chaque enfant doivent être respectés, protégés et reconnus dans l'environnement numérique. Les innovations dans le domaine des technologies numériques ont un impact sur la vie des enfants et sur leurs droits, d'une manière large et interdépendante, même lorsque les enfants n'ont pas eux-mêmes accès à Internet. Un accès éclairé aux technologies numériques peut aider les enfants à réaliser l'ensemble de leurs droits civils, politiques, culturels, économiques et sociaux. Toutefois, si l'on ne parvient pas à l'inclusion numérique, les inégalités existantes risquent de s'accroître et de nouvelles inégalités pourraient survenir.**
>
> Source : Observation générale n° 25 (2021), par. 4[44]

Aujourd'hui, l'accès au monde en ligne est crucial pour que les enfants puissent exercer leurs droits et réaliser pleinement leur potentiel. Une politique de protection en ligne pour les enfants doit être inclusive, à la fois dans ses objectifs et dans sa pratique.[45] Cela signifie qu'elle doit être assortie de ressources adéquates et qu'elle doit s'appuyer sur les meilleures pratiques et les cadres existants, en particulier dans les situations où les ressources sont limitées. Que la mise en œuvre d'une politique de protection des enfants en ligne implique d'adapter la législation existante (par exemple en matière de protection de l'enfance, de protection des consommateurs ou de réglementation des télécommunications) au contexte de la protection en ligne des enfants ou de créer de nouveaux corps de loi, elle doit promouvoir l'inclusion et l'égalité pour tous les enfants, quels qu'ils soient et où qu'ils soient.

42. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.
43. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
44. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
45. Par exemple : les enfants en situation de handicap ou les enfants issus de groupes minoritaires marginalisés, les enfants des rues, les enfants réfugiés et les enfants migrants, entre autres. Cette question est abordée dans les thèmes transversaux ci-dessous. Vous trouverez plus d'informations sur le modèle et la liste de contrôle dans « Voice » is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child (La « voix » ne suffit pas : conceptualiser l'article 12 de la Convention des Nations Unies relative aux droits de l'enfant), Laura Lundy, 2013.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

> **Les États parties doivent promouvoir les innovations technologiques qui répondent aux besoins des enfants souffrant de différents types de handicaps et veiller à ce que les produits et services numériques soient conçus pour être universellement accessibles afin qu'ils puissent être utilisés par tous les enfants sans exception et sans qu'il soit nécessaire de les adapter. Les enfants handicapés doivent être associés à la conception et à la mise en œuvre des politiques, produits et services qui ont un impact sur la réalisation de leurs droits dans l'environnement numérique.**
>
> Source : Observation générale n° 25 (2021), par. 91[46]

Les enfants ne constituent pas un groupe homogène. Les politiques de protection en ligne des enfants doivent être accessibles et inclusives pour atteindre tous les enfants, quels qu'ils soient et où qu'ils soient. Une « fracture numérique » risque fort d'apparaître lorsque certains enfants ont facilement accès à l'espace en ligne, tandis que d'autres en sont effectivement exclus. Les cadres doivent être adaptés à l'âge des enfants et convenir à tous les enfants, quels que soient leur sexe, leur race, leur religion, leur nationalité, leur origine ethnique, leur handicap ou toute autre caractéristique. La langue doit être accessible et inclusive et, le cas échéant, les supports doivent être disponibles dans un éventail de langues différentes. Les supports relatifs à la protection en ligne des enfants doivent être élaborés en consultation avec les enfants et les personnes qui s'occupent d'eux : au minimum, ils doivent être adaptés à l'âge, neutres du point de vue du sexe et facilement accessibles aux enfants d'âges différents et à leurs parents/aux personnes qui s'en occupent. Lorsque l'alphabétisation est limitée, les supports visuels permettent souvent de faire passer les messages de manière beaucoup plus efficace. L'utilisation de termes cohérents entre les différentes plateformes contribue à rendre la protection en ligne des enfants plus facilement compréhensible et accessible pour les enfants, leurs familles et les personnes qui s'en occupent.[47]

Les responsables politiques doivent s'assurer qu'ils favorisent l'accès des enfants en ligne et qu'ils les incluent dans leur démarche pour rendre les environnements numériques sûrs.

> **Les adultes et les enfants sont exposés à une gamme de risques et de dangers en ligne. Les enfants constituent néanmoins une population beaucoup plus vulnérable. Certains enfants sont également plus vulnérables que d'autres groupes d'enfants, par exemple les enfants handicapés ou les enfants en déplacement. Les responsables politiques doivent garantir que tous les enfants puissent se développer et être éduqués dans un environnement numérique sûr. La Convention des Nations Unies relative aux droits de l'enfant souligne l'idée que les enfants sont vulnérables et doivent être protégés contre toutes les formes d'exploitation.**
>
> Source : ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[48]

3. Instaurer une chaîne de responsabilité :

> **Afin d'englober les conséquences transversales de l'environnement numérique en termes de droits de l'enfant, les États parties doivent désigner un organe gouvernemental chargé de coordonner les politiques, directives et programmes relatifs aux droits de l'enfant entre les administrations centrales et les différents niveaux de gouvernement. Ce mécanisme national de coordination doit collaborer avec les écoles et le secteur des technologies de l'information et de la communication, et coopérer avec les entreprises, la société civile, les universités et les organisations, dans la réalisation des droits de l'enfant en relation avec l'environnement numérique, aux niveaux intersectoriel, national, régional et local. Il doit s'appuyer sur les expertises technologiques et autres expertises pertinentes au sein du gouvernement et au-delà, selon les besoins, et être évalué de façon indépendante quant à son efficacité à satisfaire à ses obligations.**
>
> Source : Observation générale n° 25 (2021), par. 27[49]

46. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
47. Voir l'introduction sur l'importance du langage et des définitions ainsi que la section du glossaire.
48. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.
49. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

La responsabilité de la protection en ligne des enfants implique de nombreuses personnes, spécialités et organisations, notamment le gouvernement, les services de police, les entreprises, les éducateurs, l'aide psychosociale, les familles et les enfants. Certains maillons de la chaîne portent un plus grand poids de responsabilité.[50] Par exemple, un service qui est susceptible d'être consulté par des enfants ou d'avoir un impact sur eux doit examiner si l'une de ses caractéristiques présente un risque pour les enfants. Il doit le faire avant tout contact avec les enfants utilisateurs. On parle souvent de « conception sécuritaire » ou de « conception axée sur l'enfant ». La sécurité par défaut doit être la norme.

Chaîne de responsabilité des parties prenantes

Assumer la responsabilité de la protection en ligne des enfants, c'est à la fois prévenir le mal avant qu'il ne se produise et prendre des mesures lorsque les choses tournent mal. Les mécanismes de plainte et de signalement doivent être accessibles et clairement signalés afin que les enfants, les personnes qui s'en occupent et les professionnels qui en ont besoin puissent les trouver et les utiliser facilement. Dans le cadre des systèmes professionnels en ligne, il convient de mettre en place des mécanismes permettant de suivre et d'évaluer les rapports de plaintes afin d'identifier et de traiter rapidement les sujets de préoccupation.

Les lois et les règlements doivent établir des cadres clairs en matière de prévention, de responsabilité et de réparation lorsque les choses tournent mal. Cela inclut le recueil de données concernant les rapports et les plaintes, afin qu'ils soient suivis et analysés pour améliorer le système. Les enfants et les parents/les personnes qui s'en occupent ne doivent pas être rendus responsables de la prévention ou de la prise en charge de risques et de préjudices qu'ils ne comprennent ou ne contrôlent que très peu. Le consentement ne peut être utilisé pour décharger les organisations publiques ou privées de leurs responsabilités en matière de protection en ligne des enfants. L'intégration de la protection en ligne des enfants dans les cadres existants pour la sécurité des produits[51], la protection des enfants[52], les droits des enfants[53] et les droits des consommateurs[54] peut contribuer à éviter les lacunes en matière de responsabilité et la duplication des ressources, des rôles et des responsabilités. Il ne doit pas y avoir de failles juridiques qui compromettent la protection en ligne des enfants.

Il est crucial que la protection en ligne des enfants soit intégrée dans tous les domaines politiques connexes, des plans nationaux pour le large bande aux programmes d'enseignement, d'une manière transparente, responsable et applicable. La création de silos peut conduire à des conflits réglementaires et à une fragmentation de l'élaboration et de la mise en œuvre des politiques.

Les responsables politiques doivent assumer la complexité de la responsabilité de la protection en ligne des enfants et veiller à ce qu'il existe des mécanismes de coopération et de soutien à tous les acteurs de la chaîne, afin que ceux-ci puissent jouer leur rôle dans la protection des enfants. Il est également essentiel de bien comprendre les rôles et les responsabilités, et de bien connaître les principaux acteurs des domaines spécifiques.

> **La protection des enfants et des jeunes est une responsabilité partagée, et il incombe à toutes les parties prenantes concernées de garantir un avenir durable pour tous. Pour ce faire, les responsables politiques, l'industrie, les parents, les aidants, les éducateurs et les autres parties prenantes doivent veiller à ce que les enfants et les jeunes puissent réaliser leur potentiel, en ligne et hors ligne.**
>
> Source : ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[55]

50. Voir par exemple les Principes directeurs de l'ONU sur les entreprises et les droits de l'homme
51. Normes et risques pour produits spécifiques, Commission européenne, 2014.
52. Centre de protection de l'enfance, Commission européenne, 2021.
53. Stratégie pour les droits de l'enfant, Conseil de l'Europe, 2021.
54. Directive sur les droits des consommateurs, Commission européenne, 2014.
55. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

> **La bonne gouvernance rassemble ceux qui ont la responsabilité de protéger les enfants contre l'exploitation sexuelle en ligne, et prend la forme d'un ou plusieurs organismes nationaux multipartites et intersectoriels. Il n'existe pas un modèle unique que l'organisme multipartite doive adopter : il peut s'agir d'un modèle qui régisse la gouvernance et la supervision globales de la capacité d'un pays à prévenir et à répondre à l'exploitation et aux abus sexuels sur mineur en ligne, ou simplement agisse comme un organisme de coordination du travail entre le gouvernement, l'industrie et la société civile.**
>
> Source : WeProtect Global Alliance Model National Response 2016[56]

Ces responsabilités sont également reflétées dans d'autres engagements, notamment les objectifs de développement durable codifiés en tant qu'objectif 16.2, visant à « mettre fin à la maltraitance, à l'exploitation, à la traite et à toutes les formes de violence et de torture à l'encontre des enfants ».

* Comprend les opérateurs, les FAI, les fournisseurs de contenu, les médias sociaux et les plateformes de messagerie

Source : Commission sur le large bande – Child Online Safety : Minimizing the Risk of Violence, Abuse and Exploitation Online 2019[57]

56. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect Global Alliance, 2016.
57. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect Global Alliance, 2016. Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online, Commission sur le large bande, 2019.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4. Intégrer une conception axée sur l'enfant :

> **Les États parties doivent prendre des mesures de lutte contre les préjudices connus et envisager activement de faire des recherches et de recueillir des données probantes dans le secteur de la santé publique afin d'empêcher la diffusion d'informations fausses ou trompeuses et de contenus et services susceptibles de nuire à la santé mentale ou physique des enfants. Des mesures peuvent également être nécessaires pour prévenir une participation nocive aux jeux numériques ou aux réseaux sociaux, comme la réglementation contre les conceptions numériques qui compromettent le développement et les droits des enfants.**
>
> Source : Observation générale n° 25 (2021), par. 96[58]

La protection en ligne des enfants doit être intégrée dans la conception et le développement des technologies. La conception axée sur l'enfant intègre dès le départ la protection en ligne des enfants dans les services et les produits. Il s'agit notamment de veiller à ce que la protection en ligne des enfants soit prise en compte dans les exigences réglementaires en matière de conception et dans l'octroi de licences pour les nouvelles technologies[59]. La conception axée sur l'enfant est souvent appelée sécurité/droits/vie privée/éthique dès la conception.

L'application du principe de précaution[60] aux technologies susceptibles d'avoir un impact sur les enfants et les jeunes garantit que la protection des enfants en ligne est prise en compte dès le début. La Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST) de l'UNESCO a proposé une « définition de travail » du principe de précaution :

> **« Lorsque des activités humaines peuvent causer un préjudice moralement inacceptable qui est scientifiquement plausible mais incertain, des mesures devront être prises pour éviter ou atténuer ce préjudice.**
>
> Un préjudice moral inacceptable est un danger pour l'homme ou l'environnement qui est :
>
> - ☐ **Une menace pour la vie ou la santé humaine, ou**
> - ☐ **Sérieux et effectivement irréversible, ou**
> - ☐ **Inéquitable pour les générations actuelles ou futures, ou**
> - ☐ **Imposé sans tenir suffisamment compte des droits de l'homme des personnes affectées. »[61]**

Le principe de précaution doit orienter un cadre pour la sécurité et le respect de la vie privée dès la conception, afin de garantir que la protection en ligne des enfants et les droits des enfants soient intégrés dans la technologie dès la phase de conception. La conception axée sur l'enfant ne doit pas seulement être un concept éthique, mais une obligation légale.[62] Elle doit également être intégrée dans les critères de financement de la recherche et du développement qui peuvent affecter les droits en ligne des enfants.

La technologie et l'intelligence artificielle (IA) ont le potentiel d'améliorer la protection en ligne des enfants et de protéger leurs droits. Encourager le développement d'outils technologiques permettant de concrétiser les droits de l'enfant et d'améliorer la protection en ligne des enfants est un aspect important de la politique de protection en ligne des enfants. L'impact plus large de l'IA ou d'autres technologies conçues pour protéger les enfants doit être évalué à la lumière de tous les droits de l'enfant,[63] afin d'éviter de porter atteinte à d'autres

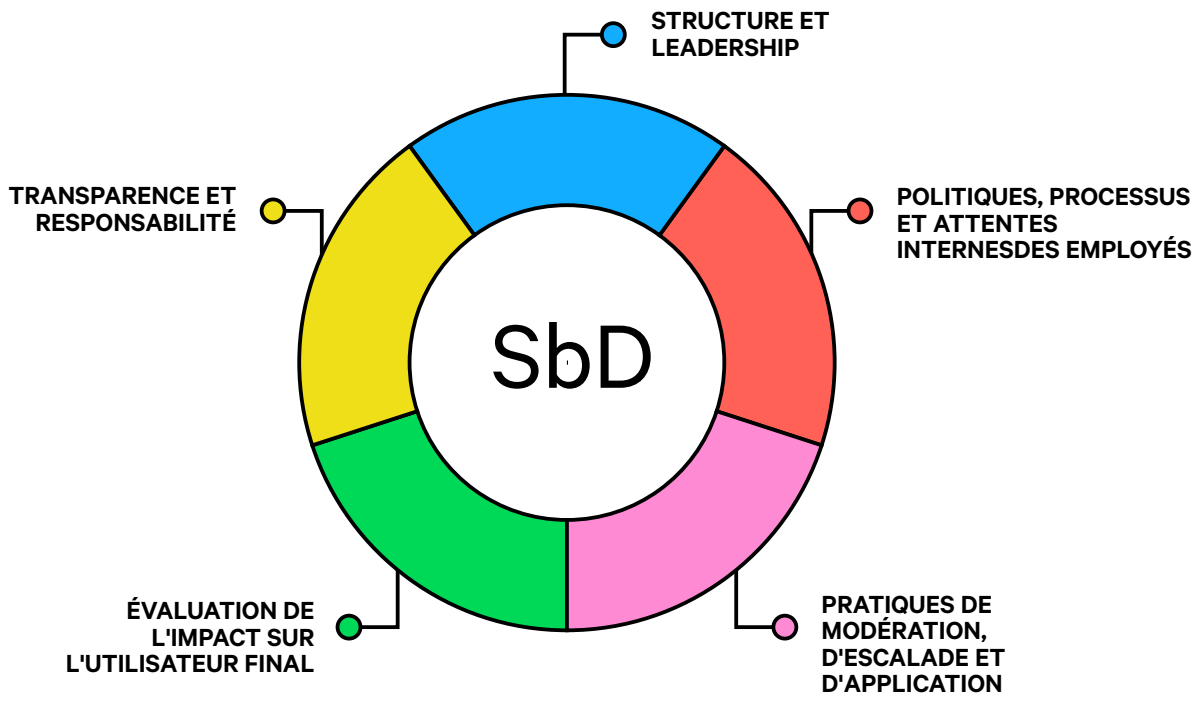
58. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
59. Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes fondamentaux visant à lutter contre l'exploitation et les abus sexuels sur mineur en ligne), GOV.UK, 2021.
60. Voir Communication de la Commission sur le principe de précaution EUR-Lex, 2000 ; Le principe de précaution : définitions, applications et gouvernance, Parlement européen, 2015.
61. The Precautionary Principle (Le principe de précaution), World Commission on the Ethics of Scientific Knowledge and Technology (Commission mondiale de l'éthique des connaissances scientifiques et des technologies), 2005.
62. Voir par exemple l'article 25, Règlement général sur la protection des données, Union européenne, 2018.
63. Voir par exemple Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

droits tels que la vie privée et la non-discrimination.

Les enfants eux-mêmes sont extrêmement différents et l'ensemble des caractéristiques, des origines et des contextes des enfants doivent être pris en compte dans l'élaboration, la mise en œuvre et le contrôle de l'efficacité des politiques dans ce domaine. Une action efficace en matière de protection des enfants en ligne doit tenir compte des tensions perçues. Par exemple, dans les débats sur le chiffrement, les défenseurs de la protection contre l'exploitation et les abus sexuels sur mineur (CSEA) peuvent voir leurs arguments se heurter à ceux liés à la vie privée et à la protection des données. Ces conflits doivent être résolus dans la mesure où une issue pratique est possible, afin d'éviter de nombreuses années de débats cycliques alors que des enfants sont mis en danger ou subissent des préjudices. Dans de tels cas, « l'intérêt supérieur » de l'enfant doit primer.[64]

Il existe plusieurs cadres et processus qui favorisent l'application de la conception axée sur l'enfant dans l'élaboration des politiques, notamment le principe de précaution, les évaluations de l'impact sur l'enfant[65] et la consultation avec l'enfant.[66] En outre, l'Association de normalisation de l'Institut des ingénieurs électriciens et électroniciens (IEEE-SA) a introduit une norme contenant des étapes pratiques que les entreprises peuvent suivre pour concevoir des produits et services numériques adaptés à l'âge des enfants, [67] et la Commission sur l'avenir numérique a indiqué comment le droit des enfants à jouer librement pourrait être renforcé dans un monde numérique en améliorant la conception des produits et services numériques. Les responsables politiques doivent toujours chercher à s'assurer que les produits et services minimisent les risques avant d'être mis à la disposition des enfants. La conception sécuritaire et la définition des droits sont systémiques par nature et visent donc à protéger des millions d'enfants dès le départ, et non après coup.



Source : Initiative eSafety sur la conception sécuritaire[68] Outils d'auto-évaluation et principes[69]

64. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989. (Voir en particulier l'article 3, section 1, sur les droits de l'enfant).
65. Child Rights Impact Assessment (Évaluation de l'impact sur les droits de l'enfant), Digital Futures Commission (Commission sur l'avenir du numérique), 2021.
66. Child Rights Impact Assessment (Évaluation de l'impact sur les droits de l'enfant), Digital Futures Commission (Commission sur l'avenir du numérique), 2021.
67. IEEE 2089-2021 Standard for Age-Appropriate Digital Services Framework (Norme pour un cadre de services numériques adaptés à l'âge), IEEE SA, 2021.
68. Safety by Design Principles, eSafety Commissioner, 2021.
69. Safety by Design Principles, eSafety Commissioner, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5. Maintenir l'efficacité :

> **Les États parties doivent mobiliser, allouer et utiliser des ressources publiques pour mettre en œuvre la législation, les politiques et les programmes visant à réaliser pleinement les droits de l'enfant dans l'environnement numérique et à améliorer l'inclusion numérique, qui est nécessaire pour faire face à l'impact croissant de l'environnement numérique sur la vie des enfants et pour promouvoir l'égalité d'accès aux services et à la connectivité, et leur accessibilité financière.**
>
> **Les États parties doivent veiller à ce que les mandats des institutions nationales de défense des droits de l'homme et des autres institutions indépendantes pertinentes couvrent les droits de l'enfant dans l'environnement numérique et à ce que celles-ci soient en mesure de recevoir les plaintes émanant d'enfants et de leurs représentants, d'enquêter à leur sujet et d'y donner suite. Lorsqu'il existe des organes de contrôle indépendants chargés de surveiller les activités relatives à l'environnement numérique, les institutions nationales de défense des droits de l'homme doivent collaborer étroitement avec ceux-ci pour s'acquitter efficacement de leur mandat en ce qui concerne les droits de l'enfant.**
>
> Source : Observation générale n° 25 (2021), par. 28 et 31 [70]

La protection en ligne et les droits des enfants dans l'environnement numérique ne peuvent être véritablement efficaces que par des actions politiques concrètes, des ressources adéquates et leur application.

La protection en ligne des enfants concerne un large éventail de domaines politiques, notamment les technologies de l'information et des communications (TIC), l'enseignement, la justice pénale, la santé, la réglementation du secteur, l'aide sociale et familiale, les entreprises, les droits de l'homme et l'égalité, le développement international, et bien d'autres encore. La coopération entre les différents ministères et agences travaillant dans des sphères politiques est donc essentielle pour une action efficace en matière de protection en ligne des enfants. Il convient d'établir un budget afin d'allouer des ressources à la politique, tant au sein des différents départements qu'entre eux. Une politique avec des fonds insuffisants, ou un partenariat sans capacité, c'est-à-dire qui n'existe que sur le papier, n'aboutira pas à une protection efficace en ligne des enfants.

Comprendre l'efficacité signifie examiner l'impact des politiques de protection en ligne des enfants. Le suivi, l'évaluation et le recueil de données sont essentiels à l'élaboration de bonnes politiques. Apprendre et partager les leçons de l'élaboration efficace des politiques au-delà des frontières est un moyen efficace de maximiser l'efficacité. Pour vérifier l'efficacité de la politique de protection en ligne des enfants, il faut consulter non seulement les principaux acteurs concernés, mais aussi les enfants, afin de comprendre comment les actions les affectent ou pourraient les toucher à l'avenir.[71] Il s'agit d'un processus continu.

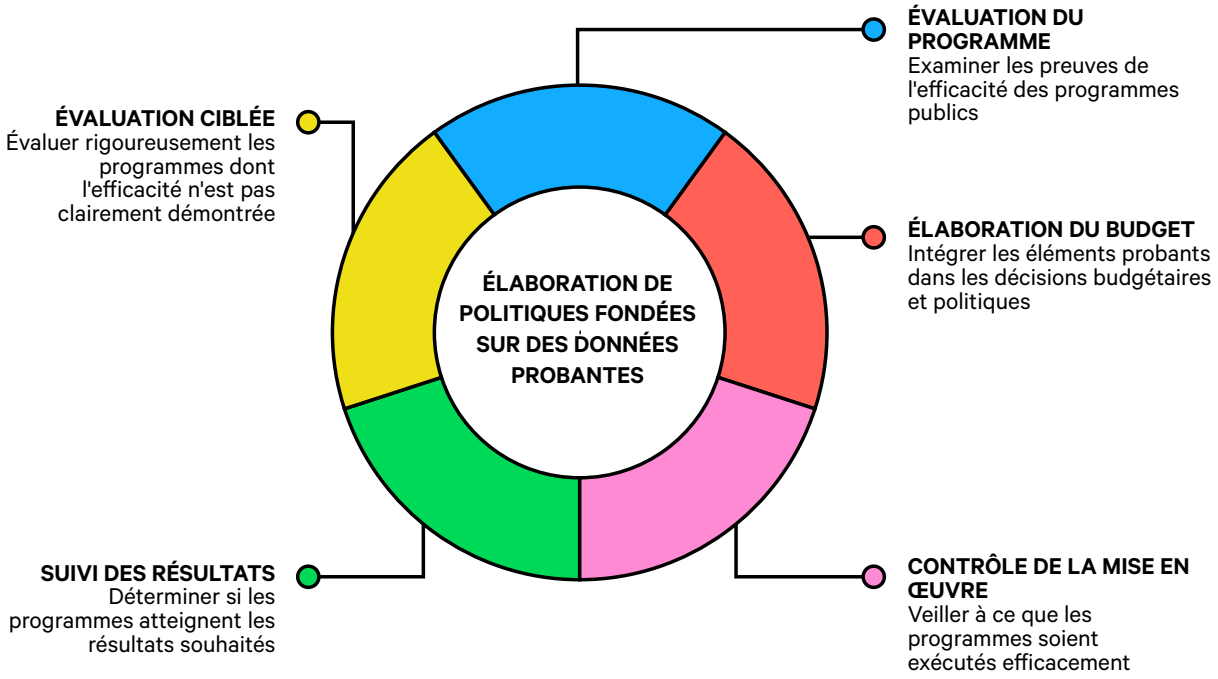
Les politiques doivent être fondées sur des données et des preuves. Aussi bien les autorités compétentes que les entreprises privées doivent être tenues de recueillir et de partager des données pour faciliter la compréhension des problèmes de protection des enfants en ligne, dans le respect des lois et des principes relatifs à la protection des données. La protection en ligne des enfants est un domaine d'action relativement nouveau, de sorte que lorsque les preuves ne sont pas disponibles ou sont contestées, les responsables politiques doivent adopter une approche de précaution, ou se tourner vers d'autres contextes et adopter une approche « qui fonctionne ». Par exemple, avec les principes de santé et de sécurité, ou des cadres tels que INSPIRE: Seven Strategies for Ending Violence Against Children (INSPIRE : sept stratégies pour mettre fin à la violence contre les enfants).[72]

70. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
71. Digital Futures Commission (Commission sur l'avenir du numérique), 5Rights Foundation, 2021.
72. INSPIRE Indicator Guidance and Results Framework (Guide des indicateurs et cadre des résultats d'INSPIRE), Organisation mondiale de la santé, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

La protection en ligne des enfants n'est pas une question isolée. L'efficacité de la politique de protection en ligne des enfants dépendra de l'efficacité globale des institutions clés et de leur capacité à collaborer en vue d'une protection efficace. La responsabilisation effective en matière de protection en ligne des enfants en général, et de prévention de l'exploitation et des abus sexuels sur mineur en particulier, repose sur des systèmes judiciaires nationaux solides. Le Modèle de réponse nationale (MRN) présente des orientations sur cette question. Les approches efficaces de la protection en ligne des enfants reposent également sur l'octroi de ressources adéquates aux institutions qui les soutiennent, notamment dans des domaines tels que l'aide psychosociale et la réglementation des TIC et des domaines connexes. Le respect effectif des droits de l'enfant par le biais d'une politique de protection en ligne dépend d'une législation efficace en matière de droits de l'homme, ainsi que d'une législation et d'une réglementation spécifiques, assorties d'organes de surveillance, afin de garantir les droits de l'enfant dans l'environnement en ligne et hors ligne.

Les responsables politiques doivent s'assurer que la capacité institutionnelle, les ressources et les mécanismes de responsabilité sont en place pour soutenir les politiques de protection en ligne des enfants. En cas de conflit, « l'intérêt supérieur » de l'enfant doit primer. Sans cela, même les meilleures politiques seront inefficaces.



Source : Pew Charitable Trusts/MacArthur Foundation: Evidence-Based Policymaking[73]

73. Evidence-Based Policymaking, MacArthur Foundation, 2014.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 5

01 Introduction 6

02 Comment l'utiliser 9

03 Pourquoi les droits de l'enfant sont-ils importants 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 **Dix domaines d'action politique** 37

06 Documents clés 169

07 Glossaire 174

08 Politique modèle 180

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Dix domaines d'action politique

Cette section fournit des modèles de politiques qui décrivent les actions pratiques nécessaires pour une politique efficace de protection en ligne des enfants, et fournit également des outils aux responsables politiques pour concevoir et fournir des mécanismes efficaces qui sont pertinents pour leur contexte national.

MODÈLES DE POLITIQUES

1. **Capacité institutionnelle**
2. **Cadre juridique et réglementaire**
3. **Données personnelles, identité et autonomie**
4. **Systèmes de réponse et d'assistance**
5. **Responsabilité d'entreprise**
6. **Formation**
7. **Enseignement**
8. **Sensibilisation du public et communications**
9. **Recherche et développement**
10. **Coopération internationale**

La mise en œuvre de chacun de ces domaines d'action politique devrait tenir compte des quatre principes directeurs sur les droits des enfants définis dans le Chapitre 3 :

PRINCIPES

- **Le droit à la non-discrimination**
- **L'intérêt supérieur de l'enfant**
- **Le droit à la vie, à la survie et au développement**
- **Le droit d'être entendu**

Et les cinq autres thèmes transversaux définis dans la section A :

CINQ ÉLÉMENTS

- **Risques et préjudices**
- **Accessibilité et inclusion**
- **Chaîne de responsabilité**
- **Conception axée sur l'enfant**
- **Efficacité**

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

> **Les États parties doivent prendre des mesures législatives et administratives pour protéger les enfants contre la violence dans l'environnement numérique, notamment en réexaminant régulièrement, en actualisant et en faisant respecter des cadres législatifs, réglementaires et institutionnels solides qui protègent les enfants contre les risques reconnus et émergents de toutes les formes de violence dans l'environnement numérique.**
>
> Source : Observation générale n° 25 (2021), par. 82[74]

Objectif :

Identifier un ministère ou un organisme responsable, chargé d'établir un Comité directeur national de la protection en ligne de l'enfant et un groupe d'experts des parties prenantes pour couvrir tous les domaines de la politique de protection en ligne des enfants. Fournir des ressources adéquates, le leadership et les capacités institutionnelles pour assurer une action et une coopération efficaces.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

1a. Affirmer l'engagement public en faveur de la protection en ligne des enfants au plus haut niveau
Les dirigeants nationaux, notamment le Premier ministre ou le Président, doivent s'engager en faveur de la protection en ligne des enfants, tant sur la scène nationale qu'internationale.

1b. Désigner un ministère ou un organisme chargé de diriger l'élaboration de la politique nationale de protection en ligne des enfants
Dans le monde entier, une série d'organismes et de ministères différents sont responsables de la politique de protection en ligne des enfants, et le choix de l'organisme ou du ministère peut affecter la manière dont la politique de protection en ligne des enfants évolue et donne la priorité à différents aspects de la protection en ligne des enfants. La protection en ligne des enfants est susceptible de relever de plusieurs ministères, mais il est important qu'un organisme responsable s'approprie le programme. Dans certains pays, la politique de protection en ligne des enfants est dirigée par le ministère responsable des TIC, dans d'autres par le ministère responsable de l'enfance et de la famille, et dans d'autres encore par le ministère de la justice. Il se peut que les groupes existants qui travaillent sur la violence à l'encontre des enfants (VEE) ou la cybersécurité puissent être élargis pour inclure l'expertise nécessaire afin d'éviter le travail en silo. *L'organisme responsable peut être choisi pour son autorité, son expertise, ses ressources, sa capacité ou sa motivation, mais tout organisme responsable devra collaborer avec d'autres.* Quel que soit le ministère qui assume la direction des opérations, il doit s'engager à adopter une approche holistique qui reflète les besoins primordiaux en matière de protection en ligne des enfants.

1c. Publier un manuel des définitions et du langage
Le ministère de tutelle désigné devra publier une liste complète des définitions et du langage qui reflète les définitions utilisées dans les meilleures pratiques internationales.[75] ▶

74. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
75. Voir par exemple Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

1d. Mettre en place un Comité directeur national chargé de la protection en ligne des enfants

Le Comité directeur national chargé de la protection en ligne des enfants sera responsable de la mise en œuvre des politiques et du développement, et servira de point focal pour la coopération nationale et régionale. Il sera responsable de la boîte à outils pour la protection en ligne des enfants et de l'élaboration d'une stratégie pour la mettre en œuvre, ce que l'on pourrait appeler le plan d'action. Le Comité se penchera sur un large éventail de compétences couvrant divers domaines d'action, notamment l'enseignement, la santé, la justice, la protection des consommateurs, la protection des données, l'application de la loi, les TIC et les services à la famille et à l'enfance, entre autres, et supervisera la mise en œuvre et le respect des normes. Le Comité sera formellement tenu de coopérer avec tous ceux qui sont chargés de la protection des enfants ou de la cybersécurité, et rendra régulièrement compte au ministère de tutelle.

1e. Comprendre les acteurs de la protection en ligne des enfants

Les organismes chargés de l'application de la loi, les entreprises, le secteur tertiaire, les organisations de défense des droits de l'enfant, les établissements d'enseignement, les parents/aidants et les universités ont tous des idées utiles et des intérêts importants en matière de protection en ligne des enfants. Dans certains contextes, la création d'un groupe de partenaires peut être utile pour soutenir le Comité dans ses activités et ancrer son plan d'action dans des scénarios réels. Dans d'autres contextes, des discussions informelles ou des appels aux preuves émanant d'un réseau ouvert d'acteurs peuvent être plus efficaces. Quoi qu'il en soit, le Comité directeur national pour la protection en ligne des enfants doit chercher à s'engager auprès des principaux acteurs susceptibles de soutenir ses activités. La coopération entre organismes doit être encouragée. L'objectif de l'engagement des partenaires est de se concentrer sur la mise en œuvre, et non sur l'élaboration de politiques.

1f. Définir les rôles et les responsabilités des partenaires

Il doit y avoir un cadre de corégulation qui définit les rôles et les responsabilités de tous les organismes développant et gérant les infrastructures numériques, les réseaux et les services, ainsi que les fonctions des ministères. Des normes minimales doivent être établies pour tous les participants à la chaîne de valeur, y compris les responsables de l'infrastructure, du matériel, des produits et services numériques et ceux qui les gèrent ou les utilisent quand ils interagissent avec les enfants. Ces normes doivent se concentrer sur la protection des enfants et la pleine réalisation des droits des enfants dans le monde numérique. La participation de la société civile et la consultation des enfants doivent être assurées dans les groupes de partenaires.

1g. Définir les indicateurs de performance et l'évaluation

Chaque aspect du plan de mise en œuvre devrait disposer d'une autorité responsable correspondante (personne, institution, organe) et de ressources humaines et financières pour mener à bien la tâche envisagée. Il se peut que la même autorité soit responsable de plus d'un domaine politique, ou d'un seul domaine d'expertise. Des indicateurs clés de performance (ICP), des mécanismes d'évaluation et des structures de signalement claires doivent être introduits pour permettre au Comité directeur de superviser et de gérer les progrès. L'environnement numérique évoluant rapidement, les indicateurs clés de performance devront être régulièrement réévalués.

1h. Assurer l'intégration de la protection en ligne des enfants dans les domaines de la politique publique

Tous les plans nationaux pertinents, tels qu'un Plan national pour le haut débit ou un cadre de maîtrise du numérique, devraient inclure une politique sur la protection en ligne des enfants dans le cadre de leur stratégie de déploiement. Les plans qui se déroulent sur plusieurs années doivent être vérifiés à des étapes clés.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

Feuille de route pour la mise en œuvre de la politique :

A **Affirmer l'engagement public en faveur de la protection en ligne des enfants au plus haut niveau**

Les dirigeants nationaux, par exemple le Premier ministre, le Président ou les ministres, doivent s'engager en faveur de la protection en ligne des enfants, tant sur la scène nationale qu'internationale.

Dans l'affirmative, veuillez préciser :

Dans la négative, cela contribuera à élaborer un plan, entièrement argumenté et s'appuyant sur un large groupe de partisans, et à le présenter aux dirigeants nationaux. Votre plan devra :

1. Décrire la justification, avec preuves et données pertinentes ; si les données ne sont pas disponibles pour votre pays, utilisez des données internationales.
2. Identifier les responsables politiques clés et cibler les efforts de plaidoyer fondés sur des preuves pour établir leur compréhension et leurs engagements.
3. Identifier et engager des défenseurs et des experts (internes, locaux et internationaux) pour plaider votre cause.
4. Examiner l'état d'avancement des efforts et politiques nationaux visant la protection en ligne des enfants et d'autres formes de violence à l'encontre des enfants (VEE), en plus des violences à l'encontre des femmes et des filles (VFF) et de la cybersécurité.
5. Sur la base de ce qui précède, convenir (en consultation avec les principales parties prenantes) de la manière de mettre en œuvre une politique globale de protection en ligne des enfants, qui inclut et s'appuie sur les programmes existants.
6. Identifier les devoirs et obligations existants conformément aux cadres existants et aux autres plans d'action nationaux et comités intersectoriels pertinents (par exemple, VEE, VFF, cybersécurité).
7. En consultation avec les principales parties prenantes, créer un plan d'action : chiffré, estimé en temps et avec un organisme responsable et une personne ou organisation désignée responsable de chaque action.
8. Apportez votre feuille de route aux responsables politiques défendant le plus votre cause, afin d'obtenir leur consentement et leur signature.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

B **Désigner un ministère ou un organisme chargé de diriger l'élaboration de la politique nationale de protection en ligne des enfants**

Dans le monde entier, une série d'agences et de ministères différents sont responsables de la politique de protection en ligne des enfants, et le choix de l'organisme ou du ministère peut affecter la manière dont la politique de protection en ligne des enfants évolue et donne la priorité à différents aspects. La protection en ligne des enfants est susceptible de relever de plusieurs ministères, mais il est important qu'un organisme responsable s'approprie le programme. Dans certains pays, la politique de protection en ligne des enfants est dirigée par le ministère responsable des TIC, dans d'autres par le ministère responsable de l'enfance et de la famille, et dans d'autres encore par le ministère de la justice. L'organisme responsable être choisi pour son autorité, son expertise, ses ressources, sa capacité ou sa motivation, mais tout organisme responsable devra collaborer avec d'autres. Quel que soit le ministère qui assume la direction des opérations, il doit s'engager à adopter une approche holistique qui reflète les besoins primordiaux en matière de protection en ligne des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile d'avoir recours à l'outil SWOT. Voir Outils d'assistance 1 (page n° 47) pour choisir un ministère ou un organisme responsable.

C **Publier un manuel des définitions et du langage**

Le ministère de tutelle désigné devra publier une liste complète des définitions et du langage qui reflète les définitions utilisées dans les meilleures pratiques internationales.[76]

Dans l'affirmative, vérifiez qu'elle est conforme aux définitions du glossaire et des définitions (page n° 178) pour assurer une traduction efficace.

Dans la négative, il sera utile de se référer au glossaire et aux définitions (page n° 178) comme meilleure pratique pour assurer une traduction efficace.

76. Voir par exemple Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

D **Comité directeur national chargé de la protection en ligne des enfants**

Le Comité directeur national chargé de la protection en ligne des enfants sera responsable de la création et de la mise en œuvre des politiques, et servira de point focal pour la coopération régionale et nationale. Il élaborera la stratégie de mise en œuvre de la Boîte à outils pour la protection en ligne des enfants. Le Comité se penchera sur un large éventail de compétences couvrant divers domaines d'action, notamment l'enseignement, la santé, la justice, la protection des consommateurs, la protection des données, l'application de la loi, les TIC et les services à la famille et à l'enfance, entre autres, et supervisera la mise en œuvre et le respect des normes. Le Comité devra rendre compte au ministère de tutelle.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Déterminer quels ministères et quelles organisations gouvernementales peuvent contribuer à la mise en œuvre efficace de la politique de protection en ligne des enfants et participer à des réunions régulières.
2. Envisager une représentation régionale ou locale qui pourrait avoir un intérêt dans la protection en ligne des enfants.
3. Faire appel à des experts de premier plan pour s'assurer que les plans sont considérés comme des pratiques exemplaires et qu'ils sont adaptés à l'objectif visé.
4. S'appuyer sur des données avérées des entreprises et de la société civile.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

E **Comprendre les acteurs de la protection en ligne des enfants**

Il peut être utile de réunir les parties prenantes au sein d'un groupe ayant pour rôle officiel d'appuyer et d'informer le Comité directeur. Il peut aussi, alternativement, être plus pratique de s'engager avec les parties prenantes sur une base plus informelle ou « selon les besoins ». Dans tous les cas, il est probable qu'il y aura un large groupe de « parties intéressées », parmi lesquelles les parents/aidants, les enseignants et les enfants, et un groupe plus restreint de personnes possédant les compétences et l'expertise pertinentes – par exemple, les organismes chargés de l'application des lois, l'industrie, les experts des droits de l'enfant, les ONG (nationales et internationales), les professionnels de santé et les universitaires. L'utilisation de leur intérêt et de leur expertise peut être très bénéfique pour défendre ou mettre en œuvre des politiques de protection en ligne des enfants dans de multiples contextes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Dresser une liste des parties prenantes, des compétences et de l'expertise qui couvrent les domaines d'action énumérés dans la boîte à outils. Pour les invites, voir le modèle fourni dans les Outils d'assistance 2 (page n° 49).
2. Veiller à ce qu'ils incluent des enfants ou des représentants qui travaillent directement avec les enfants.
3. S'il s'agit d'un groupe officiel, énoncer un mandat qui engage clairement le groupe d'intervenants à participer aux activités du Comité directeur.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

F **Définir les rôles et les responsabilités**

Il doit y avoir un cadre de corégulation qui définit les rôles et les responsabilités de tous les organismes développant et gérant les infrastructures numériques, les réseaux et les services, ainsi que les fonctions des ministères. Des normes minimales doivent être établies pour tous les participants à la chaîne de valeur, y compris les responsables de l'infrastructure, du matériel, des produits et services numériques et ceux qui les gèrent ou les utilisent quand ils interagissent avec les enfants. Ces normes doivent se concentrer sur la protection des enfants et la pleine réalisation des droits des enfants dans le monde numérique. La participation de la société civile doit être assurée dans les groupes de parties prenantes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Établir une ligne de responsabilité claire pour chacune des actions de votre plan.
2. Cartographier plusieurs agences, gouvernements, organismes réglementaires ou désignés, écoles, organismes de bienfaisance, établissements de santé et entreprises ayant des responsabilités pour s'assurer que tous les aspects sont couverts, transparents et responsables.

G **Définir les indicateurs de performance et l'évaluation**

Chaque aspect du plan de mise en œuvre devrait disposer d'une autorité responsable correspondante (personne, institution, organe) et de ressources humaines et financières pour mener à bien la tâche envisagée. Il se peut que la même autorité soit responsable de plus d'un domaine politique, ou d'un seul domaine d'expertise. Des indicateurs clés de performance (ICP), des mécanismes d'évaluation et des structures de signalement claires doivent être introduits pour permettre au Comité directeur de superviser et de gérer les progrès. L'environnement numérique évoluant rapidement, les indicateurs clés de performance devront être régulièrement réévalués.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Établir des ICP et passer en revue les processus dans le cadre du plan stratégique. Par exemple, les ICP présentés dans Child Online Protection au Rwanda.[77]
2. Délimiter clairement les attentes en termes de responsabilité avec le Comité directeur.

77. Child Online Protection in Rwanda (Protection en ligne des enfants au Rwanda), 5Rights Foundation, 2019.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

H **Assurer l'intégration de la protection en ligne des enfants dans les domaines de la politique publique**

Tous les plans nationaux pertinents, comme un Plan national pour le large bande, un plan national d'action contre la violence à l'encontre des enfants (VEE), un cadre d'habileté numérique, une stratégie de cybersécurité, etc., doivent inclure une politique de protection en ligne des enfants dans le cadre de la stratégie de déploiement. Les plans qui s'échelonnent sur plusieurs années doivent être passés en revue et mis à jour à des étapes clés.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Utiliser la liste de contrôle fournie dans les Outils d'assistance 3 pour passer en revue les domaines politiques et identifier si la protection en ligne des enfants est incluse ou non (page n° 51). Il peut être utile de nommer un expert externe pour passer en revue le plan stratégique par rapport à la politique et aux dispositions gouvernementales existantes.
2. Signaler les anomalies au Comité directeur national chargé de la protection en ligne des enfants, créé dans le cadre du processus D.

Comment cela concorde avec les documents fondamentaux :

Les gouvernements doivent mettre en place un cadre national de coordination doté d'un mandat clair et d'une autorité suffisante pour coordonner toutes les activités liées aux droits de l'enfant et aux médias numériques et aux TIC, aux niveaux intersectoriel, national, régional et local. Les gouvernements doivent fixer des objectifs assortis de délais et mettre en place un processus transparent pour évaluer et suivre les progrès accomplis et veiller à ce que les ressources humaines, techniques et financières nécessaires soient mises à disposition pour assurer le bon fonctionnement de ce cadre.

Les gouvernements doivent mettre en place une plateforme multipartite pour orienter l'élaboration, la mise en œuvre et le suivi de la stratégie numérique nationale en faveur des enfants. Une telle plateforme doit réunir des représentants des groupes les plus importants, notamment : les enfants et les jeunes ; les associations de parents/aidants ; les secteurs concernés du gouvernement ; les secteurs de l'éducation, de la justice, de la santé et de la protection sociale ; les institutions nationales des droits de l'homme et les organismes de réglementation pertinents ; la société civile ; l'industrie ; les universités ; les associations professionnelles concernées.

Source : ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[78]

78. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

Outils d'assistance :

1. Modèle SWOT pour identifier le service ou le ministère de tutelle le plus approprié

Le processus B (« Désigner un ministère ou un organisme pour prendre la direction de l'élaboration de la politique nationale de protection en ligne des enfants ») exige que vous identifiiez soigneusement le organisme responsable le plus approprié pour la protection en ligne des enfants. Cet outil est conçu pour vous aider dans ce processus.

De nombreux pays ont adopté des approches différentes pour choisir un organisme responsable, par exemple :

- **Tanzanie** – Ministère de la Santé
- **Ghana** – Ministère des Communications
- **Éthiopie** – Autorité réglementaire
- **Australie** – Ministère de l'Infrastructure, des Transports, du Développement régional et des Communications
- **Royaume-Uni** – Ministère du Numérique, de la Culture, des Médias et des Sports

Pour vous aider à sélectionner le bon ministère ou service, effectuez une analyse SWOT (anglais pour Forces, Faiblesses, Opportunités, Menaces) de chaque ministère ou service potentiel, afin d'identifier celui qui est le mieux placé pour prendre la responsabilité de la protection en ligne des enfants :

Forces	Faiblesses
Points à prendre en compte : ce ministère présente-t-il des points forts particuliers en matière de protection en ligne ? Certains des domaines d'action politique relèvent-ils déjà de la compétence du ministère ? Dispose-t-il de ressources suffisantes pour assumer les responsabilités de chef de file ? Est-il connecté et suffisamment influent pour assurer ce travail ? Est-ce que sa direction est prête à assumer le mandat et en est-elle capable ?	**Points à prendre en compte :** ce ministère présente-t-il des faiblesses particulières en matière de protection en ligne ? N'a-t-il pas les capacités ou manque-il de capacité pour assumer des responsabilités supplémentaires ? N'a-t-il pas les liens ou l'influence nécessaires pour atteindre les objectifs transversaux de cette mission ? Le mandat manque-t-il de leadership ou ne suscite-t-il pas d'intérêt ?
Opportunités	**Menaces**
Points à prendre en compte : existe-t-il des synergies entre le dossier de protection en ligne des enfants et les dossiers politiques émergents dans ce ministère (par exemple, le déploiement du haut débit ou de la 5G) ? Ce ministère est-il composé de fonctionnaires ou dirigé par des politiciens qui sont potentiellement plus efficaces que d'autres ?	**Points à prendre en compte :** ce ministère est-il déjà sous-performant sur les dossiers existants ? Existe-t-il des menaces imminentes pour le ministère (p. ex., réductions budgétaires prévues) ? Le ministère a-t-il des intérêts contradictoires qui pourraient supposer des difficultés s'il devenait responsable de ce dossier (p. ex., financement constituant conflit d'intérêt ou ententes en place avec des fournisseurs de télécommunications ou des entreprises de technologie) ? La direction est-elle proche du départ ?

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

2. Modèle pour identifier les parties prenantes

Ce modèle vous aide à répertorier les parties prenantes nécessaires pour créer un groupe de parties prenantes, avec des rôles et des responsabilités pertinents, tels que requis par le processus E (« Comprendre les parties prenantes de la protection en ligne des enfants »). Les représentants, les organisations et les rôles et responsabilités dépendront du contexte local, et il peut y en avoir plusieurs pour chaque type. Une fois que vous aurez identifié le ministère ou l'organisation qui sera responsable, il sera également important d'inclure les mêmes parties prenantes ou des parties prenantes similaires dans le processus afin d'assurer son équilibre, son efficacité et sa bonne exécution.

Les types énumérés ci-dessous reflètent ceux des Directives de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants à l'horizon 2020 et ceux mentionnés dans l'Observation générale n° 25 (2021).

Représentant des acteurs	Type	Organisation	Rôle et responsabilités
Exemple : Personne nommée ou représentant ayant le pouvoir approprié pour contribuer/prendre des décisions/assurer l'allocation des ressources	Enfants et adolescents	Groupe de jeunes X	La voix de l'enfant : fournir des idées du point de vue des enfants ; mettre en évidence les préoccupations et les questions des enfants
	Groupe consultatif des jeunes 5Rights		La voix de l'enfant : fournir des idées du point de vue des enfants ; mettre en évidence les préoccupations et les questions des enfants
	Parents, aidants, éducateurs		Veiller à ce que les politiques soutiennent les adultes assurant des prises en charge
	Industrie		Pour veiller à ce que les politiques créent des obligations de façon à ce que tous les produits et services soit axés sur l'enfant et soient sûrs
	Communauté de recherche et ONG		Pour veiller à ce que les politiques reflètent les données et l'expertise actuelles

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

Représentant des acteurs	Type	Organisation	Rôle et responsabilités
	Application de la loi		Pour veiller à ce que les politiques soient exécutoires et pour veiller à éduquer les organismes chargés de l'application de la loi
	Services sociaux		Pour veiller à ce que les politiques prennent en compte les enfants vulnérables
	Services de santé		Pour traduire les conseils médicaux et le soutien aux victimes en ligne, ou le soutien aux enfants exposés ou à qui il a été fait du mal
	Ministères du gouvernement et entités de réglementation		Pour impliquer des entités de réglementation et ministères spécialistes qui ne soient pas du ministère responsable
	Opérateurs de réseau large bande, mobile et Wi-Fi		Pour faciliter un accès au numérique qui soit sûr et économiquement abordable pour les enfants
	Organisations de défense des droits de l'enfant		Pour veiller à ce que la gamme complète des droits de l'enfant soit activée et réalisée dans les politiques numériques
	Universitaires, avocats, individus, organisations disposant d'une expertise particulière, par exemple droit, audit algorithmique, pratiques de modération, etc.		Pour fournir une aide spécialisée « selon les besoins », pour veiller à ce que les politiques soient sophistiquées mais aussi pratiques

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

3. Liste de contrôle pour identifier les domaines politiques qui traitent de la protection en ligne des enfants

Cette liste de contrôle vous aide à passer en revue les politiques existantes pertinentes, afin de déterminer si chacune contient ou non un élément traitant de la protection en ligne des enfants. Elle vous aide à remplir les conditions du processus H (« Assurer l'intégration de la protection en ligne des enfants dans tous les domaines d'action du gouvernement »).

Veuillez informer le groupe des parties prenantes travaillant sur la protection en ligne des enfants des conclusions de cet examen.

Élément de protection en ligne des enfants reflété dans la politique de protection en ligne des enfants	Cocher si déjà inclus	Si ce n'est pas le cas, identifier les lacunes et les anomalies, et les changements recommandés, et faire rapport au groupe de parties prenantes travaillant sur la protection en ligne des enfants
Plan national pour le large bande	☐	☑
Cadres de mise en œuvre des objectifs de développement durable et feuilles de route	☐	
Tous les programmes d'enseignement et de formation nécessaires	☐	
Cadres d'habileté numérique pour les enfants	☐	
Programme éducatif national pour les écoles	☐	
Programme de formation professionnelle des enseignants et des travailleurs sociaux	☐	
Programme de formation professionnelle de la police et des organismes chargés de l'application de la loi	☐	

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

Élément de protection en ligne des enfants reflété dans la politique de protection en ligne des enfants	Cocher si déjà inclus	Si ce n'est pas le cas, identifier les lacunes et les anomalies, et les changements recommandés, et faire rapport au groupe de parties prenantes travaillant sur la protection en ligne des enfants
Droits des consommateurs	☐	
Violence à l'encontre des enfants, protection de l'enfance et stratégie de sauvegarde	☐	
Justice pénale	☐	
Droits de l'homme	☐	
Droits de l'enfant	☐	
Égalités et lutte contre la discrimination	☐	
Protection des données	☐	
Commerce international	☐	
Contrôles des jeux de hasard	☐	

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

1 Capacité institutionnelle

Élément de protection en ligne des enfants reflété dans la politique de protection en ligne des enfants	Cocher si déjà inclus	Si ce n'est pas le cas, identifier les lacunes et les anomalies, et les changements recommandés, et faire rapport au groupe de parties prenantes travaillant sur la protection en ligne des enfants
Normes publicitaires	☐	
Délits financiers	☐	
Enseignement	☐	
Santé	☐	
Coopération internationale	☐	
Autres	☐	

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

1 Capacité institutionnelle

Autres ressources pour référence :

1. **Le UK Council for Internet Safety (UKCIS) comme modèle de groupe de parties prenantes travaillant sur la protection en ligne des enfants[79]**

   Le UK Council for Internet Safety (UKCIS) est un forum de collaboration via lequel le gouvernement, la communauté technologique et le secteur tertiaire travaillent tous ensemble. UKCIS fait partie du ministère du numérique, de la culture, des médias et des sports, du ministère de l'éducation et du ministère de l'intérieur. Au fil du temps, UKCIS est devenu un lieu de rencontre pour les entreprises, les universitaires, les experts de la protection des enfants, les fonctionnaires et les ministres. Il a également commandé d'importantes recherches qui ont fourni une base de données probantes pour l'élaboration de politiques. Contrairement à la recommandation de la Boîte à outils, UKCIS n'a pas été formellement attaché à un plan d'action pour un groupe de pilotage.

2. **Guide de l'UIT pour l'élaboration d'une stratégie nationale de cybersécurité – engagement stratégique dans la cybersécurité[80]**

   Avec l'aide de l'UIT, douze partenaires des secteurs public et privé, du monde universitaire et de la société civile partagent leur expérience, leurs connaissances et leur expertise, et produisent un ensemble de principes agrégés et harmonisés sur l'élaboration, l'établissement et la mise en œuvre de stratégies nationales de cybersécurité. L'objectif du guide est de susciter une réflexion stratégique et d'aider les dirigeants et les responsables politiques nationaux à élaborer, établir et mettre en œuvre des stratégies nationales de cybersécurité dans le monde entier.

3. **Manuel du Conseil de l'Europe à l'attention des responsables politiques sur les droits de l'enfant dans l'environnement numérique[81]**

   Ce manuel vise à aider les États membres du Conseil de l'Europe à mettre en œuvre la recommandation CM/Rec(2018)7 et les lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique. Ce document comprend les premières directives complètes au monde, à l'attention des États, concernant les droits de l'enfant dans l'environnement numérique.

4. **Protection en ligne des enfants au Rwanda[82]**

   Créée en partenariat entre la 5Rights Foundation, l'University of East London, l'Université du Rwanda et le gouvernement du Rwanda, la politique de protection en ligne des enfants offre un plan de mise en œuvre de haut niveau comme exemple pour toute nation se penchant sur la question de la protection en ligne des enfants.

79. UK Council for Internet Safety, Department for Digital Culture, Media & Sport, Department for Education & Home Office, 2021.
80. Guide pour l'élaboration d'une stratégie nationale de cybersécurité - Engagement stratégique dans la cybersécurité, Union internationale des télécommunications, 2018.
81. Manuel à l'attention des responsables politiques sur les droits de l'enfant dans l'environnement numérique, Conseil de l'Europe, 2020.
82. Child Online Protection in Rwanda (Protection en ligne des enfants au Rwanda), 5Rights Foundation, 2019.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

« Je pense que les données ne sont jamais vraiment sécurisées, quels que soient les paramètres de sécurité mis en place. »

– Enfant vivant en Allemagne, 16 ans

« Dès qu'on parle de quelque chose devant son téléphone, le lendemain, on a une publicité sur les réseaux sociaux pour cette même chose. Je pense que c'est parce qu'ils veulent qu'on interagisse davantage, parce que plus on interagit, plus ils gagnent de l'argent. »

– Enfant vivant au Royaume-Uni, 16 ans

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

> **Les enfants peuvent avoir des difficultés particulières à obtenir réparation lorsque leurs droits ont été violés dans l'environnement numérique par des entreprises commerciales, en particulier dans le cadre de leurs opérations mondiales. Les États parties doivent envisager des mesures qui veillent au respect, à la protection et à la mise en œuvre des droits de l'enfant dans le contexte des activités et opérations extraterritoriales des entreprises, à condition qu'il existe un lien raisonnable entre l'État et le comportement concerné. Ils doivent veiller à ce que les entreprises mettent en place des mécanismes de plainte efficaces ; ces mécanismes ne devraient toutefois pas empêcher les enfants d'avoir accès à des recours étatiques. Ils doivent également veiller à ce que les agences dotées de pouvoirs de contrôle en matière de droits de l'enfant, tels que ceux relatifs à la santé et à la sécurité, à la protection des données et aux droits des consommateurs, à l'éducation, à la publicité et au marketing, enquêtent sur les plaintes et prévoient des recours adéquats en cas de violation ou d'abus des droits de l'enfant dans l'environnement numérique.**
>
> Source : Observation générale n° 25 (2021), par. 48[83]

Objectif :

Renforcer et réaligner les régimes juridiques et réglementaires nationaux en matière de protection en ligne des enfants, et renforcer la capacité et les aptitudes des organismes de maintien de l'ordre public et des organismes de réglementation dans le domaine de la protection en ligne des enfants, y compris leur capacité à collaborer avec d'autres secteurs, en particulier le secteur TIC.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

2a. Renforcer et appliquer les lois qui interdisent les infractions liées à la protection en ligne des enfants
Les lois et les procédures pénales facilitent les enquêtes et la poursuite des infractions en ligne contrevenant au droit des enfants à la protection et devront être renforcées et modifiées conformément aux normes et aux meilleures pratiques internationales. Elles doivent inclure l'introduction de l'évaluation obligatoire des risques pour atténuer le potentiel de dommages, alourdir les sanctions et les cadres de fixation des peines lorsque cela est nécessaire. Elles doivent également inclure la possibilité de procédures de notification et de retrait. Les lois pénales relatives à la protection en ligne des enfants doivent être élaborées à la lumière de tous les droits des enfants, y compris leur droit d'être entendu et leur droit à la participation.[84]

83. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
84. Par exemple, les cadres juridiques qui ne précisent pas clairement si les images sexuelles autogénérées échangées entre enfants sur une base consensuelle seront considérées comme du matériel illégal concernant l'abus sexuel sur mineur. Même si les enfants ne sont pas poursuivis dans la pratique, cette incertitude juridique avec une criminalisation potentielle peut porter atteinte à la confiance, au contrôle et aux droits d'autonomie.

2 Cadre juridique et réglementaire

2b. Adopter une réglementation sur la protection des données et instaurer des autorités de contrôle indépendantes, en veillant à ce que les données des enfants soient adéquatement protégées et recueillies uniquement lorsque c'est nécessaire, avec des niveaux élevés de sécurité et d'attention
Une telle réglementation générale doit inclure un statut de catégorie spéciale applicable aux données relatives aux enfants, exigeant des niveaux plus élevés de protection et de garanties par défaut, ainsi que des protections contre l'utilisation commerciale inappropriée des données relatives aux enfants. Lorsque le consentement des enfants, ou des parents/personnes qui s'occupent d'eux, est demandé pour le recueil et le traitement en ligne des données des jeunes enfants, il doit être éclairé et significatif. Le recueil de données à des fins de protection doit faire l'objet d'une attention particulière dans des circonstances exceptionnelles, lorsque cela est dans l'intérêt supérieur de l'enfant.

2c. Renforcer les enquêtes pénales, les poursuites et les peines pour l'exploitation sexuelle ou les abus en ligne des enfants[85]
Les organismes de justice pénale responsables des infractions liées à la protection en ligne des enfants doivent être formés aux questions de protection en ligne des enfants afin de favoriser une meilleure prévention, des poursuites efficaces et des condamnations appropriées, ainsi qu'une meilleure compréhension de l'impact sur les victimes. Les capacités des équipes d'enquête et d'intervention concernées doivent être évaluées et renforcées pour détecter, prévenir et répondre aux menaces de cybersécurité, en particulier celles liées à la protection en ligne des enfants. Les systèmes de justice pénale doivent être en mesure d'assurer un accès rapide à la justice.

2d. Revoir et renforcer les systèmes de justice pour les jeunes
Veiller à ce que la loi soit claire et proportionnée afin de réduire au minimum le risque que des enfants ne se retrouvent dans une situation de conflit avec la loi dans le contexte de la protection en ligne des enfants. Lorsque des enfants font l'objet de sanctions pénales liées à la protection en ligne des enfants, par exemple en cas de cyberharcèlement ou d'abus sexuel basé sur l'image, le système judiciaire doit tout mettre en œuvre pour éviter que les enfants ne soient criminalisés et fournir un soutien et une représentation juridique adéquats aux enfants qui se retrouvent en conflit avec la loi afin de protéger leurs droits.

2e. Identifier et ratifier les traités et protocoles internationaux relatifs à la protection en ligne des enfants
La création d'un écosystème durable pour la protection en ligne des enfants exige une approche multipartite et une participation à l'échelle mondiale. Chaque pays doit identifier et ratifier les protocoles et traités internationaux et régionaux pertinents et prendre des mesures pour mettre en œuvre leurs dispositions.

2f. Renforcer la capacité des organismes d'application de la loi
Les lacunes dans l'application de la loi et dans le système judiciaire seront identifiées, et des mesures seront mises en place pour accroître la sensibilisation, la communication et le succès de la poursuite des délinquants. La formation internationale et le partage des compétences doivent être recherchés dans la mesure du possible, et la coordination et la collaboration intersectorielles entre l'industrie et les services chargés de l'application de la loi doivent être encouragées.

85. L'exploitation et les abus sexuels sur mineur (CSEA) désignent le fait qu'un enfant soit forcé ou pressé par autrui à prendre part à des activités sexuelles. Cela peut impliquer un contact physique ou des activités sans contact et peut se produire en ligne ou hors ligne.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

Feuille de route pour la mise en œuvre de la politique :

A **Renforcer et appliquer les lois qui interdisent les infractions liées à la protection en ligne des enfants**

Les lois et les procédures pénales facilitent les enquêtes et la poursuite des infractions en ligne contrevenant au droit des enfants à la protection et devront être renforcées et modifiées conformément aux normes et aux meilleures pratiques internationales. Elles doivent inclure l'introduction de l'évaluation obligatoire des risques pour atténuer le potentiel de dommages, alourdir des sanctions et les cadres de fixation des peines lorsque cela est nécessaire. Elles doivent également inclure la possibilité de procédures de notification et de retrait. Les lois pénales relatives à la protection en ligne des enfants doivent être élaborées à la lumière de tous les droits des enfants, y compris leur droit d'être entendu et leur droit à la participation.[86]

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Identifier les lois pertinentes. Pour les invites, voir la liste de contrôle fournie dans les Outils d'assistance 1 (page n° 64).
2. Vérifier le respect des normes internationales dans chacun des domaines, c'est-à-dire la justice pour les jeunes, etc.
3. Effectuer des évaluations des risques sur les lois existantes.
4. Analyse des lacunes de la commission par des experts.
5. Proposer des amendements aux lois existantes.
6. Planifier les efforts de plaidoyer pour s'assurer que les amendements sont adoptés et que leur mise en œuvre est adéquatement financée.

86. Par exemple, les cadres juridiques qui ne précisent pas clairement si les images sexuelles autogénérées échangées entre enfants sur une base consensuelle seront considérées comme du matériel illégal concernant l'abus sexuel sur mineur. Même si les enfants ne sont pas poursuivis dans la pratique, cette incertitude juridique avec une criminalisation potentielle peut porter atteinte à la confiance, au contrôle et aux droits d'autonomie.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

2 Cadre juridique et réglementaire

B **Adopter une réglementation sur la protection des données et instaurer des autorités de contrôle indépendantes, veiller à ce que les données des enfants soient adéquatement protégées et recueillies uniquement lorsque c'est nécessaire, avec des niveaux élevés de sécurité et d'attention**

Certaines juridictions disposent d'une législation générale sur la protection des données qui peut nécessiter un renforcement ou une formalisation, afin de garantir que les enfants bénéficient de protections adaptées à leur âge. Dans d'autres, où il n'y a pas ou peu de protection des données, il peut être nécessaire de présenter une législation sur la protection des données exclusivement pour les enfants. Dans les deux cas, les données relatives aux enfants doivent être considérées comme une catégorie spéciale, exigeant des niveaux de protection et des garanties plus élevés par défaut, ainsi que des protections contre l'utilisation commerciale inappropriée des données relatives aux enfants. Lorsque le consentement des enfants, ou des parents/aidants en leur nom, est demandé pour le recueil et le traitement en ligne des données des jeunes enfants, il doit être éclairé et significatif. Le recueil de données à des fins de protection doit faire l'objet d'une attention particulière dans des circonstances exceptionnelles, lorsque cela est dans l'intérêt supérieur de l'enfant.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Effectuer une analyse des lacunes des cadres réglementaires existants en matière de protection des données.
2. Proposer de nouveaux règlements ou des modifications, avec ressources et preuves à l'appui.
3. Mettre en place ou doter en ressources les autorités de surveillance indépendantes existantes pour surveiller et assurer la conformité.
4. Aligner la protection des données des enfants sur la pratique internationale existante.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

C **Renforcer les enquêtes pénales, les poursuites et les peines pour l'exploitation sexuelle ou les abus en ligne des enfants**[87]

Les organismes de justice pénale responsables des infractions liées à la protection en ligne des enfants doivent être formés aux questions de protection en ligne des enfants afin de favoriser une meilleure prévention, des poursuites efficaces et des condamnations appropriées, ainsi qu'une meilleure compréhension de l'impact sur les victimes. Les capacités des équipes d'enquête et d'intervention concernées doivent être évaluées et renforcées pour détecter, prévenir et répondre aux menaces de cybersécurité et aux menaces liées à la protection en ligne des enfants. Les systèmes de justice pénale doivent être en mesure d'assurer un accès rapide à la justice.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Intégrer la protection en ligne des enfants au programme (voir le domaine d'action de la politique sur la formation pour accéder à des conseils et des ressources, page n° 144).
2. Examiner les compétences et les lacunes relatives à la protection en ligne des enfants.
3. Examiner les ressources conçues pour assurer un accès effectif à une justice axée sur l'enfant.

87. L'exploitation et les abus sexuels sur mineur (CSEA) désignent le fait qu'un enfant soit forcé ou pressé par autrui à prendre part à des activités sexuelles. Cela peut impliquer un contact physique ou des activités sans contact et peut se produire en ligne ou hors ligne.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

D Revoir et renforcer les systèmes de justice pour les jeunes

Veiller à ce que la loi soit claire et proportionnée afin de réduire au minimum le risque que des enfants ne se retrouvent dans une situation de conflit avec la loi dans le contexte de la protection en ligne des enfants. Lorsque des enfants font l'objet de sanctions pénales liées à la protection en ligne des enfants, par exemple en cas de cyberharcèlement ou d'abus sexuel basé sur l'image, le système judiciaire doit tout mettre en œuvre pour éviter que les enfants ne soient criminalisés et fournir un soutien et une représentation juridique adéquats aux enfants qui se retrouvent en conflit avec la loi afin de protéger leurs droits.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Procéder à un examen et à une analyse des lacunes du système de justice pour les jeunes.
2. Proposer des amendements si nécessaire.
3. Entreprendre le renforcement des capacités des professionnels clés et envisager des stratégies de prévention et de sensibilisation pour réduire les risques de criminalisation.

E Identifier et ratifier les traités et protocoles internationaux relatifs à la protection en ligne des enfants

La création d'un écosystème durable pour la protection en ligne des enfants exige une approche multipartite et une participation à l'échelle mondiale. Chaque pays doit identifier et ratifier les protocoles et traités internationaux et régionaux pertinents et prendre des mesures pour mettre en œuvre leurs dispositions.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Consulter les ressources dans l'annexe D.
2. Répertorier les instruments pertinents.
3. Identifier les obstacles à la ratification.
4. Élaborer des propositions de signature et de ratification.
5. Signer et ratifier.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

F **Renforcer la capacité des organismes d'application de la loi**

Les lacunes dans l'application de la loi et dans le système judiciaire doivent être identifiées, et des mesures mises en place pour accroître la sensibilisation, la communication et le succès de la poursuite des délinquants. La formation internationale et le partage des compétences doivent être recherchés dans la mesure du possible, et la coordination et la collaboration intersectorielles entre l'industrie et les services chargés de l'application de la loi doivent être encouragées.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Identifier les lacunes en matière de compétences
2. Identifier les modules de formation (voir Domaine d'action politique sur la formation pour accéder à des conseils et des ressources, page n° 144).
3. Identifier les partenaires nationaux et internationaux possibles pour le partage des compétences (voir Action politique sur la coopération internationale pour les ressources, page n° 161).

Comment cela concorde avec les documents fondamentaux :

« La législation et la réglementation sont des instruments essentiels pour s'assurer que les activités et les opérations des entreprises ne nuisent pas aux droits de l'enfant et ne les enfreignent pas. Les États devraient légiférer pour assurer la réalisation des droits de l'enfant et établir un cadre législatif et réglementaire clair et prévisible qui permette aux entreprises de respecter ces droits. »

Source : Observation générale n° 16 (2013) sur les obligations de l'État concernant l'impact du secteur privé sur les droits de l'enfant, par. 53[88].

Nonobstant l'existence de mécanismes internes de réclamation, les gouvernements doivent mettre en place des mécanismes de surveillance qui permettent d'enquêter sur les violations aux droits de l'enfant et d'obtenir réparation, en vue d'améliorer la responsabilisation des TIC et d'autres entreprises concernées, et de renforcer la responsabilité des organismes de réglementation en ce qui concerne l'élaboration de normes relatives aux droits de l'enfant et aux TIC. Cela est d'autant plus important que les autres voies de recours ouvertes aux personnes lésées par les actions des entreprises, telles que les procédures civiles et autres recours judiciaires, sont souvent lourdes et coûteuses.

Source : ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[89]

88. Observation générale n° 16 (2013) sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant, Convention des Nations Unies relative aux droits de l'enfant, 2013.
89. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

Outils d'assistance :

1. Liste de contrôle juridique : un exemple

Conçue pour vous aider à identifier les lois et les politiques pertinentes dans votre juridiction dans le cadre du processus A (« Renforcer et appliquer les lois qui interdisent les infractions liées à la protection des enfants en ligne »). Les exemples au Royaume-Uni sont donnés à titre indicatif et doivent être remplacés par des exemples nationaux ou régionaux pertinents.

Domaines politiques	Loi/réglementation	Statut	La protection en ligne des enfants y est-elle incluse ?	Entité de réglementation/ tribunal
Droits des consommateurs	Consumer Rights Act 2015 (Loi de 2015 sur les droits des consommateurs)[90] Toy (Safety) Regulations 2011 (Règlements de 2011 sur les jouets (sécurité))[91] General Product Safety Regulations 2005 (Règlement général de 2005 sur la sécurité des produits)[92]	Loi Texte réglementaire Texte réglementaire	Oui	Tribunal
Protection de l'enfance	Children and Social Work Act 2017 (Loi de 2017 sur les enfants et le travail social)[93] Children Act 2004 (Loi de 2004 sur l'enfance)[94] Digital Economy Act 2017 (Loi de 2017 sur l'économie numérique)[95]	Loi Loi Loi	Oui	Tribunal des affaires familiales
Justice pénale	Différentes infractions définies par la législation pénale	Loi	Oui	Tribunal
Droits de l'homme, y compris droits de l'enfant	Human Rights Act 1998 (Loi de 1998 relative aux droits de l'homme)[96] Convention des Nations Unies sur les droits de l'enfant[97] Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique[98]	Loi Traité Traité	Oui	Tribunal Commission de l'égalité et des droits de l'homme (et commissions nationales) Rapport au Comité des droits de l'enfant des Nations unies Tribunaux des Nations Unies

90. Consumer Rights Act 2015, Chapter 3 Digital Content, Royaume-Uni ; Consumer Rights Act (Digital Content) Guidance for Business, Department for Business Innovation and Skills, 2015.
91. Toy (Safety) Regulations 2011, Office for Product Safety & Standard, 2011.
92. General Product Safety Regulations 2005, gouvernement du Royaume-Uni, 2017.
93. Children and Social Work Act 2017, Chapter 2 Safeguarding Children, gouvernement du Royaume-Uni, 2004.
94. Children Act 2004, gouvernement du Royaume-Uni, 2004.
95. Digital Economy Act 2017, gouvernement du Royaume-Uni, 2017.
96. Human Rights Act 1998, gouvernement du Royaume-Uni, 1998.
97. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
98. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, Comité des droits de l'enfant des Nations Unies, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

Domaines politiques	Loi/réglementation	Statut	La protection en ligne des enfants y est-elle incluse ?	Entité de réglementation/ tribunal
Protection des données	Code de conception adaptée à l'âge 2020[99] Loi sur la protection des données de 2018[100]	Loi Loi	Oui	Bureau du Commissaire à l'information
Commerce international	Trade Act 2021[101] (ajoute une clause de protection de l'enfance)	Loi	Oui	Tribunal
Jeux de hasard	Gambling Act 2005 (Loi de 2005 sur les jeux de hasard)[102]	Loi	Oui	Commission des jeux de hasard
Publicité	Autorité des normes régissant la publicité, CAP code 2010[103] Autorité des normes régissant la publicité, BCAP Code 2010[104]	Volontaire Volontaire	Oui	Organisation associative avec corégulation sous l'égide de l'Ofcom
Délits financiers	Fraud Act 2006 (Loi sur la fraude de 2006)[105] Theft Act 1968 (Loi de 1968 sur le vol)[106] Proceeds of Crime Act 2002 (Loi de 2002 sur les produits du crime)[107] Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017 (Règlement de 2017 sur le blanchiment d'argent, le financement du terrorisme et le transfert de fonds (renseignements à l'attention du payeur))[108] Sanctions and Anti-Money Laundering Act 2018 (Loi de 2018 sur les sanctions et la lutte contre le blanchiment d'argent)[109]	Loi Loi Loi Loi Loi	Non, mais il existe en revanche un code de conduite volontaire des sociétés de cartes de crédit relatif à l'exploitation et aux abus sexuels sur mineurs et à la pornographie	Tribunal Tribunal Tribunal Autorité des services judiciaires et financiers Autorité des services judiciaires et financiers

99. Age appropriate design code 2020 (Code de conception adapté à l'âge), gouvernement du Royaume-Uni, 2020.
100. Data Protection Act 2018, gouvernement du Royaume-Uni, 2018.
101. Trade Act 2021, gouvernement du Royaume-Uni, 2021.
102. Voir Gambling Act 2005 Part 1, Section 4 (Remote gambling) and Part 4 (Protection of children and young persons) 2005, Gouvernement du Royaume-Uni, 2005.
103. Voir Advertising Standards Authority Non Broadcast CAP Code Section 5 (Children), Advertising Standards Authority (Autorité des normes régissant la publicité), 2010.
104. Voir Advertising Standards Authority Broadcast BCAP Code Section 5 (Children), Advertising Standards Authority (Autorité des normes régissant la publicité), 2010.
105. Fraud Act 2006, gouvernement du Royaume-Uni, 2006.
106. Theft Act 1968, gouvernement du Royaume-Uni, 1968.
107. Proceeds of Crime Act 2002, gouvernement du Royaume-Uni, 2002.
108. Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017 (Règlement de 2017 sur le blanchiment d'argent, le financement du terrorisme et le transfert de fonds (renseignements à l'attention du payeur), gouvernement du Royaume-Uni, 2017.
109. Sanctions an Anti-Money Laundering Act 2018, gouvernement du Royaume-Uni, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2 Cadre juridique et réglementaire

Domaines politiques	Loi/réglementation	Statut	La protection en ligne des enfants y est-elle incluse ?	Entité de réglementation/ tribunal
Enseignement	Children and Social Work Act 2017 (Loi de 2017 sur les enfants et le travail social)[110] Convention des Nations Unies sur les droits de l'enfant[111] Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique[112]	Loi Traité Traité	Oui	Tribunal, Ofsted Rapport au Comité des droits de l'enfant des Nations unies
Santé	Loi sur la santé et la protection sociale 2012[113]	Loi	Non	Médecin-chef Tribunal Tribunal des affaires familiales
Coopération internationale	Objectifs de Développement Durable[114]	Accord international	Non	Tribunal
Égalité	Equality Act 2010 (Loi sur l'égalité de 2010)[115]	Loi	Non	Tribunal Commission de l'égalité et des droits de l'homme et Commissions nationales dans les pays décentralisés

110. Children and Social Work Act 2017, gouvernement du Royaume-Uni, 2017 (en particulier le Chapitre 4 sur les relations, le sexe et l'éducation personnelle, sociale, sanitaire et économique).
111. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
112. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, Comité des droits de l'enfant des Nations Unies, 2021.
113. Health and Social Care Act 2012 (Loi sur la santé et la protection sociale de 2012), gouvernement britannique, 2012.
114. Transforming our world: the 2030 Agenda for Sustainable Development (Transformer notre monde : l'Agenda 2030 pour le développement durable), Nations Unies, 2021.
115. Equality Act 2010 (Loi de 2010 sur l'égalité), gouvernement britannique, 2010.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

2. Une liste de contrôle juridique vierge à compléter

Conçue pour vous aider à identifier les lois et les politiques pertinentes dans votre juridiction dans le cadre du processus A (« Renforcer et appliquer les lois qui interdisent les infractions liées à la protection des enfants en ligne »).

Domaines politiques	Loi/réglementation	Statut	La protection en ligne des enfants y est-elle incluse ?	Entité de réglementation/ tribunal
Droits des consommateurs				
Protection de l'enfance				
Justice pénale				
Droits de l'homme, y compris droits de l'enfant				
Protection des données				
Plans nationaux sur le large bande				
Commerce international				

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

2 Cadre juridique et réglementaire

Domaines politiques	Loi/réglementation	Statut	La protection en ligne des enfants y est-elle incluse ?	Entité de réglementation/ tribunal
Jeux de hasard				
Publicité				
Délits financiers				
Enseignement				
Santé				
Coopération internationale				
Égalité				
Autre				

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

Autres ressources pour références :

1. Étude de cas sur les mécanismes de contrôle en Albanie[116]

Le Conseil national pour les droits et la protection de l'enfant est créé par la loi, sous la forme d'un comité national de gouvernance et de contrôle responsable ; la protection contre l'exploitation et les abus sexuels des enfants en ligne est incluse aux principales politiques et législations.

2. La loi ghanéenne sur la cybersécurité (loi 1038)[117]

La loi ghanéenne sur la cybersécurité (loi 1038) contient des dispositions visant à protéger les enfants en ligne, en érigeant en infraction pénale les comportements sexuels impliquant des enfants. Les images et photographies indécentes d'enfants, la manipulation psychologique des enfants à des fins d'abus sexuels, le harcèlement en ligne et l'extorsion sexuelle sont tous interdits par la loi. La loi impose certaines obligations aux fournisseurs de services de télécommunication aux fins de protéger les enfants dans l'espace numérique. D'autres amendements ont été proposés à la loi sur l'enfance (loi 560).

116. Programming for children's protection online in Albania: A Promising Practice (Programmation pour la protection des enfants en ligne en Albanie : une pratique prometteuse), UNICEF, 2020.
117. Loi sur la cybersécurité de 2020, gouvernement du Ghana, ministère des Communications et de la Numérisation (Loi 1038), 2020.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

« J'aimerais utiliser les technologies numériques pour améliorer le monde, ce que je ne suis pas vraiment en mesure de faire actuellement. J'aimerais quand même pouvoir y parvenir, car ce serait quelque chose de positif et ça servirait l'intérêt général. »

– Enfant vivant en Allemagne, 16 ans

« J'utilise des fils de discussion en ligne pour parler de questions importantes avec d'autres personnes. »

– Enfant vivant en Indonésie, 14 ans

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

> **Les États parties doivent prendre des mesures législatives, administratives et autres pour faire en sorte que la vie privée des enfants soit respectée et protégée par toutes les organisations et dans tous les environnements qui traitent leurs données. La législation doit prévoir des garanties solides, assurer la transparence, un contrôle indépendant et l'accès à des voies de recours. Les États parties doivent exiger l'intégration de la protection de la confidentialité dès la conception dans les produits et services numériques qui touchent les enfants. Ils doivent réexaminer régulièrement la législation relative à la protection de la confidentialité et des données et veiller à ce que les procédures et les pratiques empêchent les violations délibérées ou accidentelles de la confidentialité des enfants. Lorsque le chiffrement est considéré comme un moyen approprié, les États parties doivent envisager des mesures appropriées permettant de détecter et de signaler l'exploitation et les abus sexuels d'enfants ou le matériel concernant l'abus sexuel sur mineur. Ces mesures doivent être strictement limitées, conformément aux principes de légalité, de nécessité et de proportionnalité.**
>
> Source : Observation générale n° 25 (2021), par. 701[118]

Objectif :

Reconnaître les bienfaits des mesures et répondre aux menaces actuelles et émergentes concernant la confidentialité, l'identité et la représentation des enfants dans le monde numérique, posées par l'utilisation de données, y compris de données à caractère personnel, de biométrie et de prise de décision automatisée.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

3a. Établir ou s'assurer que les cadres de protection des données existants sont efficaces pour fournir une protection spécifique des données des enfants

Les droits des enfants dans l'environnement en ligne sont intimement liés à la façon dont leurs données sont collectées, stockées et utilisées. La loi et la réglementation sur la protection des données liées aux enfants doivent être accessibles, efficaces et capables d'évoluer pour faire face aux risques émergents.[119] Cela suppose non seulement d'établir des cadres juridiques et réglementaires, mais aussi de s'assurer qu'ils fonctionnent dans la pratique et sont mis en œuvre en conséquence.

3b. Établir des protocoles et des restrictions quant à l'utilisation de la prise de décision automatisée pouvant affecter les enfants

Les normes, les lois et les codes de pratique doivent garantir que les enfants bénéficient des systèmes automatisés et ne soient pas pénalisés par la prise de décision automatisée.[120] Il est particulièrement important d'éviter le risque de discrimination dans la prise de décision automatisée. Ces protocoles et ces limites peuvent s'appliquer dans le cadre de la justice pénale, la protection sociale, la santé et la médecine, l'enseignement et le secteur privé, entre autres. ▶

118. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
119. Règlement général sur la protection des données, Union européenne, 2018.
120. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert (Un expert des droits de l'homme de l'ONU met en garde contre la dérive du monde vers une dystopie de l'aide sociale numérique), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2019.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

3c. Assurer des protections juridiques et réglementaires adéquates pour les données biométriques des enfants
Le gouvernement et les organismes de réglementation doivent établir des protocoles juridiques et réglementaires appropriés et des restrictions à l'utilisation des données biométriques des enfants à la lumière des principes des droits des enfants, de la limitation de la finalité et des exigences de la politique de protection en ligne des enfants.

3d. Établir des directives, des lois et des réglementations claires sur les pratiques susceptibles d'affecter la représentation des enfants
Créer des cadres juridiques empêchant le ciblage et le suivi personnalisés des enfants à des fins commerciales sur la base de leurs données personnelles. Établir des codes concernant l'utilisation des systèmes de recommandation et des autres processus ou technologies de prise de décision automatisée susceptibles d'orienter le comportement des enfants, de modeler leurs préférences et leurs opinions, de porter atteinte à leur réputation ou de limiter leur expérience.[121]

3e. Mettre en place une surveillance et un suivi efficaces
Créer des organes et des systèmes qui puissent recueillir des informations pertinentes pour la protection en ligne des enfants et assurer la transparence et la mise en œuvre efficace des droits et des protections des enfants par les entreprises, les gouvernements et les autres organisations.

3f. Établir des cadres pour assurer la transparence
La surveillance doit être assurée par un organisme de réglementation désigné qui dispose de ressources suffisantes et qui dispose des capacités et de l'expertise nécessaires pour comprendre les systèmes utilisés et leur impact sur les droits des enfants. L'organisme de contrôle doit également avoir accès à des chercheurs et des experts indépendants.

121. Voir, par exemple, YouTube Data Breach Claim (Réclamation pour violation de données sur YouTube), McCann contre Google, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

Feuille de route pour atteindre l'objectif :

A **Établir ou s'assurer que les cadres de protection des données existants sont efficaces pour fournir une protection spécifique aux données des enfants**

Les droits des enfants dans l'environnement en ligne sont intimement liés à la façon dont leurs données sont recueillies, sauvegardées et utilisées. La loi et la réglementation sur la protection des données liées aux enfants doivent être accessibles, efficaces et capables d'évoluer pour faire face aux risques émergents.[122] Cela signifie non seulement établir les cadres juridiques et réglementaires, mais faire en sorte qu'ils fonctionnent dans la pratique.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Consultez le Code de conception adapté à l'âge[123] du Royaume-Uni , qui constitue le mètre-étalon en matière de protection des données pour les enfants (voir « Autres ressources pour référence 2 »).
2. Considérez le RGPD[124] comme source modèle pour établir une réglementation plus large ou une réglementation contenant des dispositions d'application et des définitions clés.
3. Envisager la nécessité de codes spécialisés ou distincts, par exemple des codes couvrant l'utilisation des données dans les milieux de l'éducation et de la santé, ou des données détenues par les organismes gouvernementaux.
4. S'assurer qu'ils sont couverts par votre plan, tel que développé dans le domaine d'action politique sur le cadre juridique et réglementaire. Voir les outils d'assistance n° 1 (page n° 80).

122. Règlement général sur la protection des données, Union européenne, 2018.
123. Age appropriate design code (Code de conception adapté à l'âge) – Executive summary, Commissaire de l'information du Royaume-Uni, 2020.
124. Règlement général sur la protection des données, Union européenne, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

B **Établir des protocoles et des limites à l'utilisation de la prise de décision automatisée qui peut affecter les enfants.**

Les normes, lois et codes de pratiques devraient veiller à ce que les enfants bénéficient de systèmes automatisés et ne soient pas pénalisés par la prise de décision automatisée.[125] Il est particulièrement important d'éviter le risque de discrimination dans la prise de décision automatisée. Ces protocoles et ces limites peuvent s'appliquer dans le cadre de la justice pénale, la protection sociale, la santé et la médecine, l'enseignement et le secteur privé, entre autres.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de rechercher les législations, les réglementations et les normes techniques internationales récentes en matière de conception, d'audit et de supervision de l'IA dans d'autres juridictions ou organisations régionales ou internationales – par exemple, la loi sur l'intelligence artificielle dans UE[126] – et de les adapter à votre pays.

125. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert (Un expert des droits de l'homme de l'ONU met en garde contre la dérive du monde vers une dystopie de l'aide sociale numérique), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2019.
126. Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union COM/2021/206, EUR-Lex, 2021 ; Global Policy AI, Organisation de coopération et de développement économiques, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

C **Garantir des protections juridiques et réglementaires adéquates concernant les données biométriques des enfants**

Les pouvoirs publics et les organismes de réglementation doivent établir des protocoles juridiques et réglementaires appropriés pour l'utilisation des données biométriques des enfants, ainsi que des limites à cette utilisation, à la lumière des principes des droits de l'enfant, de la limitation des objectifs et des exigences de la politique de protection en ligne des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Voir si les données biométriques sont couvertes par d'autres lois ou réglementations nationales (par exemple, la législation sur les données). Il se peut que certaines lois qui ne mentionnent pas les données biométriques puissent être interprétées de façon à les inclure :[127]

   A. Le cas échéant, assurer une meilleure protection des enfants.

   B. Lorsque rien n'est en place, il conviendra d'élaborer une disposition pour les données biométriques. Elle devra couvrir les données biométriques pour lesquelles le consentement a été donné (par exemple, le déverrouillage d'un téléphone) et celles où le consentement n'est pas donné ou son utilisation n'est pas évidente (par exemple, la reconnaissance faciale dans les systèmes d'entrée à l'école ou l'identification des empreintes digitales pour avoir accès au déjeuner à l'école).

127. Voir par exemple, Chili : les enfants doivent fournir leurs données biométriques pour obtenir leur repas dans les écoles, Privacy International, 2019.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

D **Établir des directives, des lois et des règlements clairs sur les pratiques susceptibles d'affecter la représentation des enfants**

Créer des cadres juridiques qui empêchent le ciblage et le suivi personnalisés des enfants à des fins commerciales sur la base de leurs données personnelles. Établir des codes concernant l'utilisation des systèmes de recommandation et des autres processus ou autre technologie de prise de décision automatisée susceptibles d'orienter le comportement des enfants, de modeler leurs préférences et leurs opinions, de porter atteinte à leur réputation ou de limiter leur expérience.[128]

Dans l'affirmative, veuillez préciser :

Dans la négative, cela permettra de consulter l'évolution récente du droit des données, et d'établir si des réglementations mises en place dans d'autres juridictions, qui garantissent une utilisation équitable du profilage personnel ou limitent les incitations excessives, sont en train de voir le jour. Par exemple, le Code de conception adapté à l'âge (Royaume-Uni),[129], le Règlement général sur la protection des données (RGPD, UE)[130] ou la Loi sur les services numériques (UE)[131] et le Code of Non-broadcast Advertising and Direct & Promotional Marketing (Code de la publicité non radiodiffusée et du marketing direct et promotionnel) (CAP Code, Royaume-Uni).[132]

128. Voir, par exemple, YouTube Data Breach Claim (Réclamation pour violation de données sur YouTube), McCann contre Google, 2021.
129. Age appropriate design code (Code de conception adapté à l'âge), Commissaire de l'information du Royaume-Uni, 2020.
130. Règlement général sur la protection des données, Union européenne, 2018.
131. The Digital Services Act : Ensuring a Safe and Accountable Online Environment, Commission européenne, 2019.
132. The Code of Non-broadcast Advertising and Direct & Promotional Marketing, CAP Code, Royaume-Uni.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

E **Mettre en place une surveillance et un suivi efficaces**

La création d'organes et de systèmes pouvant recueillir des informations relatives à la protection en ligne des enfants et assurer la transparence et l'application effective des droits et de la protection des enfants par les entreprises, les pouvoirs publics et d'autres organismes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. S'assurer qu'il existe une institution ou un ou plusieurs organes habilités à recommander et à faire appliquer la pratique convenue. Par exemple, les directives du National Centre for Missing & Exploited Children.[133]
2. Clarifier ce point dans la stratégie élaborée dans le domaine d'action politique sur les cadres juridiques et réglementaires avec des lignes de responsabilité et de surveillance (page n° 56).

133. Our work, National Centre for Missing and Exploited Children (NCMEC).

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

F **Établir des cadres pour assurer la transparence**

La surveillance doit être assurée par un organisme de réglementation désigné qui dispose de ressources suffisantes et qui dispose des capacités et de l'expertise nécessaires pour comprendre les systèmes utilisés et leur impact sur les droits des enfants. L'organisme de contrôle doit également avoir accès à des chercheurs et des experts indépendants.

Dans l'affirmative, veuillez préciser :

Dans la négative, cela aidera à s'assurer que l'organisme de réglementation choisi est mandaté par la loi, doté de ressources et habilité à gérer cette situation. Par exemple, le Bureau du commissaire à l'information (BCI).[134] L'ICO est l'autorité indépendante du Royaume-Uni créée pour défendre les normes et les droits en matière d'information dans l'intérêt public. Ou l'Autorité nationale de protection des données (ANPD) agissant en vertu de la loi générale brésilienne sur la protection des données.[135]

134. UK Information Commissioner's Office (ICO) (Commissaire de l'information du Royaume-Uni).
135. Autorité nationale de protection des données (ANPD), gouvernement fédéral du Brésil.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

Comment cela concorde avec les documents fondamentaux :

L'adoption de garanties relatives à l'identité numérique est essentielle pour les gouvernements et l'Organisation des Nations Unies, qui s'efforcent d'en réaliser pleinement l'utilité et le potentiel tout en renforçant la confiance dans son utilisation. Cela implique, entre autres, la mise en place d'efforts tels que le stockage décentralisé des données, l'identification et l'authentification, les communications chiffrées et la prise en compte des principes de « protection de la confidentialité dès la conception ».

Source : Feuille de route du Secrétaire général des Nations Unies pour la coopération numérique, juin 2020[136]

Lorsque le consentement est demandé pour traiter les données d'un enfant, les États parties doivent veiller à ce que le consentement soit donné librement et en connaissance de cause par l'enfant ou, selon l'âge de l'enfant et le degré d'évolution de ses capacités, par le parent ou le tuteur, et obtenu avant le traitement desdites données. Lorsque le consentement de l'enfant est jugé insuffisant et que le consentement des parents est requis pour traiter les données personnelles de l'enfant, les États parties doivent exiger des organisations qui traitent ces données qu'elles vérifient que le consentement est éclairé, valable et fourni par le parent ou le tuteur de l'enfant.

Source : Observation générale n° 25 (2021), par. 71[137]

Les États parties doivent veiller à ce que les enfants et leurs parents ou tuteurs puissent accéder facilement aux données stockées, rectifier les données inexactes ou périmées et supprimer les données stockées illégalement ou inutilement par les autorités publiques, les particuliers ou d'autres organismes, sous réserve de limitations raisonnables et légales. Ils doivent en outre garantir le droit des enfants à retirer leur consentement et à s'opposer au traitement des données à caractère personnel lorsque le responsable du traitement n'est pas en mesure d'établir la preuve que le traitement est justifié par des motifs légitimes et impérieux. Ils doivent également fournir des informations aux enfants, aux parents et aux tuteurs sur ces questions, dans un langage adapté aux enfants et dans des formats accessibles.

Source : Observation générale n° 25 (2021), par. 72[138]

136. Feuille de route du Secrétaire général des Nations Unies pour la coopération numérique, Nations Unies, juin 2020.
137. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
138. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

Le processus A (« Établir ou s'assurer que les cadres de protection des données existants sont efficaces pour fournir une protection spécifique aux données des enfants ») nécessite de s'assurer que tous les aspects des données des enfants sont adéquatement protégés, dans la législation et dans la réglementation. Cet outil est conçu pour aider les responsables politiques à réfléchir à l'ampleur des questions que les cadres de protection des données doivent couvrir pour les enfants.

Outils d'assistance :

1. Liste de contrôle pour s'assurer que la législation sur la protection des données pour les enfants est complète

Avez-vous des cadres de protection des données qui couvrent :	
La collecte	
Le stockage	
L'utilisation	
Les données sur l'éducation	
Les données relatives à la santé	
Les données gouvernementales et administratives	
Les données utilisées pour la prise de décision automatisée	
Les données utilisées dans d'autres systèmes d'IA	
Les données biométriques	

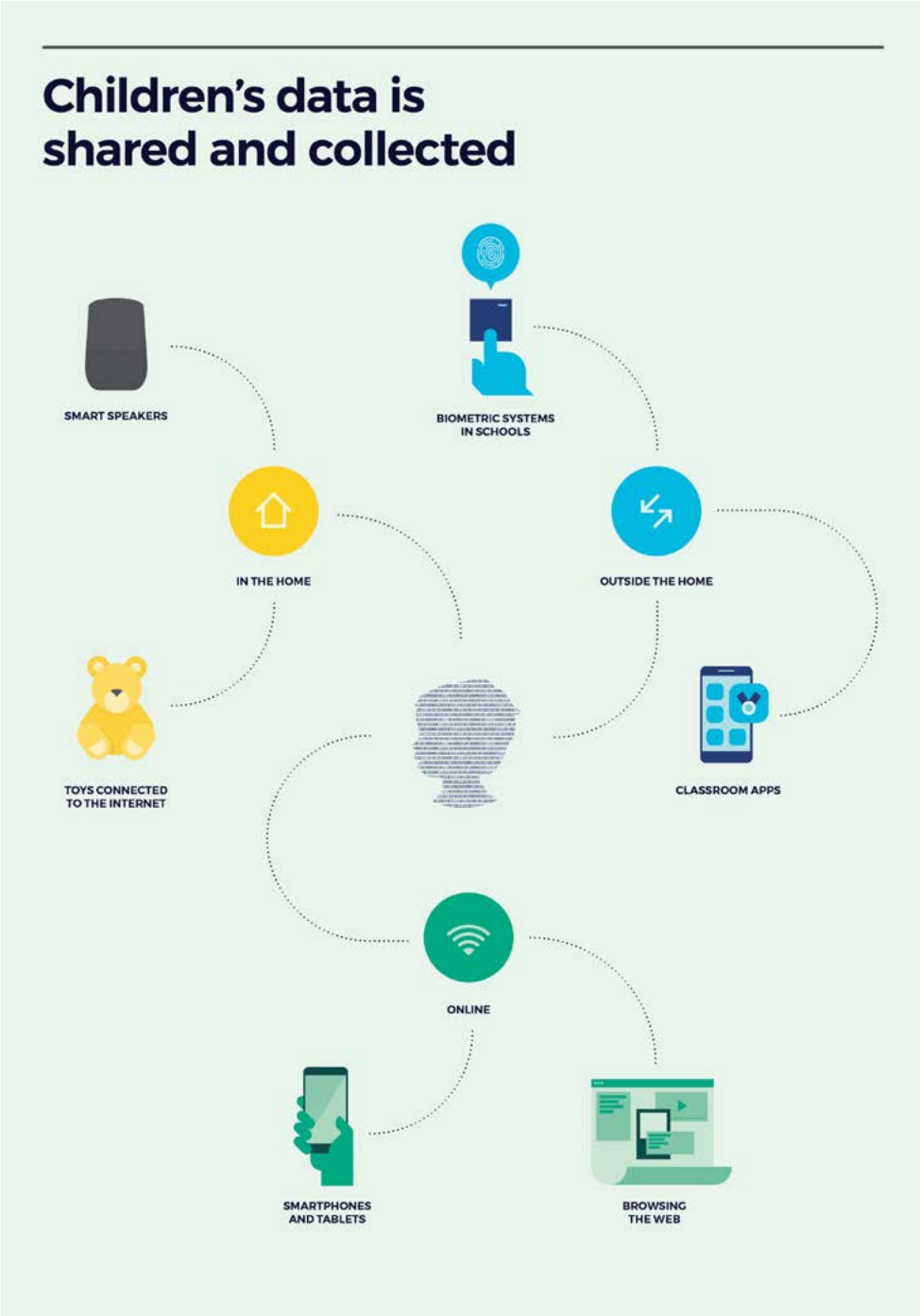
< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

Autres ressources pour référence :

1. Des visuels pour aider à comprendre l'ampleur et le volume des données collectées sur les enfants



Source : infographie du Children's Commissioner « Who knows what about me »[139]

139. Who knows what about me?, Children's Commissioner, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

3 Données personnelles, identité et autonomie

Source : infographie du Children's Commissioner « Who knows what about me »[140]

2. Étude de cas du code de conception adapté à l'âge du Royaume-Uni[141]

Le Royaume-Uni a mis en œuvre un texte législatif novateur qui traite de la manière dont les données sur les enfants peuvent être utilisées, appelé *Age Appropriate Design Code (Code de conception adapté à l'âge)*.

> **« Ce code traite de la manière de concevoir des garanties de protection des données dans les services en ligne, de façon à s'assurer qu'elles sont adaptées à une utilisation par les enfants et répondent à leurs besoins de développement. Il reflète l'inquiétude croissante que suscite la situation des enfants dans la société et dans le monde numérique moderne en particulier. On s'accorde, au niveau international et au Royaume-Uni, pour reconnaître qu'il faut faire beaucoup plus pour créer un espace en ligne sûr, qui garantisse aux enfants de pouvoir apprendre, explorer et jouer. Ce code y parvient, non pas en cherchant à protéger les enfants du monde numérique, mais en les protégeant en son sein. »**

Le code énonce 15 normes de conception adaptées à l'âge, reflétant une approche fondée sur le risque. L'accent est mis sur la fourniture de paramètres par défaut qui garantissent aux enfants le meilleur accès possible aux services en ligne, tout en réduisant la collecte et l'utilisation des données, par défaut. Ces principes sont les suivants :

1. Intérêt supérieur de l'enfant
2. Analyses de l'impact sur la protection des données
3. Application adaptée à l'âge
4. Transparence
5. Utilisation préjudiciable des données
6. Politiques et normes communautaires
7. Paramètres par défaut
8. Minimisation des données
9. Partage de données
10. Géolocalisation
11. Contrôle parental
12. Profilage
13. Techniques d'incitation
14. Jouets et appareils connectés
15. Outils en ligne

140. Who knows what about me?, Children's Commissioner, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

Le code de conception adapté à l'âge est entré en vigueur au Royaume-Uni le 2 septembre 2021. Il est fondé sur le règlement général sur la protection des données (RGPD) à l'échelle de l'UE et est donc susceptible d'être reconnu par les pays ayant adopté des schémas conformes au RGPD. Il est largement considéré comme le régime de protection des données le plus avancé au monde pour les enfants. Depuis sa mise en œuvre, les services ont annoncé une série de changements dans leur engagement auprès des enfants, parmi lesquels :

- Sur Instagram, les adultes ne peuvent pas envoyer de messages aux moins de 18 ans qui ne les suivent pas.
- Google SafeSearch sera activé par défaut pour tous les moins de 18 ans.
- Sur YouTube, la lecture automatique est désactivée pour les moins de 18 ans et les rappels de pause et d'heure de coucher sont activés par défaut.
- Les enfants de moins de 16 ans ne sont pas en mesure d'héberger des diffusions en direct sur TikTok et les notifications push sont désactivées après 21 h.
- Google et Facebook mettront fin à la publicité comportementale destinée aux enfants.

Certains secteurs ou types d'informations peuvent faire l'objet de dispositions supplémentaires, par exemple les données sur la santé, les données financières et les données scolaires. Certains autres domaines exigent l'ajout de codes ou de compléments, mais tous doivent respecter un niveau élevé de confidentialité et fonctionner dans l'intérêt supérieur des enfants.

3. Manifeste de l'UNICEF pour une meilleure gouvernance des données sur les enfants[142]

Le groupe de travail de l'UNICEF sur la gouvernance des données a produit un rapport documentant les motifs et les principes d'une meilleure gouvernance des données relatives aux enfants. Les dix points d'action du manifeste se concentrent sur l'utilisation des données dans l'intérêt supérieur des enfants, le travail avec les enfants eux-mêmes pour comprendre les utilisations bénéfiques, et le comblement du fossé des connaissances entre la technologie et les institutions et les personnes qui l'utilisent.

4. Cadre de confidentialité de l'OCDE[143]

Le Cadre de confidentialité de l'OCDE regroupe les éléments clés du cadre de confidentialité de l'OCDE, sur la base des lignes directrices de confidentialité révisées :

PRINCIPES FONDAMENTAUX D'APPLICATION NATIONALE :

Principe de restriction de la collecte
Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Principe de qualité des données
Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

141. Age appropriate design code (Code de conception adapté à l'âge), Commissaire de l'information du Royaume-Uni, 2020.
142. The Case for Better Governance of Children' s Data : A Manifesto, Bureau de la connaissance et des politiques mondiales de l'UNICEF, 2021.
143. Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel, Organisation de coopération et de développement économiques, 2013.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

Principe de spécification des finalités
Les finalités pour lesquelles les données à caractère personnel sont collectées doivent être précisées au plus tard au moment de la collecte des données et l'utilisation ultérieure limitée à la réalisation de ces finalités ou d'autres qui ne sont pas incompatibles avec ces finalités et qui sont précisées à chaque occasion de changement de finalité.

Principe de limitation d'utilisation
Les données à caractère personnel ne doivent pas être divulguées, mises à disposition ou utilisées d'une autre manière à des fins autres que celles spécifiées dans le paragraphe 9, sauf : a) avec le consentement de la personne concernée ; ou b) par autorité de la loi.

Principe des mesures de sécurité
Les données à caractère personnel doivent être protégées par des mesures de sécurité raisonnables contre les risques tels que la perte ou l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation des données.

Principe d'ouverture
Il doit y avoir une politique générale d'ouverture sur les développements, les pratiques et les politiques en matière de données à caractère personnel. Il doit être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel et les finalités principales de leur utilisation, de même que l'identité du responsable du traitement et le siège habituel de ses activités.

Principe de la participation individuelle
Les individus doivent avoir le droit :

a) d'obtenir auprès d'un responsable du traitement, ou autre, la confirmation que le responsable du traitement possède ou non des données les concernant ;

b) d'exiger que les données les concernant leur soient communiquées

   i. dans un délai raisonnable ;

   ii. à un tarif, le cas échéant, qui ne soit pas excessif ;

   iii. d'une manière raisonnable ; et

   iv. sous une forme qui leur soit aisément compréhensible ;

c) d'obtenir les motifs justificatifs, si une demande faite en vertu des alinéas a) et b) est rejetée, et de pouvoir contester ce refus ;

d) de contester les données les concernant et, si la contestation aboutit, de les faire effacer, rectifier, compléter ou modifier.

Principe de responsabilité
Un responsable du traitement doit être en charge de respecter les mesures qui donnent effet aux principes énoncés ci-dessus.

Principes fondamentaux d'application internationale : libre circulation et restrictions légitimes

- Un responsable du traitement reste en charge des données à caractère personnel sous son contrôle, quel que soit l'emplacement des données.
- Un pays membre doit s'abstenir de restreindre les flux transfrontaliers de données à caractère personnel entre lui-même et un autre pays dès lors (a) que l'autre pays respecte substantiellement les présentes lignes directrices ou (b) qu'il existe des garanties suffisantes, y compris des mécanismes d'application efficaces et des mesures appropriées mises en place par le responsable du traitement, pour assurer un niveau de protection continu compatible avec les présentes lignes directrices.
- Toute restriction aux flux transfrontaliers de données à caractère personnel doit être proportionnée aux risques présentés, et tenir compte de la sensibilité des données, ainsi que de l'objet et du contexte du traitement.

5. **Règlement général sur la protection des données de l'Union européenne (texte et outils)** [144]
   Le Règlement général sur la protection des données (RGPD) est une loi sur la confidentialité et la sécurité autorisée par l'Union européenne. Il exige des entreprises opérant à l'intérieur et à l'extérieur des pays européens qu'elles utilisent les données personnelles des citoyens de l'UE en se conformant à la loi.

6. **Stratégie numérique européenne (y compris propositions sur l'intelligence artificielle et les données)**[145]
   Il s'agit du guide permettant de comprendre comment l'Union européenne façonne son avenir numérique. La stratégie numérique européenne vise à développer un marché unique permettant à toutes les entreprises de fonctionner sur un pied d'égalité, sans violer le droit des consommateurs à la confidentialité, et à façonner une meilleure société numérique dans la région et à l'échelle mondiale.

7. **Fondamentaux du commissaire irlandais à la protection des données pour une approche du traitement des données axée sur l'enfant (The Fundamentals)**[146]
   Élaboré par la Commission irlandaise de protection des données (DPC, Data Protection Commission), The Fundamentals visent à améliorer les normes de traitement des données. Ils servent de guide aux organisations impliquées dans le traitement des données des enfants, avec les principes générés dans le cadre du RGPD.

8. **Mémorandum de l'UNICEF sur l'intelligence artificielle et les droits de l'enfant**[147]
   Le Mémorandum fourni par l'UNICEF décrit les éléments clés sur la façon dont l'IA influence les droits des enfants dans différents domaines, comme la très connue plateforme de visionnage YouTube, les jouets intelligents et l'IA dans l'enseignement. Il formule également des recommandations initiales à l'intention des responsables politiques, des entreprises, des parents et des éducateurs.

9. **Rapport sur les droits fondamentaux de l'Agence des droits fondamentaux de l'UE – Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights**[148]
   Les systèmes informatiques mis en place par l'UE jouent un rôle essentiel dans la sécurité régionale, par exemple dans la gestion des migrations et la lutte contre le terrorisme et les formes graves de criminalité. Toutefois, les incidences de ces systèmes sur les droits fondamentaux n'ont pas encore été étudiées. Par exemple, avec le cadre fourni par la Convention relative aux droits de l'enfant du HCDH à l'article 24, le rapport au chapitre 7 renforce que les systèmes doivent accorder la priorité à l'intérêt supérieur de l'enfant lors de la collecte des éléments d'identification biométrique.

144. Règlement général sur la protection des données, Union européenne, 2018.
145. Façonner l'avenir numérique de l'Europe, Union européenne, 2020.
146. Fundamentals for a Child-Oriented Approach to Data Processing, Commission irlandaise de protection des données, 2020.
147. Intelligence artificielle et droits de l'enfant, Fonds des Nations Unies pour l'enfance, 2019.
148. Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights (Sous haute surveillance : biométrie, systèmes informatiques et droits fondamentaux de l'UE), Agence des droits fondamentaux de l'Union européenne, 2018.

10. Directives de l'UNICEF sur l'IA et les enfants[149]

Bien que les systèmes d'IA aient été largement déployés par les pays, les inquiétudes suscitées par cette nouvelle technologie ont également poussé les gouvernements, les entreprises et la société civile à élaborer des principes à exploiter par le biais de l'éthique. Bien que les droits de l'homme aient été inclus dans ces stratégies d'IA, les droits de l'enfant en particulier n'ont pas encore été suffisamment pris en compte. Dans ces directives, l'UNICEF vise à sensibiliser aux droits de l'enfant et à fournir des recommandations aux différentes parties, principalement les responsables politiques et les chefs d'entreprise, sur les politiques et pratiques d'IA chez les enfants.

Assistants vocaux et robots de messagerie alimentés par l'IA

Les assistants vocaux virtuels et les robots de messagerie utilisent le NLP (Natural Language Processing : traitement du langage naturel), la reconnaissance vocale automatique et l'apprentissage automatique pour reconnaître les commandes verbales, identifier des modèles, récupérer des informations et générer des réponses. Bien que ces systèmes n'aient pas toujours été conçus ou adaptés aux enfants, ils contribuent à façonner des millions d'enfants, sur le plan émotionnel ou sur le plan comportemental. Les partisans de ces technologies avancent des bienfaits tels que l'assistance aux enfants ayant une déficience visuelle ou une mobilité limitée, et décrivent ces systèmes comme de nouvelles façons d'apprendre et de stimuler la curiosité et la créativité des enfants. En outre, certains robots de messagerie visent à rendre l'étude plus facile et plus efficace pour les élèves.

Cependant, l'utilisation de robots de messagerie peut entraîner des risques supplémentaires pour les enfants, en particulier en termes de santé mentale, lorsque les robots ne reconnaissent pas les appels à l'aide ou fournissent des conseils inadéquats. Par exemple, en 2018, le test de deux robots de messagerie de santé mentale par la BBC a révélé que les applications ne traitaient pas correctement les signalements d'abus sexuels des enfants, même si les deux applications avaient été considérées comme adaptées aux enfants. Selon une note d'information de l'UNICEF, « lorsqu'ils ne sont pas conçus avec soin, les robots de messagerie peuvent aggraver la détresse plutôt que de la dissiper », ce qui est « particulièrement risqué dans le cas des jeunes utilisateurs, qui peuvent ne pas avoir la résilience émotionnelle nécessaire pour faire face à une expérience de réponse négative ou déroutante des robots de messagerie ». En outre, les robots de messagerie peuvent poser plusieurs menaces de sécurité, y compris celle de l'usurpation d'identité (le fait qu'un individu se fasse passer pour quelqu'un d'autre), de la falsification de données, du vol de données et de la vulnérabilité aux cyberattaques, et peuvent imposer un biais, étant donné qu'ils sélectionnent souvent une réponse prédéterminée en fonction des mots-clés qui correspondent le plus ou d'un modèle de libellé similaire.

Les technologies de robot de messagerie et d'assistant personnel impliquent également d'autres soucis liés à la confidentialité et à la propriété des données. Par exemple, étant donné que les assistants vocaux comptent généralement sur le stockage des enregistrements vocaux pour faciliter l'apprentissage continu du système, les défenseurs des droits de l'enfant ont soulevé des questions sur le manque de clarté des politiques de conservation des données par les entreprises et du consentement des enfants et des parents.

Reconnaissance faciale pour identification biométrique

Les systèmes de reconnaissance faciale utilisent des techniques de vision par ordinateur et des algorithmes d'apprentissage automatique pour déterminer, traiter et analyser les caractéristiques faciales d'une personne, à des fins très variées, comme la vérification de l'identité d'une personne par rapport à un enregistrement existant. La reconnaissance faciale à des fins d'identification peut être

149. Directives politiques sur l'IA pour les enfants, Fonds des Nations Unies pour l'enfance, 2020.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

utilisée dans la gestion des frontières, l'analyse et la prévention de la criminalité, et la surveillance scolaire, pour des raisons alléguées d'amélioration de la sécurité. La reconnaissance faciale est de plus en plus utilisée comme moyen d '« authentification » d'identité numérique, pour l'identification juridique et fonctionnelle. Bien qu'elle ne remplace pas l'identification légale, qui rend les personnes visibles pour un État et constitue un droit reconnu, cette technologie peut plus rapidement ou plus facilement valider un document d'identité existant.

Les risques et les limites en matière de droits de l'homme et de droits de l'enfant sont considérables. Les défenseurs du droit à la confidentialité ont mis en garde contre son utilisation réelle dans les activités de surveillance de masse par les gouvernements, qui s'en servent comme d'un outil d'enquête pour les forces de l'ordre, en particulier parce qu'elle peut être utilisée pour profiler, suivre et réprimer les communautés vulnérables. Dans certains cas, ces systèmes soulèvent également des questions de consentement éclairé, car les individus peuvent ne pas savoir qui recueille les données biométriques ou même ignorer qu'elles sont recueillies, comment elles sont stockées ou quelles applications peuvent en être faites. En outre, des inexactitudes persistent dans la détection par reconnaissance faciale, notamment des degrés de correspondance moins fiables concernant le visage des enfants et d'autres groupes fondés sur le sexe et l'origine ethnique, notamment les femmes de couleur. En conséquence, l'utilisation de la reconnaissance faciale pourrait venir renforcer les préjugés sociaux existants et conduire à une discrimination ou à une marginalisation accrue des communautés minoritaires.

Source : directives politiques sur l'IA pour les enfants, Fonds des Nations Unies pour l'enfance, 2020[150].

1. **Code de l'enfant : ressources supplémentaires[151]**
   Ce site Web rassemble toutes les ressources supplémentaires du bureau du commissaire à l'information du Royaume-Uni concernant le code de conception adapté à l'âge, y compris une FAQ et un modèle d'évaluation de l'impact sur la protection des données.

2. **5Rights Foundation's Demystifying the Age Appropriate Design Code[152]**
   Il s'agit d'une brochure destinée aux enfants, traitant de l'élaboration du Code de conception adapté à l'âge, au Royaume-Uni.

150. Directives politiques sur l'IA pour les enfants, Fonds des Nations Unies pour l'enfance, 2020.
151. Code de l'enfant : ressources supplémentaires, ICO 2021.
152. Demystifying the Age Appropriate Design Code, 5Rights Foundation, 2020.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

Les États parties doivent fournir aux enfants des informations adaptées à leur âge et adaptées à leurs besoins, dans un langage adapté à leurs besoins, sur leurs droits et sur les mécanismes de plainte et de signalement, les services ainsi que les recours dont ils disposent en cas de violation ou d'abus de leurs droits dans l'environnement numérique. Ces informations doivent également être fournies aux parents, aux aidants et aux professionnels travaillant avec et pour les enfants.

Source : Observation générale n° 25 (2021), par. 49[153]

Capacités 4 Modèle de réponse nationale – Bonnes pratiques en matière d'application de la loi

Pour les pays ne disposant pas actuellement d'une capacité dédiée d'application de la loi sur l'Exploitation et les abus sexuels sur mineur (CSEA, de l'anglais Child Sexual Exploitation and Abuse), l'organisme national d'application de la loi doit identifier ladite capacité et s'engager à la mettre en œuvre.

Pour les pays disposant déjà d'une capacité dédiée d'application de la loi CSEA, mais qui doivent encore développer une approche multipartite, l'inclusion de professionnels de la protection de l'enfance dédiés à collaborer avec les enquêteurs constitue une première étape importante. Les principes directeurs en matière de protection de l'enfance pour l'application de la loi doivent être suivis en permanence lors de la planification et de la conduite d'une enquête CSEA ; ceci permettra de veiller à ce que les besoins et les droits de l'enfant soient toujours considérés comme primordiaux. L'approche multipartite assurera un niveau accru de protection et de soutien à la victime et contribuera à obtenir les meilleurs éléments de preuve de la part de la victime, augmentant ainsi la probabilité de poursuites fructueuses. Il est également souhaitable de partager les meilleures pratiques dans toute la région.

Source : WeProtect Global Alliance Model National Response[154]

Objectif :

Établir un cadre multilatéral coordonné pour lutter contre les risques encourus en ligne par les enfants, en particulier les risques d'exploitation et d'abus (CSEA) : notamment par des mécanismes d'application juridique et réglementaire efficace, par la prévention, par des recours et par l'accès à des conseils d'experts en protection en ligne des enfants.

153. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
154. L'exploitation et les abus sexuels sur mineur (CSEA) désignent le fait qu'un enfant soit forcé ou pressé par autrui à prendre part à des activités sexuelles. Cela peut impliquer un contact physique ou des activités sans contact et peut se produire en ligne ou hors ligne.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

4a. Avis et retrait
Les institutions gouvernementales travailleront avec les experts, les organismes d'application de la loi et l'industrie pour établir et surveiller des protocoles efficaces d'avis et de retrait des contenus illégaux et nocifs. Cela nécessitera, entre autres, l'élaboration de protocoles pour garantir que les fournisseurs de services Internet (FSI) locaux soient autorisés à restreindre l'accès aux hôtes qui ne retirent pas les contenus signalés ou qui enfreignent de manière persistante les lois ou autres exigences réglementaires relatives à la protection en ligne des enfants.

4b. Établir des processus pour la gestion du risque des délinquants en relation avec l'exploitation et les abus sexuels sur mineur
Un système efficace processus multipartite de gestion des délinquants devra être mis en place, élaborant des normes internationales de bonnes pratiques. Les professionnels du maintien de l'ordre et d'autres personnels de la justice pénale seront formés à reconnaître les comportements délictueux et à enquêter dessus. La gestion des risques des délinquants est un élément essentiel de la protection en ligne des enfants, car des personnes individuelles ou des groupes de délinquants peuvent toucher en ligne un grand nombre d'enfants victimes.

4c. Fournir des ressources suffisantes pour le soutien psychosocial des enfants victimes primaires et secondaires et de leurs familles
Les organisations formant des praticiens dans les domaines de la santé mentale, de la psychologie et du travail social qui travaillent avec des enfants vulnérables doivent être tenues d'avoir une compréhension de base des questions de protection en ligne des enfants.[155] La protection en ligne des enfants doit être intégrée dans des systèmes plus larges de sécurité et de protection des enfants, tels que la sauvegarde dans les écoles ou la violence à l'encontre des enfants (VEE).

4d. Mettre en place des cadres de détection et de protection des victimes
Un objectif clé de la prévention du préjudice causé en ligne sera de prendre en compte les besoins des enfants vulnérables et de savoir comment les soutenir de manière optimale. Les centres One Stop font office d'institution de coordination pour les victimes d'abus : ils permettent d'accéder à une série de services essentiels, de l'aide médicale à l'aide juridique, en un lieu centralisé. Ils offrent un cadre pour les procédures de sauvegarde et de protection des enfants, apportent un soutien aux victimes et transmettent rapidement les signalements de crimes en ligne aux autorités compétentes.[156]

4e. Veiller à ce que les cadres pertinents ne criminalisent pas les enfants
Il est important d'établir des cadres appropriés pour gérer les enfants qui peuvent se trouver eux-mêmes en conflit avec la loi dans le contexte de la protection en ligne des enfants, par exemple, dans les cas de cyberharcèlement, de diffusion d'informations malveillantes ou de piratage. Dans la mesure du possible, les enfants devraient être orientés hors du système de justice pénale, et les possibilités de conseil ou de justice réparatrice devraient être privilégiées. Il convient de veiller tout particulièrement à ce que la situation de l'enfant soit parfaitement comprise. Par exemple, le comportement d'un enfant peut être le résultat d'une intimidation, d'une sollicitation sexuelle ou d'une autre forme de coercition.

155. What Works to Prevent Violence Against Women and Girls Evidence Reviews Paper 3: Response mechanisms to prevent violence (Ce qui marche pour prévenir la violence contre les femmes et les filles, Document d'analyse 3 : Mécanismes d'intervention pour prévenir la violence), What Works, 2015. p. 28.
156. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect Global Alliance, 2016.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

Feuille de route pour atteindre l'objectif :

A **Avis et retrait**

Les institutions gouvernementales devront travailler avec les experts, les organismes d'application de la loi et l'industrie pour établir et surveiller des protocoles efficaces d'avis et de retrait des contenus illégaux et nocifs. Cela nécessitera, entre autres, l'élaboration de protocoles pour garantir que les fournisseurs de services Internet (FSI) locaux soient autorisés à restreindre l'accès aux hôtes qui ne retirent pas les contenus signalés ou qui enfreignent de manière persistante les lois ou autres exigences réglementaires relatives à la protection en ligne des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Élaborer et mettre en œuvre des plans pour combler les lacunes en matière de fourniture. Voir les Outils d'assistance 1 (page n° 97).
2. Pensez à consulter les documents fondamentaux fournis dans les documents clés et autres ressources, en particulier le MNR,[157] pour accéder à des conseils (voir Autres ressources pour référence 1).

157. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect Global Alliance, 2016.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

B **Établir des processus pour la gestion du risque des délinquants en relation avec l'exploitation et les abus sexuels sur mineur**

Un système efficace processus multipartite de gestion des délinquants devra être mis en place, élaborant des normes internationales de bonnes pratiques. Les professionnels du maintien de l'ordre et d'autres personnels de la justice pénale seront formés à reconnaître les comportements délictueux et à enquêter dessus. La gestion des risques des délinquants est un élément essentiel de la protection en ligne des enfants, car des personnes individuelles ou des groupes de délinquants peuvent toucher en ligne un grand nombre d'enfants victimes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Recueillir l'expertise existante pour créer une base de connaissances riche, par exemple National Crime Agency (Agence nationale de lutte contre la criminalité)[158] et Europol.[159]
2. Si nécessaire, contactez des experts internationaux ou régionaux pour obtenir de l'aide, comme le National Center for Missing & Exploited Children,[160] Internet Watch Foundation ,[161] INTERPOL[162] et ECPAT.[163]

158. About us, National Crime Agency.
159. About Europol, Europol.
160. Our work, National Center for Missing and Exploited Children.
161. About Us, Internet Watch Foundation (IWF).
162. Who we are, INTERPOL.
163. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

C Fournir des ressources suffisantes pour le soutien psychosocial des enfants victimes primaires et secondaires et de leurs familles

Les organisations formant des praticiens dans les domaines de la santé mentale, de la psychologie et du travail social qui travaillent avec des enfants vulnérables doivent être tenues d'avoir une compréhension de base des questions de protection en ligne des enfants.[164] La protection en ligne des enfants doit être intégrée à des systèmes plus larges de sécurité et de protection des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Établir un renforcement des capacités à long terme dans le domaine de l'exploitation et des abus sexuels des enfants, dans le cadre de votre plan en cours. Voir Outils d'assistance 1 dans le domaine d'action politique sur la formation pour obtenir de l'aide dans l'identification des besoins de formation nécessaires pour accroître ces capacités (page n° 119).

2. Si nécessaire, contacter des experts internationaux ou régionaux pour obtenir de l'aide, comme le National Center for Missing & Exploited Children[165] Internet Watch Foundation,[166] INTERPOL[167] et ECPAT.[168]

164. Les abus sexuels sur mineur (CSA, de l'anglais Child Sexual Abuse) désignent le fait qu'un enfant soit forcé ou pressé par autrui à prendre part à des activités sexuelles. Cela peut impliquer un contact physique ou des activités sans contact et peut se produire en ligne ou hors ligne.
165. Our work, National Center for Missing and Exploited Children.
166. About Us, Internet Watch Foundation (IWF).
167. Who we are, INTERPOL.
168. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

D **Mettre en place des cadres de détection et de protection des victimes**

Un objectif clé de la prévention du préjudice causé en ligne sera de prendre en compte les besoins des enfants vulnérables et de savoir comment les soutenir de manière optimale. Les capacités des centres One Stop seront renforcées pour suivre les procédures de sauvegarde et de protection de l'enfance, apporter un soutien aux victimes, et intensifier rapidement la dénonciation de délits en ligne aux autorités compétentes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Étudier les centres One Stop existants (comme le MNR[169] fourni dans Autres ressources pour référence 1). Par exemple, Police Scotland.[170]
2. Si nécessaire, rechercher l'expertise internationale ou régionale pour établir un réseau des compétences nécessaires, comme le National Center for Missing & Exploited Children,[171] Internet Watch Foundation,[172] INTERPOL[173] et ECPAT.[174]

169. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect, 2016.
170. Internet Safety, Police Scotland.
171. Our work, National Centre for Missing and Exploited Children (NCMEC).
172. About Us, Internet Watch Foundation (IWF).
173. Who we are, INTERPOL.
174. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

E Veiller à ce que les cadres pertinents ne criminalisent pas les enfants

Il est important d'établir des cadres appropriés pour gérer les enfants qui peuvent se trouver eux-mêmes en conflit avec la loi dans le contexte de la protection en ligne des enfants, par exemple, dans les cas de cyberharcèlement, de diffusion d'informations malveillantes ou de piratage. Dans la mesure du possible, les enfants devraient être orientés hors du système de justice pénale, et les possibilités de conseil ou de justice réparatrice devraient être privilégiées. Il convient de veiller tout particulièrement à ce que la situation de l'enfant soit parfaitement comprise. Le comportement d'un enfant peut être le résultat d'une intimidation, d'une sollicitation sexuelle ou d'une autre forme de coercition.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de :

1. Impliquer votre ministère de la justice dans la formulation de la/des loi(s) existante(s).
2. Consulter les principales parties prenantes, y compris les enfants, les jeunes et les parents/aidants, pour modifier ou mettre à jour les lois et les directives réglementaires, le cas échéant.
3. Solliciter les experts des droits de l'enfant pour s'assurer que la réadaptation et la protection des mineurs, plutôt que la punition (sauf dans les cas les plus graves) puissent être réalisées.

Comment cela concorde avec les documents fondamentaux :

Pour les pays qui ne disposent pas actuellement d'une capacité d'application de la loi dédiée à la question de l'exploitation et des abus sexuels sur mineur, l'organisme national chargé de l'application de la loi doit identifier cette capacité et s'engager à la renforcer : ceci implique l'identification d'agents dédiés qui resteront en poste pendant une période minimale (minimum suggéré de deux ans) ; l'attribution d'un lieu approprié pour accueillir ces ressources ; l'acquisition d'équipements essentiels ; la fourniture d'une formation et de techniques spécialisées dans la question de l'exploitation et des abus sexuels sur mineur ; le soutien en matière de santé psychologique et de bien-être pour les agents ; l'élaboration et la fourniture d'une formation de sensibilisation à la question de l'exploitation et des abus sexuels sur mineur pour les entités locales d'application de la loi dans tout le pays. Pour les pays disposant déjà d'une capacité dédiée d'application de la loi CSEA, mais qui doivent encore développer une approche multipartite, l'inclusion de professionnels de la protection de l'enfance dédiés à collaborer avec les enquêteurs constitue une première étape importante. Les principes directeurs en matière de protection de l'enfance pour l'application de la loi doivent être suivis en permanence lors de la planification et de la conduite d'une enquête CSEA ; ceci permettra de veiller à ce que les besoins et les droits de l'enfant soient toujours considérés comme primordiaux. L'approche multipartite assurera un niveau accru de protection et de soutien à la victime et contribuera à obtenir les meilleurs éléments de preuve de la part de la victime, augmentant ainsi la probabilité de poursuites fructueuses. Il est également souhaitable de partager les meilleures pratiques dans toute la région.

Source : WeProtect Global Alliance Model National Response[175]

175. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect, 2016.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Outils d'assistance :

1. Liste de contrôle pour l'élaboration de procédures d'avis et de retrait adéquates

Le processus A (« Avis et retrait ») commence par l'identification des lacunes dans les systèmes d'avis et de retrait. Cette liste de contrôle est conçue pour aider les responsables politiques à identifier les étapes et les exigences nécessaires pour s'assurer que les contenus illégaux et préjudiciables puissent être rapidement supprimés une fois qu'ils sont identifiés.

	Définition légale du contenu illégal, version détaillée	**Exigences légales de suppression du contenu illégal, version détaillée**	**Processus en temps opportun pour supprimer le contenu illégal, version requise (« avis de retrait »)**	**Définition légale du contenu nuisible mais pas illégal, version détaillée**	**Exigences légales de suppression du contenu préjudiciable mais pas illégal, version détaillée**	**Processus en temps opportun pour supprimer le contenu préjudiciable, version requise (« avis de retrait »)**
Fournisseurs de services Internet						
Plateformes de réseaux sociaux						
Plateformes de streaming						
Cloud et autres services d'hébergement						
Autre						

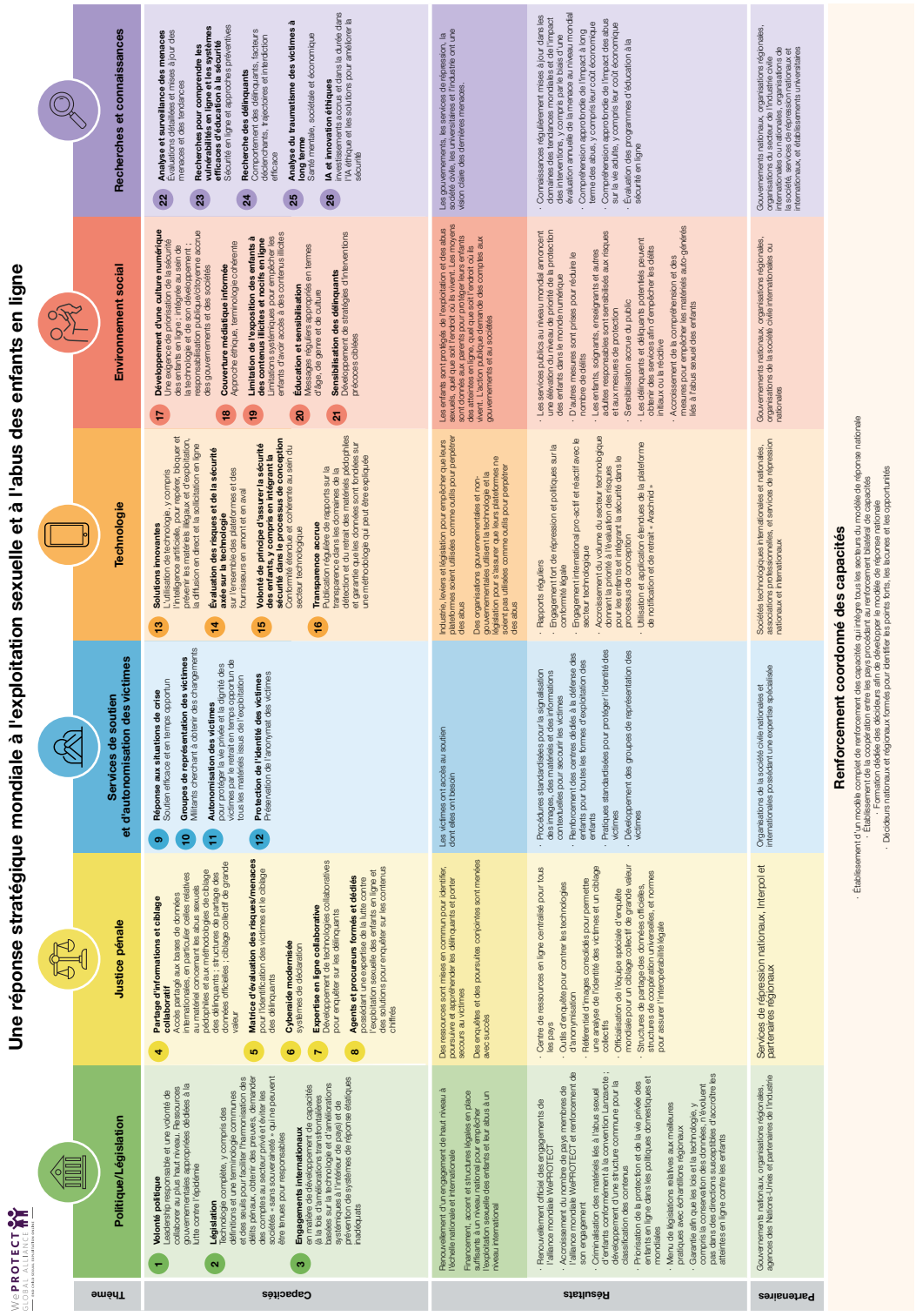
< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

4 Systèmes de réponse et d'assistance

Autres ressources pour référence :

1. Exemples de travail Modèle de réponse nationale de WeProtect Global Alliance[176]



176. Exemples de travail Modèle de réponse nationale, capacités et mise en œuvre, WeProtect, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

2. Australia's Bill for an Online Safety Act (Projet de loi australien sur la protection en ligne)[177]

La loi australienne sur la protection en ligne comprend :

- Des mises à jour de la législation australienne antérieure qui fonctionne bien (en particulier, le *Enhancing Online Safety Act 2015* et son système d'identification des abus basés sur l'image).
- Un ensemble d'attentes de base en matière de protection en ligne pour les services de réseaux sociaux, les services électroniques pertinents et les services Internet désignés, énonçant clairement les attentes de la communauté et décrivant les exigences en matière de signalement obligatoire.
- Un programme amélioré de lutte contre la cyberintimidation pour les enfants australiens, qui réunit un ensemble de services en ligne, pas seulement des plateformes de réseaux sociaux.
- Un nouveau système de lutte contre les abus en ligne, pour les adultes australiens, qui facilite la suppression des abus et du harcèlement en ligne graves.
- Un système de contenu en ligne modernisé, destiné à remplacer les systèmes des annexes 5 et 7 de la Broadcasting Services Act 1992 (BSA) (loi de 1992 sur les services de radiodiffusion). Le projet de loi créera de nouvelles catégories de contenus en ligne préjudiciables et revigorera les codes désuets du secteur pour traiter ces contenus.
- De nouveaux dispositifs de blocage des contenus haineux/violents qui permettent au commissaire à la protection en ligne de réagir rapidement à un événement de crise en ligne, comme les attentats terroristes de Christchurch, en demandant aux fournisseurs de services Internet de bloquer l'accès aux sites hébergeant des contenus gravement préjudiciables.
- Des exigences de retrait cohérentes pour les abus basés sur l'image, les abus en ligne, la cyberintimidation et les contenus en ligne préjudiciables, exigeant des fournisseurs de services Internet qu'ils retirent lesdits contenus dans les 24 heures suivant la réception d'un avis du commissaire à la protection en ligne.

3. Outils d'EndOCSEA@Europe[178]

EndOCSEA a été conçu pour garantir la protection des droits des enfants via une coopération multinationale, interdisciplinaire et intersectorielle efficace et des mesures adaptées aux enfants pour prévenir et combattre l'exploitation et les abus sexuels sur mineur facilités par les TIC (OCSEA) à l'échelle paneuropéenne.

Le projet comprend trois composantes qui se renforcent mutuellement, chacune visant à :

- créer des environnements propices à une collaboration transsectorielle et multidisciplinaire aux niveaux national et régional, en renforçant les structures de gouvernance nationales et en procédant à une analyse de la situation des risques et des réponses de l'OCSEA dans les contextes nationaux et paneuropéens ;
- soutenir les réformes législatives et procédurales, la formation et l'amélioration des capacités des responsables de l'application de la loi, du pouvoir judiciaire et des procureurs, et promouvoir la coopération interinstitutionnelle pluridisciplinaire pour un soutien de bout en bout aux victimes ;
- s'attaquer aux capacités sociétales en mettant l'accent sur la sensibilisation, l'éducation des principaux groupes cibles et l'autonomisation des enfants.

177. Consultation on a Bill for a new Online Safety Act (Consultation sur un projet de loi pour une nouvelle loi sur la protection en ligne), Ministère des infrastructures, des transports, du développement régional et des communications, 2020.
178. Mettre fin à l'exploitation et aux abus sexuels des enfants en ligne, Conseil de l'Europe, 2020.

4. **Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest)**[179]
   Il s'agit d'un traité de l'UE sur les infractions commises via Internet et d'autres réseaux informatiques, qui traite en particulier des violations du droit d'auteur, des fraudes informatiques, du matériel concernant l'abus sexuel sur mineur et des violations de la sécurité des réseaux. Il fixe également une série de compétences et de procédures telles que la fouille des réseaux informatiques et l'interception.

5. **Directives de la ligne d'assistance téléphonique INHOPE**[180]
   La mission d'INHOPE est de soutenir le réseau de lignes d'assistance téléphonique de lutte contre le matériel concernant les abus sexuel sur mineur en ligne. INHOPE est composée de plusieurs lignes d'assistance téléphonique à travers le monde, qui opèrent dans tous les États membres de l'UE, en Russie, en Afrique du Sud, en Amérique du Nord et du Sud, en Asie, en Australie et en Nouvelle-Zélande. INHOPE soutient les lignes d'assistance téléphonique et leurs organisations partenaires par la formation, le partage des meilleures pratiques, l'assurance qualité et le bien-être du personnel.

6. **Ressources de l'UNICEF et de la GSMA sur l'avis et le retrait**[181]
   Il s'agit d'un guide à l'attention des fournisseurs de services Internet, sur les politiques et procédures d'avis et de retrait, visant à empêcher l'utilisation abusive de leurs services pour partager du matériel concernant l'abus sexuel sur mineur.

7. **R;pple Suicide Prevention**[182]
   R;pple Suicide Prevention est un outil de surveillance en ligne conçu pour présenter une page visuelle sur l'appareil d'un utilisateur dès que celui-ci est identifié comme recherchant un mot-clé ou une phrase préjudiciable, tel qu'indiqué dans la configuration de l'outil de surveillance R;pple. Les mots-clés et les phrases comprennent tous les mots ou tous les termes qui ont été identifiés comme étant liés à un contenu en ligne potentiellement préjudiciable.

8. **Étude de cas sur l'approche de l'Albanie en matière de soutien aux survivants**[183]
   Le concept de soutien de bout en bout est bien établi dans cette étude de cas. Un processus immédiat de conseil psychosocial est mis en place pour les enfants qui signalent des cas de violence en ligne via la ligne d'assistance téléphonique nationale albanaise pour les enfants, ALO 116 111, et il existe une procédure d'orientation vers les autorités compétentes, de sorte qu'en 2019, tous les enfants ayant fait un signalement et ayant besoin d'aide ont été orientés. Des investissements importants dans le renforcement des capacités du personnel de protection sociale ont permis de réviser le programme de travail social et d'intégrer le signalement et la réponse à la violence en ligne à l'égard des enfants au programme permanent de formation continue de l'École albanaise d'administration publique.

9. **Plan d'action national du Cambodge pour prévenir et combattre l'exploitation sexuelle en ligne des enfants 2021-2025**[184]
   Ce plan a été élaboré par le Groupe de travail technique sur l'exploitation sexuelle en ligne des enfants, composé de 11 ministères, de l'UNICEF et de diverses ONG. Reconnaissant le lien entre l'exploitation et les abus sexuels des enfants en ligne et hors ligne, ce plan d'action s'inscrit dans le cadre plus large du Plan d'action pour prévenir et combattre la violence à l'encontre des enfants 2017-2021, ainsi que du prochain cycle qui débutera en 2022.

179. Convention de Budapest, Conseil de l'Europe, 2021.
180. Our Story, INHOPE, 2021.
181. Company policies and practices to remove online child sexual abuse material (Politiques et pratiques des entreprises en matière de retrait de matériel concernant l'abus sexuel sur mineur en ligne), Fonds des Nations Unies pour l'enfance et GSMA, 2016.
182. R;pple Suicide Prevention, R;pple, 2021.
183. Programming for children's protection online in Albania: A Promising Practice (Programmation pour la protection des enfants en ligne en Albanie : une pratique prometteuse), Fonds des Nations Unies pour l'enfance, 2020.
184. Lancement officiel du Plan d'action national pour prévenir et combattre l'exploitation sexuelle en ligne des enfants au Cambodge 2021-2025.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

10. **Internet Watch Foundation (IWF)**[185]
    IWF recherche, bloque, supprime et prévient les images d'abus sexuels d'enfants en ligne. L'entité utilise ses données uniques et fiables pour rechercher les nouvelles tendances, tactiques et méthodes utilisées par les auteurs d'infractions en ligne. Elle canalise cette expertise pour développer des services de pointe, afin d'aider la communauté technologique à prévenir, interrompre et supprimer les images d'abus sexuels d'enfants en ligne à l'échelle mondiale.

11. **Unité de lutte contre la pédocriminalité d'Interpol**[186]
    INTERPOL veille à lutter contre les actes de criminalité envers les enfants qui ont une dimension internationale. Pour aider à retrouver les enfants disparus, Interpol publie des Notices Jaunes, et ses experts de la traite des êtres humains travaillent aux côtés des pays membres pour secourir les enfants victimes de la traite et du travail forcé. L'unité bloque également l'accès au matériel concernant l'abus sexuel sur mineur.

185. About Us, Internet Watch Foundation.
186. Who We Are, INTERPOL.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

« Oui, mes parents me soutiennent pour que je puisse être détendu du point de vue psychologique, et que je puisse m'exprimer...dans la communauté, mais d'une manière respectueuse. »

– Enfant vivant au Liban, 16 ans

« Être en mesure de s'exprimer [en ligne] est un élément important pour avoir une identité. »

– Enfant vivant en Nouvelle-Zélande, 17 ans

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

5 Responsabilité de l'entreprise

Le secteur des entreprises, y compris les organisations à but non lucratif, a une incidence directe et indirecte sur les droits de l'enfant, dans la fourniture de services et de produits liés à l'environnement numérique. Les entreprises doivent respecter les droits de l'enfant et prévenir et réparer les abus de leurs droits en relation avec l'environnement numérique. Les États parties ont l'obligation de veiller à ce que les entreprises s'acquittent de ces responsabilités.

Les États parties doivent prendre des mesures, notamment par l'élaboration, le suivi, la mise en œuvre et l'évaluation de lois, de règlements et de politiques, pour faire en sorte que les entreprises s'acquittent de l'obligation qui leur incombe d'empêcher que leurs réseaux ou services en ligne ne soient utilisés pour attenter aux droits de l'enfant, y compris du droit à la confidentialité et à la protection, ou y contribuer, et pour offrir aux enfants, aux parents et aux personnes qui s'occupent d'eux des recours rapides et efficaces. Ils doivent également encourager les entreprises à fournir des informations publiques et des conseils accessibles et opportuns qui visent à renforcer la sécurité et les bienfaits des activités numériques des enfants.

Les États parties ont le devoir de protéger les enfants contre les violations de leurs droits par les entreprises, y compris le droit d'être protégés contre toutes les formes de violence dans l'environnement numérique. Bien que les entreprises ne soient pas directement impliquées dans la perpétration d'actes préjudiciables, elles peuvent causer ou contribuer à des violations du droit de l'enfant à être protégé de la violence, y compris par la conception et l'exploitation de services numériques. Les États parties devront mettre en place, surveiller et appliquer des lois et des règlements visant à prévenir les violations du droit à la protection contre la violence, ainsi que des lois et des règlements visant à enquêter, à statuer et à réparer les violations qui se produisent dans l'environnement numérique.

Les États parties devront exiger du secteur privé qu'il fasse preuve de diligence raisonnable en matière de droits de l'enfant, en particulier qu'il réalise des évaluations d'impact sur les droits de l'enfant et qu'il les rende publiques, en accordant une attention particulière aux impacts différenciés et, parfois, graves de l'environnement numérique sur les enfants. Ils devront prendre des mesures appropriées pour prévenir, surveiller, enquêter sur et punir les violations des droits de l'enfant par le secteur privé.

Outre l'élaboration de lois et de politiques, les États parties devront exiger de toutes les entreprises qui ont une incidence sur les droits de l'enfant en relation avec l'environnement numérique qu'elles mettent en œuvre des cadres réglementaires, des codes sectoriels et des conditions de service respectant les normes les plus élevées en matière d'éthique, de respect de la vie privée et de sécurité en ce qui concerne la conception, l'ingénierie, le développement, le fonctionnement, la distribution et la commercialisation de leurs produits et services. Cela inclut les entreprises qui ciblent les enfants, qui comptent des enfants parmi leurs utilisateurs finaux ou qui sont en contact avec les enfants de toute autre manière. Ils devront exiger de telles entreprises qu'elles maintiennent des normes élevées de transparence et de responsabilité et les encourager à prendre des mesures pour innover dans les meilleurs intérêts de l'enfant. Ils devront également exiger la fourniture d'explications adaptées à l'âge des enfants, ou des parents et des personnes en charge de très jeunes enfants, sur leurs conditions de service.

Source : Observation générale n° 25 (2021), par. 35 à 39[187].

187. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5 Responsabilité de l'entreprise

Objectif :

Promouvoir une conception axée sur l'enfant, des normes minimales, des accords sectoriels, l'adoption des meilleures pratiques, la sensibilisation culturelle et le renforcement de la protection en ligne des enfants par le biais de la réglementation et des cadres liés à la responsabilité de l'entreprise.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

5a. Mettre en œuvre la sécurité, les droits et l'éthique dès le stade de la conception
Des normes et des codes de pratique devront être élaborés pour exiger des concepteurs de produits, des fabricants et des fournisseurs de services qu'ils respectent les droits des enfants et contribuent à la sûreté et à la protection en ligne des enfants. Les conditions générales devront refléter l'intérêt supérieur de l'enfant. Entre autres, les normes et les codes de pratiques auront pour objectif d'empêcher qu'on propose aux enfants du contenu ou des contacts nocifs ou inappropriés ; de protéger la vie privée en ligne des enfants dans le système ou au niveau du périphérique ; de répondre aux préoccupations de sécurité soulevées par l'Internet des objets, les jouets et les services liés à la fonction de streaming, afin de garantir que les entreprises privées ont envisagé, par le biais d'une évaluation de l'impact sur les enfants, un processus de réduction des risques et d'atténuation des effets qui conduit à proposer aux enfants un service adapté à leur âge.

5b. Adopter des normes minimales[188]
L'industrie a la responsabilité de veiller à ce que les enfants bénéficient d'une protection en ligne. Cela oblige à créer un espace en ligne sûr et accessible aux enfants, et pas seulement à empêcher l'accès à des contenus nocifs. Les entreprises seront tenues de montrer quelles procédures et considérations spéciales elles ont adoptées pour assurer la sécurité et le respect des droits des enfants (en utilisant le cadre de risque 4C[189]) lorsqu'elles élaborent et établissent leurs services en ligne.[190] Un code doit être créé par le ministère ou l'organisme responsable et supervisé par le Comité directeur. Ces normes seront obligatoires et exécutoires.

5c. Application d'une classification par tranche d'âge
L'application de la classification cohérente par âge des contenus commerciaux, des médias de service public, des jeux et des activités en ligne propose une approche transparente et efficace pour gérer le contenu et les services qui ont un impact sur les enfants. Une telle démarche peut être nécessaire pour les biens et les services concernés et pour le contenu adapté aux différentes tranches d'âge. Un système de vérification de l'âge ou la création d'espaces réservés aux adultes seront nécessaires pour des contenus interdits ou des activités qui ne conviennent pas aux enfants. Cela peut inclure notamment des filtres de contenu pour bloquer les contenus indésirables.[191]

5d. Mettre en place des systèmes de modération et de notifications
Des mécanismes permettant d'identifier des contenus choquants ou inappropriés seront requis de la part des fournisseurs de services, et des systèmes de contrôle transparents et robustes doivent être mis en place pour tous les services en ligne, y compris des mécanismes de retrait. Une ligne d'assistance téléphonique publique gratuite sera disponible pour les notifications et l'accès à un soutien et des conseils spécialisés. Les mécanismes de notification doivent être aisément accessibles aux enfants. Des systèmes de signalement devront être envisagés comme outil supplémentaire. ▶

188. Voir, par exemple, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes volontaires visant à lutter contre l'exploitation et les abus sexuels sur mineur en ligne), GOV.UK, 2020.
189. Voir la section sur les risques et les dommages.
190. Children's Rights In Impact Assessments (Les droits de l'enfant dans les évaluations d'impact), Fonds des Nations Unies pour l'enfance, 2013.
191. But how do they know it is a child? (Mais comment savent-ils que c'est un enfant ?), 5Rights Foundation, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5 Responsabilité de l'entreprise

5e. Assurer la protection des enfants contre les pressions commerciales
Les efforts déployés pour protéger les enfants contre les pressions commerciales comprennent : la promotion d'une conception appropriée à l'âge ; la désactivation de la publicité ciblée et du partage avec des tiers ; la sensibilisation au contexte dans lequel les enfants grandissent. Les produits et les services qui renforcent les droits et la protection en ligne des enfants peuvent être certifiés, et des mesures peuvent être prises contre les créateurs de produits et de services qui ne respectent pas ces valeurs.

5f. Veiller à ce que les principes de conception axée sur l'enfant soient appliqués pour réduire au minimum les risques liés à la protection en ligne des enfants
Cette démarche inclut, par exemple, la possibilité de mettre des adultes étrangers en contact avec des enfants, la publicité ciblée pour les jeux de hasard ou encore la recommandation de contenus nocifs. La protection en ligne des enfants doit être intégrée au stade de la conception pour éviter que des problèmes ne surgissent plus tard.

Feuille de route pour atteindre l'objectif :

A **Mettre en œuvre la sécurité, les droits et l'éthique dès le stade de la conception**

Des normes et des codes de pratique devront être élaborés pour exiger des concepteurs de produits, des fabricants et des fournisseurs de services qu'ils respectent les droits de l'enfant et contribuent à la sûreté et à la protection en ligne des enfants. Les conditions générales devront refléter l'intérêt supérieur de l'enfant. Entre autres, les normes et les codes de pratiques auront pour objectif d'empêcher qu'on propose aux enfants du contenu ou des contacts nocifs ou inappropriés ; de protéger la vie privée en ligne des enfants dans le système ou au niveau du périphérique ; de répondre aux préoccupations de sécurité soulevées par l'Internet des objets, les jouets et les services liés à la fonction de streaming, afin de garantir que les entreprises privées ont envisagé, par le biais d'une évaluation de l'impact sur les enfants, un processus de réduction des risques et d'atténuation des effets qui conduit à proposer aux enfants un service adapté à leur âge.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les possibilités réglementaires ou légales de mettre en place un code de conduite de conception sécuritaire.
2. Trouver une autorité ou un organisme de réglementation disposant des ressources et de l'expertise nécessaires pour assurer la conformité et la mise en œuvre le cas échéant.
3. Développer un cadre de sécurité/droits par la conception. Il existe de nombreux exemples de ce type, par exemple Safety by Design (La conception sécuritaire),[192] dont on peut s'inspirer ou prendre exemple.
4. Veiller à ce que toutes les parties prenantes soient conscientes des processus (tant technologiques que de gouvernance) nécessaires à la mise en œuvre du cadre.
5. Entreprendre un examen régulier du paysage des préjudices émergents et de l'efficacité des cadres pour s'assurer qu'ils suivent le rythme de l'innovation et des pratiques commerciales.

192. Safety by Design, eSafety Commissioner, 2018.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5 Responsabilité de l'entreprise

B **Adoption de normes minimales**[193]

L'industrie a la responsabilité de veiller à ce que les enfants bénéficient d'une protection en ligne. Cela oblige à créer un espace en ligne sûr et accessible aux enfants, et pas seulement à empêcher l'accès à des contenus nocifs. Les entreprises seront tenues de montrer quelles procédures et considérations spéciales elles ont adoptées pour assurer la sécurité et le respect des droits des enfants (en utilisant le cadre de risque 4C[194]) lorsqu'elles élaborent et établissent leurs services en ligne.[195] Un code doit être créé par le ministère ou l'organisme responsable, supervisé par le Comité directeur. Ces normes seront obligatoires et exécutoires.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Introduire des normes minimales dans les domaines couverts par le cadre ci-dessus. Identifier les modèles pertinents[196] d'autres pays ou régions.
2. Vérifier que les normes minimales couvrent les domaines suivants : vérification de l'âge, modération, conditions ou règles de la communauté, prise de décision automatisée et publicité. Voir l'outil d'assistance n° 1 (page n° 109).

193. Voir, par exemple, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes volontaires visant à lutter contre l'exploitation et les abus sexuels sur mineur en ligne), GOV.UK, 2020.
194. Voir la section sur les risques et les dommages.
195. Children's Rights In Impact Assessments (Les droits de l'enfant dans les évaluations d'impact), Fonds des Nations Unies pour l'enfance, 2013.
196. Voir par exemple Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes volontaires visant à lutter contre l'exploitation et les abus sexuels sur mineur en ligne), GOV.UK, 2020.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5 Responsabilité de l'entreprise

C Application d'une classification par tranche d'âge

L'application de la classification cohérente par âge des contenus commerciaux, des médias de service public, des jeux et des activités en ligne propose une approche transparente et efficace pour gérer le contenu et les services qui ont un impact sur les enfants. Une telle démarche peut être nécessaire, pour les biens et les services concernés, pour le contenu adapté aux différentes tranches d'âge. Un système de vérification de l'âge ou la création d'espaces réservés aux adultes seront nécessaires pour des contenus interdits ou des activités qui ne conviennent pas aux enfants. Cela peut inclure notamment des filtres de contenu pour bloquer les contenus indésirables.[197]

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Trouver un service de classification par âge approprié. De nombreux pays ont déjà mis en place une classification par âge pour les films commerciaux[198] ou les jouets et il est possible d'utiliser ces mêmes critères pour le matériel et les activités en ligne.
2. Étendre l'obligation de classer par âge les contenus et les activités aux espaces numériques, y compris les applications.
3. Veiller à ce qu'un organisme approprié supervise les litiges et les manquements.

D Mettre en place des systèmes de modération et de notification

Des mécanismes permettant d'identifier des contenus choquants ou inappropriés seront requis de la part des fournisseurs de services, et des systèmes de contrôle transparents et robustes doivent être mis en place pour tous les services en ligne, y compris des mécanismes de retrait. Une ligne d'assistance téléphonique publique gratuite sera disponible pour les notifications et l'accès à un soutien et des conseils spécialisés. Les mécanismes de notification doivent être aisément accessibles aux enfants. Des systèmes de signalement devront être envisagés comme outil supplémentaire.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Établir des normes minimales, comme indiqué dans le processus A.
2. Déterminer quel organisme sera responsable d'une ligne d'assistance téléphonique publique.
3. Consulter des experts pour s'assurer que les mécanismes seront accessibles aux enfants.

197. But how do they know it is a child? (Mais comment savent-ils que c'est un enfant ?), 5Rights Foundation, 2021.
198. Voir par exemple le British Board of Film Classification.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5 Responsabilité de l'entreprise

E **Assurer la protection des enfants contre les pressions commerciales**

Les efforts déployés pour protéger les enfants contre les pressions commerciales comprennent : la promotion d'une conception appropriée à l'âge ; la désactivation de la publicité ciblée et du partage avec des tiers ; la sensibilisation au contexte dans lequel les enfants grandissent. Les produits et les services qui renforcent les droits et la protection en ligne des enfants peuvent être certifiés, et des mesures peuvent être prises contre les fournisseurs de produits et de services qui ne respectent pas ces valeurs.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les lois et réglementations existantes relatives à l'engagement commercial avec les enfants : la protection de l'enfance, le droit de la consommation et les droits de l'enfant ont tous des restrictions sur la manière dont on peut être en contact commercial avec les enfants, tout comme des secteurs particuliers tels que la santé ou l'enseignement.
2. Harmoniser les orientations afin qu'elles s'étendent explicitement aux produits et services numériques.

F **Veiller à ce que les principes de conception axée sur l'enfant soient appliqués pour réduire au minimum les risques liés à la protection en ligne des enfants**

Cette démarche inclut, par exemple, la possibilité de mettre des adultes étrangers en contact avec des enfants, la publicité ciblée pour les jeux de hasard ou encore la recommandation de contenus nocifs. La protection en ligne des enfants doit être intégrée au stade de la conception pour éviter que des problèmes ne surgissent plus tard.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

Envisager des normes de conception sécuritaire[199] dans des domaines spécifiques qui touchent les enfants de manière non intentionnelle, tels que les jeux de hasard pour adultes, les services financiers, la pornographie ou d'autres endroits que les enfants ne sont pas censés visiter en ligne.

199. Mais comment savent-ils que c'est un enfant ? 5Rights Foundation, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

5 Responsabilité de l'entreprise

Comment cela concorde avec les documents fondamentaux :

Fonctions générales de réglementation et de politique de l'État

Pour remplir leur obligation de protéger, les États sont tenus :

a) D'appliquer des lois tendant à exiger des entreprises qu'elles respectent les droits de l'homme, ou qui ont cet effet, et, périodiquement, d'évaluer la validité de ces lois et de combler les éventuelles lacunes ;

b) De faire en sorte que les autres lois et politiques régissant la création et l'exploitation courante des entreprises, comme le droit des sociétés, n'entravent pas mais favorisent le respect des droits de l'homme par ces entités ;

c) De fournir des orientations effectives aux entreprises sur la manière de respecter les droits de l'homme dans toutes leurs activités ;

d) D'inciter les entreprises à faire connaître la façon dont elles gèrent les incidences de leur activité sur les droits de l'homme, et de les y contraindre, le cas échéant.

Source : Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, 2011, section 3[200]

Les États parties doivent faire des meilleurs intérêts de l'enfant une priorité lorsqu'ils réglementent la publicité et le marketing destinés et accessibles à ces derniers. Le parrainage, le placement de produits et toutes les autres formes de contenu à caractère commercial doivent être clairement distingués de tout autre contenu et ne doivent pas perpétuer les stéréotypes sexistes ou raciaux.

Observation générale n° 25 (2021), par. 41[201]

Les États parties devront interdire par la loi le profilage ou le ciblage d'enfants de tout âge à des fins commerciales sur la base d'un enregistrement numérique de leurs caractéristiques réelles ou déduites, y compris les données de groupe ou collectives, le ciblage par association ou le profilage par affinité. Les pratiques qui s'appuient sur le neuromarketing, les analyses émotionnelles, la publicité immersive et la publicité dans des environnements de réalité virtuelle et augmentée pour promouvoir des produits, des applications et des services doivent également être interdites de tout engagement direct ou indirect impliquant des enfants.

Source : Observation générale n° 25 (2021), par. 42[202].

Outils d'assistance :

1. Étapes pour concevoir des produits et services numériques en tenant compte des droits de l'enfant

5Rights Foundation et l'Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) ont créé une norme qui présente des étapes pratiques que les entreprises sont en mesure de suivre pour concevoir des produits et services numériques adaptés à l'âge des utilisateurs. Elle introduit une série de processus permettant aux entreprises de mettre les besoins des jeunes au cœur de la conception.

200. Principes directeurs relatifs aux entreprises et aux droits de l'homme, Bureau du Haut Commissariat des Nations Unies aux droits de l'homme 2011.
201. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
202. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

5 Responsabilité de l'entreprise

Autres ressources pour référence :

1. Un exemple de la réflexion des jeunes sur la responsabilité de l'entreprise

Les jeunes avec qui 5Rights s'est entretenu attendaient ce qui suit de la part des entreprises :

- Des règles communautaires cohérentes sur toutes les plateformes
- Des délais précis pour les notifications
- Pouvoir informer les victimes de ce qui est arrivé à leur harceleur
- Une meilleure classification du contenu
- Des moyens faciles de retirer du contenu
- L'interdiction de diffuser des abus
- Des fenêtres pop-up qui signalent les bons comportements et encouragent l'utilisation de paramètres de confidentialité élevés
- Un système de traitement des plaintes clairement défini
- Des politiques rédigées en langage clair

2. Orientations des principes des Nations Unies relatifs aux droits de l'enfant et aux entreprises concernant la responsabilité du secteur privé[203]

Le secteur privé a également des responsabilités en matière de protection en ligne des enfants, ce qui doit être précisé dans les domaines politiques pertinents. Certains domaines, tels que le cyberharcèlement, l'exploitation et les abus sexuels sur mineur, la fraude financière, etc., disposent de cadres spécifiques pour renforcer la protection en ligne des enfants, mais il existe également des cadres généraux pour la responsabilité de l'entreprise.

Les principes sur les droits de l'enfant et les entreprises appellent toutes les sociétés à :

- ☐ Assumer leur responsabilité de respecter les droits de l'enfant et s'engager à soutenir les droits fondamentaux des enfants.
- ☐ Contribuer à éradiquer le travail des enfants, y compris dans toutes les activités et relations commerciales des entreprises.
- ☐ Offrir un travail décent aux jeunes travailleurs, aux parents et aux soignants.
- ☐ Assurer la protection et la sécurité des enfants dans toutes les activités et installations de l'entreprise.
- ☐ Veiller à ce que les produits et services soient sûrs, et chercher à soutenir les droits des enfants à travers ces derniers.
- ☐ Utiliser un marketing et une publicité qui respectent et défendent les droits de l'enfant.
- ☐ Respecter et soutenir les droits des enfants en matière d'environnement ainsi que d'acquisition et d'utilisation des terres.
- ☐ Respecter et défendre les droits des enfants dans les dispositifs de sécurité.
- ☐ Aider à protéger les enfants touchés par les situations d'urgence.
- ☐ Renforcer les efforts de la communauté et des pouvoirs publics pour protéger et appliquer les droits des enfants.

203. Obligations et actions sur les droits de l'enfant et les entreprises, Commission internationale des juristes et Fonds des Nations Unies pour l'enfance, 2015.

3. **Observation générale n° 16 (2013) sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant**[204]
   Il s'agit des orientations du Comité des droits de l'enfant des Nations Unies concernant les obligations des États en matière d'impact des activités et opérations commerciales sur les droits de l'enfant.

4. **Présentation des droits de l'enfant et des entreprises**[205]
   Il s'agit d'une version facile à lire de l'observation générale n° 16 (2013) du Comité des droits de l'enfant sur les obligations des États concernant l'impact du secteur des entreprises sur les droits de l'enfant.

5. **Principes directeurs relatifs aux droits de l'enfant et aux entreprises**[206]
   Développé par l'UNICEF, le Pacte Mondial des Nations Unies et Save the Children, il s'agit d'un ensemble complet de principes destinés à guider les entreprises sur l'ensemble des actions qu'elles peuvent entreprendre sur le lieu de travail, sur le marché et dans la communauté pour respecter et défendre les droits de l'enfant.

6. **Obligations et actions sur les droits de l'enfant et les entreprises**[207]
   Il s'agit d'un guide pratique destiné aux États sur la manière de mettre en œuvre l'observation générale n° 16 (2013) du Comité des droits de l'enfant des Nations Unies.

7. **IEEE 2089-2021 Standard for Age-Appropriate Digital Services Framework (Norme pour un cadre de services numériques adaptés à l'âge)**[208]
   5Rights Foundation et l'Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) ont créé une norme qui présente des étapes pratiques que les entreprises sont en mesure de suivre pour concevoir des produits et services numériques adaptés à l'âge des utilisateurs.

8. **UNICEF Guide to Using the Child Online Safety Assessment Tool – Empowering technology companies to promote a safe online environment for children (Guide de l'UNICEF pour l'utilisation de l'outil d'évaluation de la protection en ligne des enfants : donner aux entreprises technologiques les moyens de promouvoir un environnement en ligne sûr pour les enfants)**[209]
   Ce sont les conseils de l'UNICEF sur l'utilisation de leur outil d'évaluation de la protection en ligne des enfants, pour aider les entreprises à préparer et à réaliser une évaluation de leurs impacts sur les enfants. Ce guide décrit l'objectif, le contexte et les fonctions de l'outil d'évaluation de la protection en ligne des enfants, et propose des instructions et des conseils détaillés sur la manière de l'utiliser.

9. **Child Safety Online – A Practical Guide for Providers of Social Media and Interactive Services (protection en ligne des enfants : guide pratique pour les fournisseurs de médias sociaux et de services interactifs)**[210]
   Il s'agit du guide du gouvernement britannique à l'attention des fournisseurs de réseaux sociaux afin de rendre leurs plateformes plus sûres pour les utilisateurs. Il s'appuie sur le cadre de sécurité de l'ICT Coalition for Children Online – a European industry initiative (ICT Coalition pour les enfants en ligne, une initiative de l'industrie européenne).

204. Observation générale n° 16 (2013) sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant, Convention des Nations Unies relative aux droits de l'enfant, 2013.
205. Présentation des droits de l'enfant et des entreprises, Fonds des Nations Unies pour l'enfance et Save the Children, 2015.
206. Droits de l'enfant et principes régissant les entreprises, Fonds des Nations Unies pour l'enfance, Pacte mondial des Nations Unies et Save the Children, 2013.
207. Obligations et actions sur les droits de l'enfant et les entreprises, Commission internationale des juristes et Fonds des Nations Unies pour l'enfance, 2015.
208. IEEE 2089-2021 Standard for Age-Appropriate Digital Services Framework (Norme pour un cadre de services numériques adaptés à l'âge), IEEE SA, 2021.
209. Guide to Using the Child Online Safety Assessment Tool (Guide pour l'utilisation de l'outil d'évaluation de la protection en ligne des enfants), Fonds des Nations Unies pour l'enfance, 2016.
210. Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services (protection en ligne des enfants : guide pratique pour les fournisseurs de médias sociaux et des services interactifs), Ministère britannique du numérique, de la culture, des médias et des sports, 2016.

10. **5Rights Foundation report – But How Do They Know It Is a Child (Rapport de la 5Rights Foundation : mais comment savent-ils que c'est un enfant ?)**[211]
    Ce rapport de la 5Rights Foundation aborde le débat sur la vérification et l'estimation de l'âge.

11. **Code italien sur le cyberharcèlement**[212]
    Il s'agit du code officiel du gouvernement italien sur le cyberharcèlement (en italien).

12. **Financial Coalition Against Child Pornography (Coalition financière contre la pédopornographie)**[213]
    Ce rapport décrit les méthodes utilisées par certains membres de la Financial Coalition Against Child Pornography dans leur processus de demande et de vérification, et par la suite pour détecter le matériel concernant l'abus sexuel sur mineur et empêcher l'établissement ou le maintien de comptes marchands liés à la distribution commerciale et à la vente de ce matériel.

13. **Exploitation sexuelle commerciale des enfants en ligne 2015**[214]
    Ce rapport de la Coalition financière européenne contre l'exploitation sexuelle commerciale des enfants en ligne est une mise à jour de l'évaluation stratégique de l'exploitation sexuelle commerciale des enfants en ligne publiée en octobre 2013, dans le cadre de la Coalition financière européenne. En plus de présenter les faits et chiffres de 2013, il examine d'autres facteurs essentiels dans ce domaine.

14. **Déclaration universelle de protection en ligne des enfants**[215]
    Il s'agit de la déclaration de la Commission sur le large bande, qui vise à aligner toutes les parties prenantes sur la mission commune de défendre la cause de la protection en ligne des enfants.

15. **UNICEF Albania Trilogy of Promising Practice (UNICEF Albanie : la trilogie des pratiques prometteuses)**[216]
    Cette analyse est une étude de cas de l'Albanie. Quatre des cinq plus grandes entreprises des secteurs des communications et des services Internet se sont engagées dans un processus participatif visant à élaborer des lignes directrices sectorielles qui ont été publiées par l'Autorité nationale pour la certification électronique et la cybersécurité.

16. **OECD Guidelines for Digital Service Providers (Lignes directrices de l'OCDE pour les fournisseurs de services numériques)**[217]
    Les présentes lignes directrices visent à compléter la Recommandation du Conseil sur les enfants dans l'environnement numérique [NOTE DE BAS DE PAGE 2] et à aider les fournisseurs de services numériques, lorsqu'ils prennent des mesures susceptibles d'affecter directement ou indirectement les enfants dans l'environnement numérique, à déterminer la meilleure façon de protéger et de respecter les droits, la sécurité et les intérêts des enfants.

211. But how do they know it is a child? (Mais comment savent-ils que c'est un enfant ?), 5Rights Foundation, 2021.
212. Dispositions pour la protection des mineurs en vue de la prévention et du contraste du phénomène de cyberharcèlement, Gazzetta Ufficiale, 2017.
213. Pratiques saines d'acquisition et de surveillance des commerçants sur Internet pour contribuer à réduire la prolifération de la pédopornographie commerciale, Centre international pour les enfants disparus et exploités, 2016.
214. Exploitation sexuelle commerciale des enfants en ligne, Europol, 2015
215. Déclaration universelle de protection en ligne des enfants, Commission sur le large bande, 2019.
216. Programmation de la protection de l'enfance en ligne en Albanie, Fonds des Nations Unies pour l'enfance, 2020.
217. OECD Guidelines for Digital Service Providers (Lignes directrices de l'OCDE pour les fournisseurs de services numériques), OCDE, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

« Nous devons réformer les réseaux sociaux pour permettre aux enfants en situation de handicap d'en bénéficier. Nous devons simplifier [...] l'utilisation d'internet en langue des signes pour que nous, les malentendants, puissions être en mesure d'utiliser les plateformes numériques. »

– Enfant vivant en Tanzanie, 15 ans

« Je souhaite que les enfants [des zones rurales] puissent profiter des avantages offerts par Internet comme les autres. »

– Enfant vivant en Malaisie, 13 ans

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

6 Formation

> **Les professionnels travaillant pour et avec les enfants et le secteur des entreprises, y compris l'industrie technologique, doivent recevoir une formation portant notamment sur la manière dont l'environnement numérique affecte les droits de l'enfant dans de multiples contextes, sur la façon dont les enfants exercent leurs droits dans l'environnement numérique et sur les moyens d'accéder aux technologies et de les utiliser. Ils doivent également recevoir une formation sur l'application des normes internationales en matière de droits de l'homme à l'environnement numérique. Les États parties doivent veiller à ce que les professionnels travaillant à tous les niveaux de l'enseignement bénéficient d'une formation initiale et continue relative à l'environnement numérique, afin de favoriser le développement de leurs connaissances, de leurs compétences et de leurs pratiques.**
>
> Source : Observation générale n° 25 (2021), par. 33[218]

Objectif :

Veiller à ce que tous les acteurs impliqués dans les services concernant les enfants, y compris les pouvoirs publics, les forces de l'ordre, la justice, la santé et le bien-être, les politiciens et les fonctionnaires, ainsi que les concepteurs de technologies, aient une bonne compréhension de la protection en ligne des enfants et des meilleurs intérêts des enfants.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

6a. Offrir une formation, le perfectionnement des compétences et un mentorat à tous les acteurs de la protection en ligne des enfants
Des premiers intervenants aux juges, tous les acteurs de la chaîne de maintien de l'ordre public et les professionnels qui travaillent avec les enfants dans d'autres milieux tels que l'enseignement ou la santé doivent être conscients de la protection en ligne des enfants. Ils devront bénéficier d'une formation complète, y compris sur la façon dont la protection en ligne des enfants concerne leur rôle particulier, comment comprendre le comportement choquant, et comment assurer l'accès à l'aide aux victimes.

6b. Offrir une formation spécialisée pour le soutien psychosocial et l'identification des signes de toute la gamme des questions de protection en ligne des enfants
Pour être efficaces, les praticiens concernés doivent bénéficier d'une formation sur la protection en ligne des enfants, une formation sur les politiques de protection et de sauvegarde des enfants ainsi qu'une formation sur les conseils destinés aux enfants et aux familles. La sensibilisation à la protection en ligne des enfants devra être intégrée dans les cadres existants pour la protection des enfants. Les professionnels qui travaillent avec des enfants dans l'enseignement, la santé, les services communautaires et d'autres paramètres doivent être formés à reconnaître les signes et les symptômes de problèmes de protection en ligne des enfants.

6c. Développer des programmes d'enseignement supérieur
Les sessions relatives à la protection en ligne des enfants devront obligatoirement faire partie de l'enseignement, du travail social, de la santé, de la psychologie et d'autres programmes d'études pertinents dans les universités ou les établissements d'enseignement publics et privés. Il convient de réexaminer régulièrement l'efficacité de cet enseignement à la lumière des progrès réalisés en matière de formation à la protection en ligne des enfants et des questions émergentes. Les programmes scolaires doivent couvrir tous les aspects de la protection en ligne des enfants, tels que définis dans la présente politique. ▶

218. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

6 Formation

6d. Encourager le perfectionnement professionnel

Des programmes de formation continue sur la protection en ligne des enfants et la protection des enfants pour les professionnels travaillant dans les domaines pertinents seront établis, revus régulièrement et mis à jour pour suivre le rythme des nouvelles technologies et pour aborder les nouveaux obstacles ainsi que les nouvelles préoccupations à mesure qu'ils apparaissent.

Feuille de route pour atteindre l'objectif :

A **Offrir une formation, le perfectionnement des compétences et un mentorat à tous les acteurs de la protection en ligne des enfants**

Des premiers intervenants aux juges, tous les acteurs de la chaîne de maintien de l'ordre public et les professionnels qui travaillent avec les enfants dans d'autres milieux tels que l'enseignement ou la santé doivent être conscients de la protection en ligne des enfants. Ils devront bénéficier d'une formation complète, y compris sur la façon dont la protection en ligne des enfants concerne leur rôle particulier, comment comprendre le comportement choquant, et comment assurer l'accès à l'aide aux victimes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier toutes les professions et les interlocuteurs concernés qui pourraient avoir besoin d'une formation sur la protection en ligne des enfants. L'outil d'assistance 1 ci-dessous peut être utile à cet égard (voir page n° 119).
2. Examiner les programmes de formation existants et déterminer à quel moment et à quel niveau de détail une formation sur la protection en ligne des enfants est nécessaire (voir les ressources ci-dessous).
3. Mettre en place ou mettre à jour une formation existante sur la protection en ligne des enfants, adaptée au domaine. Ces matériels peuvent être partagés entre les disciplines afin de garantir une formation de haute qualité.
4. L'obtention d'une qualification dans n'importe quel domaine est sujette à sa réussite.
5. Veiller à ce que les supports de formation soient régulièrement mis à jour et couvrent tous les aspects de la vie en ligne d'un enfant : risques relatifs au contenu, aux contacts, à la conduite et aux activités commerciales.
6. Réfléchir à la manière d'impliquer la voix et l'opinion des enfants et des jeunes dans la formation.[219]

219. Voir, par exemple, The Lundy Model of Child Participation (Le modèle Lundy de participation des enfants), Commission européenne, 2007.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

6 Formation

B **Offrir une formation spécialisée pour le soutien psychosocial et l'identification des signes de toute la gamme des questions de protection en ligne des enfants**

Pour être efficaces, les praticiens concernés doivent bénéficier d'une formation sur la protection en ligne des enfants, une formation sur les politiques de protection et de sauvegarde des enfants ainsi qu'une formation sur les conseils destinés aux enfants et aux familles. La sensibilisation à la protection en ligne des enfants devra être intégrée dans les cadres existants pour la protection des enfants. Les professionnels qui travaillent avec des enfants dans l'enseignement, la santé, les services communautaires et d'autres secteurs doivent être formés à reconnaître les signes et les symptômes de problèmes de protection en ligne des enfants, à comprendre les comportements délictueux et à fournir un accès à des services d'aide aux victimes.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier ceux qui ont besoin d'une formation en matière de soutien psychosocial et d'exploitation et d'abus sexuels sur mineur.
2. Identifier des formations entièrement testées, au niveau international ou régional (voir Autres ressources pour référence 1-4 ci-dessous).
3. S'assurer que les ressources financières et le temps sont une priorité pour la formation en matière d'exploitation et d'abus sexuels sur mineur.
4. Identifier quand et comment la formation sera dispensée, évaluée et améliorée.
5. Réfléchir à la manière d'impliquer la voix et l'opinion des enfants et des jeunes dans la formation.[220]
6. Établir des indicateurs clés de performance pour la formation de la main-d'œuvre qui doivent être évalués et faire l'objet de rapports réguliers.

220. Voir, par exemple, The Lundy Model of Child Participation (Le modèle Lundy de participation des enfants), Commission européenne, 2007.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

6 Formation

C Développer des programmes d'enseignement supérieur

Les sessions relatives à la protection en ligne des enfants devront obligatoirement faire partie de l'enseignement, du travail social, de la santé, de la psychologie et d'autres programmes d'études pertinents dans les universités ou les établissements d'enseignement publics et privés. Il convient de réexaminer régulièrement l'efficacité de cet enseignement à la lumière des progrès réalisés en matière de formation à la protection en ligne des enfants et des questions émergentes. Les programmes scolaires doivent couvrir tous les aspects de la protection en ligne des enfants, tels que définis dans la présente politique.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de consulter la rubrique Autres ressources pour référence 1 (ci-dessous) qui contient des exemples.

D Encourager le perfectionnement professionnel

Des programmes de formation continue sur la protection en ligne des enfants et la protection des enfants pour les professionnels travaillant dans les domaines pertinents seront établis, revus régulièrement et mis à jour pour suivre le rythme des nouvelles technologies et pour aborder les nouveaux obstacles ainsi que les nouvelles préoccupations à mesure qu'ils apparaissent.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Veiller à ce que la formation soit disponible tout au long du cycle de vie d'un professionnel, et répondre aux changements tant dans le monde numérique que dans les rôles des professionnels.
2. Identifier les possibilités de formation continue.
3. Élaborer des programmes de formation qui encouragent un apprentissage plus détaillé ou « complémentaire » (voir Autres ressources pour référence 1-4 ci-dessous).
4. Réfléchir à la manière d'impliquer la voix et l'opinion des jeunes dans la formation.[221]

221. Voir, par exemple, The Lundy model of child participation (Le modèle Lundy de participation des enfants), Commission européenne, 2007.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

6 Formation

Comment cela concorde avec les documents fondamentaux :

> **Les États parties doivent examiner la manière dont les utilisations des technologies numériques peuvent faciliter ou entraver les enquêtes et les poursuites relatives aux crimes contre les enfants et prendre toutes les mesures préventives, répressives et correctives disponibles, y compris en coopération avec les partenaires internationaux. Ils doivent fournir une formation spécialisée aux responsables de l'application des lois, aux procureurs et aux juges concernant les violations des droits de l'enfant spécifiquement associées à l'environnement numérique, y compris par le biais de la coopération internationale.**
>
> Source : Observation générale n° 25 (2021), par. 47[222]

222. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

6 Formation

Outils d'assistance :

1. Une liste des professions pouvant bénéficier d'une formation spécifique, ainsi que des sujets à aborder

Elle est conçue pour vous aider à déterminer si la formation existante est appropriée et pertinente pour les professionnels de votre juridiction, et à identifier les lacunes. Cette initiative s'inscrit dans le cadre de la réalisation du processus A (« Offrir une formation, le perfectionnement des compétences et un mentorat à tous les acteurs de la protection en ligne des enfants »).

Profession	Formation sur toutes les questions relatives à la protection en ligne des enfants, et sur les 4C de risque	Formation sur la protection et les politiques de protection	Reconnaître les problèmes de protection en ligne des enfants	Comprendre le comportement et la réhabilitation d'une personne délinquante	Services de conseil	Aider les victimes
Juges	*[identifier la formation existante ou identifier les lacunes]*					
Application de la loi						
Assistants sociaux						
Professionnels de santé						
Enseignants						
Travailleurs en milieu communautaire						
Psychologues						
Autres						

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

6 Formation

Autres ressources pour référence :

Il existe de nombreux exemples de modules de formation disponibles en ligne pour différents groupes de professionnels. Des formations initiales, tertiaires et continues doivent être dispensées à un large éventail de professionnels, notamment les enseignants/éducateurs, les agents chargés du maintien de l'ordre, les travailleurs du secteur de la justice, les travailleurs sociaux et les jeunes, les professionnels de la santé, les parlementaires, les fonctionnaires, les technologues (y compris les programmeurs informatiques, les concepteurs UX et les responsables de la gouvernance) et les régulateurs dans les domaines concernés.

1. **Ressources pour les enseignants, les travailleurs sociaux et les animateurs de jeunesse**
   Voir la formation à la protection en ligne de la NSPCC. Toute personne qui travaille avec des enfants et des jeunes doit savoir ce qu'il faut faire si un enfant vient les voir pour leur parler de quelque chose d'inquiétant qu'il a vu en ligne. Cette formation est conçue pour aider les professionnels à se sentir responsables de la protection en ligne des enfants.[223]

2. **Ressources pour les professionnels de la santé**
   La formation en ligne d'eIntegrity sur la protection de l'enfance destinée aux professionnels de la santé (Safeguarding Children and Young People, Protection des enfants et des jeunes) couvre les connaissances et les compétences nécessaires aux professionnels de la santé et des services sociaux pour préserver le bien-être des enfants. Elle a été élaborée par un consortium d'organismes professionnels, dirigé par le Royal College of Paediatrics and Child Health.[224]

   Ce cours de protection en ligne est mis en correspondance avec le cadre britannique de formation dans ce domaine, le document intercollégial Safeguarding Children and Young People: Roles and Competencies for Health Care Staff (Protection des enfants et des jeunes : rôles et compétences du personnel de santé) (2019).[225] Toutefois, les thèmes sont pertinents pour les professionnels de la santé et de l'aide sociale dans le monde entier.[226]

3. **Ressources pour les forces de l'ordre**[227]
   L'ICMEC offre une série de possibilités de formation et de cours différents, telles que :

   - ☐ Les principes fondamentaux des crimes contre les enfants facilités par la technologie
   - ☐ Des recherches avancées sur l'exploitation en ligne
   - ☐ Des technologies de pointe
   - ☐ Les principes fondamentaux de l'intervention en cas de disparition d'enfants.

223. Introduction à la formation sur la sauvegarde et la protection des enfants, National Society for the Prevention of Cruelty to Children (Société nationale pour la prévention de la cruauté envers les enfants).
224. Formation en ligne sur la protection des enfants pour les professionnels de la santé, eIntegrity.
225. Safeguarding children and young people – roles and competencies (Protection des enfants et des jeunes : rôles et compétences), Royal College of Paediatrics and Child Health, 2019.
226. Online child protection training for healthcare professionals (Formation en ligne sur la protection des enfants pour les professionnels de la santé), eIntegrity.
227. Building global capacity to keep children safer from harm (Renforcer les capacités mondiales pour protéger les enfants contre les dangers), Le Centre international pour enfants disparus et sexuellement exploités, 2015 et Ressources ICMEC, Centre international pour enfants disparus et sexuellement exploités.

4. **Gender-Based Violence in Namibia: An exploratory assessment and mapping of GBV response services in Windhoek (La violence basée sur le genre en Namibie : une évaluation exploratoire et une cartographie des services de réponse à la VBG à Windhoek), 2016**[228]
   En Namibie, l'unité de protection contre la violence basée sur le genre (GBVPU) et les programmes de formation des enfants témoins proposent des formations aux enquêteurs de la police, aux procureurs, aux magistrats et aux travailleurs sociaux (personnel chargé de la protection de l'enfance) afin de garantir un meilleur soutien de bout en bout aux victimes. La GBVPU est accessible aux personnes en situation de handicap, dispose d'une salle d'interview vidéo adaptée aux enfants et est encadrée par des procédures opérationnelles standard pour la VBG/VEE (Violence à l'encontre des enfants).

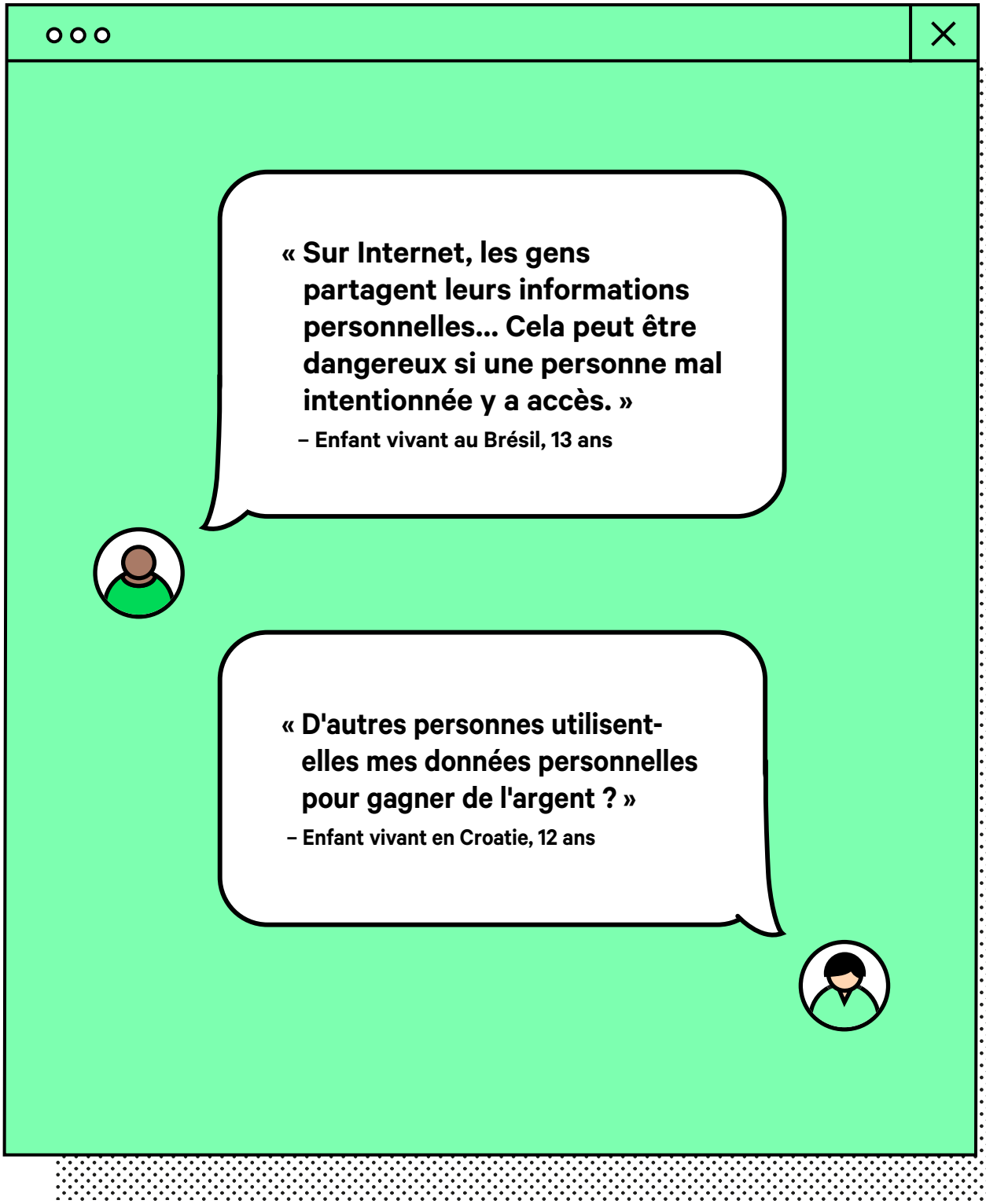
5. **Ressources pour le secteur de la justice**[229]
   Le projet EndOCSEA du Conseil de l'Europe offre une formation aux juges et aux procureurs sur l'exploitation et les abus sexuels sur mineur.

6. **Ressources générales**
   La Queensland Family and Child Commission (Commission de la famille et de l'enfance du Queensland) a produit un module de protection en ligne des enfants.[230]

228. Gender-Based Violence in Namibia: An exploratory assessment and mapping of GBV response services in Windhoek (La violence basée sur le genre en Namibie : une évaluation exploratoire et une cartographie des services de réponse à la VBG à Windhoek), Victims 2 Survivors et ONUSIDA, 2016.
229. Mettre fin à l'exploitation et aux abus sexuels des enfants en ligne, Conseil de l'Europe, 2021.
230. Module de protection en ligne des enfants, Queensland Family & Child Commission (Commission de la famille et de l'enfance du Queensland), 2022.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >



< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

7 Enseignement

> **Les États parties devront fournir et encourager la création de contenus numériques adaptés à l'âge et à l'autonomie des enfants, en fonction de l'évolution de leurs capacités, et veiller à ce que les enfants aient accès à une grande diversité d'informations, y compris celles détenues par les organismes publics, sur la culture, les sports, les arts, la santé, les affaires civiles et politiques, ainsi que les droits de l'enfant.**
>
> **Les États parties devront promouvoir la production et la diffusion de ces contenus sous des formes multiples et à partir d'une pluralité de sources nationales et internationales, notamment les médias d'information, les organismes de radiodiffusion, les musées, les bibliothèques et les organisations éducatives, scientifiques et culturelles. Ils devront notamment s'efforcer d'améliorer l'offre de contenus diversifiés, accessibles et bénéfiques pour les enfants en situation de handicap et les enfants appartenant à des groupes ethniques, linguistiques, autochtones et autres minorités. La possibilité d'accéder à des informations pertinentes, dans les langues que les enfants comprennent, peut avoir un impact positif significatif sur l'égalité.**
>
> Source : Observation générale n° 25 (2021), par. 51 et 52[231]

Objectif :

Promouvoir l'utilisation positive de la technologie numérique comme source de divertissement, d'information et d'apprentissage pour les enfants dans un environnement sûr.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

7a. Désigner des responsables de la protection de l'enfance

Chaque école doit désigner un responsable de la protection de l'enfance.[232] Chaque responsable doit recevoir une formation sur les procédures de protection des enfants et une formation spécifique à la protection en ligne des enfants. Les responsables seront chargés de veiller à ce que les politiques de protection en ligne des enfants (y compris les procédures de protection et les systèmes de signalement anonyme) soient adoptées, mises en œuvre et appliquées dans les écoles. Le responsable de la protection de l'enfance sera le point de contact concernant les préoccupations liées à la protection de l'enfance et à la protection en ligne des enfants, et transmettra les préjudices signalés aux autorités compétentes. Les responsables doivent également faciliter les plans d'intervention, afin de protéger les enfants contre tous les dangers qui les menacent. ▶

231. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, Comité des droits de l'enfant des Nations Unies, 2021.
232. Il peut s'agir d'un membre du comité de sécurité de l'école, d'un éducateur ou d'un membre du comité de protection de l'enfance d'un village ou d'une communauté où les écoles sont représentées.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

7 Enseignement

7b. Promouvoir un enseignement numérique accessible
Promouvoir les contenus, y compris les programmes de pair à pair, qui sont conçus et montrés pour aider les enfants à développer des compétences numériques et leur donner les moyens de bâtir des communautés respectueuses qui favorisent la protection en ligne des enfants. Le système d'enseignement numérique devra être holistique et couvrir l'éducation aux données et aux médias, ainsi que les questions de protection, en particulier les questions de sexualité et de consentement. L'enseignement sera également étendu aux parents/personnes en charge d'enfants afin de les aider à promouvoir la protection en ligne des enfants.

7c. Promouvoir le contenu pédagogique
Au rythme de la généralisation de l'adoption numérique, les élèves et les enseignants apprendront les compétences nécessaires pour interagir avec les systèmes numériques et tirer pleinement profit du contenu des programmes, tant dans les langues locales qu'internationales.

7d. Promouvoir l'habileté numérique
Un programme d'habileté numérique sera introduit dans les programmes scolaires. Le programme sensibilisera les enfants à la manière dont leurs données peuvent être utilisées et leur fournira une compréhension de base de l'économie des données. Il mettra l'accent sur l'utilisation positive, autonome et créative des technologies numériques par les enfants et l'encouragera ; il définira clairement les risques, les avantages et les conséquences sociales de l'utilisation des technologies ; il visera à garantir que les mesures de protection et de prévention sont largement diffusées, comprises et appliquées. L'enseignement de l'habileté numérique devra préciser clairement les différentes parties prenantes responsables de la protection en ligne.

7e. Promouvoir la pensée critique
L'enseignement destiné aux enfants et aux parents/personnes en charge d'enfants sur la pensée critique ainsi que la sensibilisation aux risques de la désinformation en ligne devront être intégrés dans l'enseignement de l'habileté numérique. Cette démarche doit inclure un enseignement plus large pour promouvoir la compréhension et la sensibilisation aux droits de l'homme, en particulier les droits de l'enfant, et la manière dont ils fonctionnent en ligne et hors ligne.[233]

7f. Introduire des procédures formelles de protection en ligne pour les enfants dans les écoles
La formation à la protection en ligne des enfants doit faire partie intégrante des diplômes d'enseignement, tant au niveau de l'école primaire que de l'école secondaire, et faire l'objet d'une formation continue en service. Tous les enseignants doivent suivre une formation obligatoire sur la protection en ligne des enfants, connaître la politique de l'école en matière de protection en ligne des enfants et donner des cours sur la protection en ligne des enfants aux élèves. Toutes les écoles doivent nommer un responsable de la protection en ligne des enfants, chargé de défendre les normes de protection en ligne des enfants et d'assumer la responsabilité de l'application de la politique de l'école en matière de protection en ligne des enfants.

233. Voir l'article 29 de la Convention relative aux droits de l'enfant, et les articles pertinents d'observation générale.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

7 Enseignement

Feuille de route pour atteindre l'objectif :

A **Désigner des responsables de la protection de l'enfance**

Chaque école doit désigner un responsable de la protection de l'enfance.[234] Chaque responsable doit recevoir une formation sur les procédures de protection des enfants et une formation spécifique à la protection en ligne des enfants. Les responsables seront chargés de mettre en œuvre et d'appliquer les politiques de protection de l'enfance (y compris les procédures de protection et les systèmes de signalement anonyme) dans les écoles. Le responsable sera le point de contact concernant les préoccupations liées à la protection de l'enfance et à la protection en ligne des enfants, et transmettra les préjudices signalés aux autorités compétentes. Les responsables doivent également faciliter les plans d'intervention, afin de protéger les enfants contre tous les dangers qui les menacent.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les politiques et règles existantes de l'école en matière de sécurité et de protection de l'enfance, et s'assurer qu'elles comprennent des modules sur la protection en ligne des enfants. À défaut, rechercher les meilleures pratiques. Voir Autres ressources 1-6 pour obtenir des exemples.
2. Dans un cas comme dans l'autre, veiller à ce que la préparation de chaque année scolaire comprenne des mesures actualisées de sécurité et de protection de l'enfance, en fournissant à tous les enseignants un aperçu des questions relatives à la sécurité des enfants. Voir Autres ressources 2 à propos des cours en ligne disponibles pour les intervenants de première ligne.

234. Il peut s'agir d'un membre du comité de sécurité de l'école, d'un éducateur ou d'un membre du comité de protection de l'enfance d'un village ou d'une communauté où les écoles sont représentées.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

7 Enseignement

B **Promouvoir un enseignement numérique accessible**

Promouvoir les contenus, y compris les programmes de pair à pair, qui sont conçus et montrés pour aider les enfants à développer des compétences numériques et leur donner les moyens de bâtir des communautés respectueuses qui favorisent la protection en ligne des enfants. Le système d'enseignement numérique doit être holistique et couvrir l'éducation aux données et aux médias, ainsi que les questions de sexualité et de consentement. L'enseignement relatif à la sécurité et à la protection de l'enfance sera également étendu aux parents/personnes en charge d'enfants afin de les aider à promouvoir la protection en ligne des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Veiller à ce que l'habileté numérique couvre l'ensemble de l'expérience en ligne, et pas seulement les questions de sécurité, car de nombreux enfants qui n'apprécient pas l'e-sécurité sont très ouverts à une compréhension plus large des possibilités et des risques. Étudier le modèle DQ (voir Autres ressources 3) des domaines qui doivent être couverts (voir Ressources ci-dessous), et s'assurer que tous les domaines qui traitent du risque couvrent les 4C (voir l'article Identification des risques et atténuation des dommages).
2. Veiller à ce que l'éducation sexuelle, la sexualité et le consentement soient enseignés dans le contexte du monde numérique, afin que les enfants aient un maximum de contrôle sur les questions connexes qui peuvent se poser en ligne.
3. Identifier les programmes d'habileté numérique dans une langue appropriée ou qui sont disponibles à la traduction si nécessaire.[235]
4. Veiller à ce que l'habileté numérique pour les parents/personnes en charge d'enfants soit pleinement alignée sur l'habileté numérique pour les enfants. Les ressources parentales doivent être positives et bien équilibrées et ne pas provoquer de panique excessive à propos du monde numérique ou encourager des mesures drastiques à l'encontre des enfants.[236]
5. Identifier les entreprises technologiques qui proposent des programmes gratuits d'habileté numérique pour les enfants et les adultes. Ces derniers sont souvent très bien conçus et très efficaces, mais ne parviennent pas à identifier les risques et les dommages commerciaux de la technologie elle-même. Si la solution locale consiste à utiliser ces programmes, s'assurer qu'ils couvrent tous les aspects du risque, y compris ceux créés par les programmes eux-mêmes.

235. Voir par exemple Habileté numérique, Union internationale des télécommunications.
236. Voir par exemple Media and Digital Literacy: Resources for Parents (Habileté numérique et de médias : Ressources pour les parents), The George Lucas Educational Foundation, 2012.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

7 Enseignement

C **Promouvoir le contenu pédagogique**

Au rythme de la généralisation de l'adoption numérique, les élèves et les enseignants apprendront les compétences nécessaires pour interagir avec les systèmes numériques et tirer pleinement profit du contenu des programmes, tant dans les langues locales qu'internationales.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Trouver un bon contenu éducatif en rapport avec le programme scolaire ou les activités extrascolaires de l'école.
2. S'assurer que les conditions générales d'utilisation sont adaptées à la confidentialité et à la sécurité des élèves.
3. Veiller à ce que tous les élèves, indépendamment de leur sexe, de leur handicap et de leur statut socio-économique, puissent accéder aux ressources : pour ce faire, il peut être nécessaire de prendre en compte la connectivité, le coût (y compris les données) et l'accès à des appareils adaptés.
4. Rechercher des ressources auprès d'institutions réputées (par exemple, des universités, des écoles, des ONG) proposées dans une grande variété de sujets et de ressources. Pour certains sujets, il peut être préférable de tenir compte du coût de la traduction ou de l'utilisation de matériel existant plutôt que de créer du matériel à partir de zéro ; dans d'autres cas, commander ou identifier du matériel dans les langues locales, qui couvre la culture ou l'histoire locales, peut être un investissement important.
5. Considérer que la large disponibilité de matériel en ligne doit permettre d'étendre les sujets au-delà de l'enseignement compétent disponible localement. Il n'en reste pas moins qu'un enseignant expérimenté offre une expérience qualitativement différente de l'apprentissage en ligne.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

7 Enseignement

D **Promouvoir l'habileté numérique**

Un programme d'habileté numérique sera introduit dans les programmes scolaires. Le programme sensibilisera les enfants à la manière dont leurs données peuvent être utilisées et leur fournira une compréhension de base de l'économie des données. Il mettra l'accent sur l'utilisation positive, autonome et créative des technologies numériques par les enfants et l'encouragera ; il définira clairement les risques, les avantages et les conséquences sociales de l'utilisation des technologies ; il visera à garantir que les mesures de protection et de prévention sont largement diffusées, comprises et appliquées. L'enseignement de l'habileté en matière de données devra préciser clairement les différentes parties prenantes responsables de la protection en ligne.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de se pencher sur les ressources et les actions couvertes aux points A à C ci-dessus.

E **Promouvoir la pensée critique**

L'enseignement destiné aux enfants et aux parents/personnes en charge d'enfants sur la pensée critique ainsi que la sensibilisation aux risques de la désinformation en ligne devront être intégrés dans l'enseignement de l'habileté numérique. Cette démarche doit inclure un enseignement plus large pour promouvoir la compréhension et la sensibilisation aux droits de l'homme, en particulier les droits de l'enfant, et la manière dont ils fonctionnent en ligne et hors ligne.[237]

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de se pencher sur les ressources et les actions couvertes aux points A à C ci-dessus.

237. Voir l'article 29 de la Convention relative aux droits de l'enfant, et les articles pertinents d'observation générale.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

7 Enseignement

F **Introduire des procédures formelles de protection en ligne pour les enfants dans les écoles**

La formation à la protection en ligne des enfants doit faire partie intégrante des diplômes d'enseignement, tant au niveau de l'école primaire que de l'école secondaire, et faire l'objet d'une formation continue en service. Tous les enseignants doivent suivre une formation obligatoire sur la protection en ligne des enfants, connaître la politique de l'école en matière de protection en ligne des enfants et prodiguer aux élèves des cours sur la protection en ligne des enfants. Toutes les écoles doivent nommer un responsable de la protection en ligne des enfants, chargé de défendre les normes de protection en ligne des enfants et d'assumer la responsabilité de l'application de la politique de l'école en matière de protection en ligne des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de se pencher sur les ressources et les actions couvertes aux points A à C ci-dessus.

Comment cela concorde avec les documents fondamentaux :

Sensibiliser les enfants à l'habileté numérique dans le cadre d'une stratégie visant à garantir qu'ils puissent bénéficier de la technologie sans subir de dommages. Cela permettra aux enfants de développer un esprit critique qui les aidera à identifier et à comprendre les bons et mauvais côtés de leur comportement dans l'espace numérique. S'il est important d'illustrer aux enfants les dangers qui peuvent se produire en ligne, cette démarche ne sera efficace que si elle fait partie d'un programme plus large d'habileté numérique, adapté à l'âge des enfants et axé sur les aptitudes et les compétences. Il est important d'inclure les concepts d'apprentissage social et émotionnel dans l'enseignement de la protection en ligne, car ils aideront les élèves à comprendre et à gérer leurs émotions pour avoir des relations saines et respectueuses, tant en ligne qu'hors ligne.

Source: ITU Guidelines for policy-makers on Child Online Protection 2020 (Lignes directrices de l'UIT à l'attention des responsables politiques sur la protection en ligne des enfants 2020)[238]

Assurer un enseignement de qualité inclusif et équitable et promouvoir les possibilités d'apprentissage tout au long de la vie pour tous.

Source : Objectif de développement durable 4[239]

238. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.
239. Objectif 4 : Assurer un enseignement de qualité inclusif et équitable et promouvoir les possibilités d'apprentissage tout au long de la vie pour tous, Nations Unies, 2017.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

7 Enseignement

Outils d'assistance :

1. Une liste de contrôle pour garantir des procédures formelles de protection en ligne pour les enfants dans les écoles

Il s'agit d'identifier les lacunes dans les procédures de protection en ligne des enfants scolarisés. Elle permettra de suivre les progrès réalisés dans le cadre du Processus F (« Introduire des procédures formelles de protection en ligne pour les enfants dans les écoles »).

Question	Réponse
La protection en ligne des enfants fait-elle partie des cours de formation des enseignants ?	
Toutes les écoles primaires et secondaires ont-elles un responsable de la protection en ligne des enfants ?	
Toutes les écoles primaires et secondaires ont-elles une politique de protection en ligne pour les enfants ?	
Toutes les écoles primaires dispensent-elles des cours de protection en ligne aux élèves ? a. Désigner des responsables de la protection de l'enfance b. Promouvoir un enseignement numérique accessible c. Promouvoir le contenu pédagogique d. Promouvoir l'habileté numérique e. Promouvoir la pensée critique f. Introduire des procédures formelles de protection en ligne pour les enfants dans les écoles	
Toutes les écoles secondaires dispensent-elles des cours de protection en ligne aux élèves ?	

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

7 Enseignement

Autres ressources pour référence :

1. **DQ Child Digital Readiness Kit: 8-Day Home-Based e-Learning for Children (ages 8-12) and Parents (Kit de préparation des enfants au numérique de DQ : 8 jours d'apprentissage en ligne à domicile pour les enfants (8-12 ans) et les parents)**[240]
   Il s'agit d'un programme d'apprentissage en ligne de 8 jours, au cours duquel les enfants apprennent les 8 compétences de citoyenneté numérique, avec une aide minimale des parents ou des enseignants. Au fur et à mesure que les enfants acquièrent chaque compétence de citoyenneté numérique, les parents reçoivent par courrier électronique une carte de score DQ, qui détaille les progrès de leur enfant et son exposition aux cyber-risques. Les parents reçoivent également une copie numérique du Manuel parental DQ pour les aider à améliorer l'habileté DQ de toute leur famille.

2. **protection en ligne des enfants en Afrique du Sud**[241]
   Ce site Web fournit des conseils interactifs aux éducateurs et aux soignants concernant la protection en ligne des enfants. Les soignants et les éducateurs sont encouragés à partager leurs stratégies ou leurs politiques scolaires sur la plateforme.

3. **National Association of School Psychologists – A Framework for Safe and Successful Schools (Association nationale des psychologues scolaires : un cadre pour la sécurité et la réussite des écoles)**[242]
   Ce cadre fournit des recommandations sur la manière d'améliorer la sécurité physique et mentale des enfants et des jeunes grâce à une stratégie pour des écoles sûres et solidaires.

4. **International Task Force on Child Protection – International Child Protection Standards and Expectations (Groupe de travail international sur la protection de l'enfant : normes et attentes internationales en matière de protection de l'enfant)**[243]
   Ce rapport, préparé par le comité d'évaluation des écoles, fournit les exigences d'évaluation de la protection de l'enfance pour les agences d'accréditation et d'inspection.

5. **Council of International Schools (Conseil des écoles internationales)**[244]
   Ce site Web fournit des conseils et des outils utiles aux soignants et aux éducateurs concernant la sécurité des enfants et des jeunes. Il propose des exemples d'ateliers sur la protection de l'enfance, sur la santé mentale et le bien-être, sur les normes de recrutement plus sûr, etc.

6. **NSPCC Online safety training in English (Formation à la protection en ligne de la NSPCC en anglais)**[245]
   Ce cours en ligne propose une formation à la sécurité destinée aux personnes en charge d'enfants et vise à leur apprendre comment et à quoi faire attention en ce qui concerne la protection en ligne des enfants. Il aborde des sujets importants tels que la radicalisation et l'extrémisme en ligne, le harcèlement et la délinquance sexuelle. ▶

240. Global Digital Citizenship Movement for 8-12 Year-Olds (Mouvement mondial de citoyenneté numérique pour les 8 à 12 ans), DQ Institute.
241. Child Online Safety (protection en ligne des enfants), Portail de l'enseignement de Thutong.
242. A Framework for Safe and Successful Schools (Un cadre pour des écoles sûres et performantes), National Association of School Psychologists (Association nationale des psychologues scolaires), 2013.
243. Updated Standards for Child Protection Adopted by School Evaluation Agencies (Normes actualisées de protection de l'enfance adoptées par les agences d'évaluation des écoles), Centre international pour enfants disparus et sexuellement exploités, 2021.
244. Resources, Council of International Schools.
245. Introduction à la formation sur la sauvegarde et la protection des enfants, National Society for the Prevention of Cruelty to Children (Société nationale pour la prévention de la cruauté envers les enfants).

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

7 Enseignement

7. Exemples de ressources éducatives visant à promouvoir la protection en ligne des enfants

A. Sample Syllabus – Young and eSafe Curriculum from Australian Office of the eSafety Commissioner (Exemple Syllabus - Programme éducatif jeunesse et e-sécurité du Bureau australien du commissaire à l'e-sécurité)[246]
Ce site Web fournit des ressources telles que de courtes vidéos et du contenu éducatif pour aider les jeunes à adopter des comportements positifs en ligne.

B. Common Sense Education Media Free Lessons to Teach Digital Citizenship to Children of All Ages (Leçons gratuites sur les médias Common Sense Education enseignant les notions de citoyenneté numérique aux enfants de tous âges)[247]
Ce site Web propose des leçons gratuites pour aider les enfants et les jeunes à acquérir des compétences en matière de citoyenneté numérique. Ces leçons portent, par exemple, sur des questions telles que le cyberharcèlement et la confidentialité en ligne.

C. International Telecommunication Union: Online safety activity book (Union internationale des télécommunications : cahier d'activités sur la protection en ligne)[248]
Ce cahier d'activités sur la protection en ligne propose une introduction à la Convention relative aux droits de l'enfant et des exercices sur la manière d'interagir en toute sécurité avec des personnes sur Internet.

D. Union internationale des télécommunications : guide de l'enseignant (Teacher's Guide)[249]
Ce manuel contient les instructions et les ressources nécessaires pour réaliser ces exercices de protection en ligne dans une salle de classe avec des enfants de 9 à 12 ans. L'objectif de ces activités est d'inciter les élèves et les enseignants à discuter des problèmes de protection en ligne et de la manière de les gérer.

E. ITU Digiworld: An example of how the ITU Guidelines on Child Online Protection can be delivered in practice (Digiworld de l'UIT : un exemple de la façon dont les lignes directrices de l'UIT sur la protection en ligne des enfants peuvent être mises en pratique)[250]
Ce document décrit comment les lignes directrices de l'UIT peuvent être utilisées dans la pratique pour développer la protection en ligne des enfants.

F. Boîte à outils pédagogique de Childnet International[251]
Le programme Step Up, Speak Up! (Agissez, parlez !) La boîte à outils pédagogique est une ressource pratique, interactive et basée sur des scénarios qui aborde la question du harcèlement sexuel en ligne chez les 13-17 ans. Cette boîte à outils se compose de 4 plans de cours accompagnés de films, d'une histoire audio, d'ateliers et d'une présentation dans le cadre d'un rassemblement.

G. UK Guidance – Teaching online safety in school (Directive du Royaume-Uni : enseigner la protection en ligne à l'école)[252]
Il s'agit d'orientations qui aident les écoles à enseigner à leurs élèves comment assurer leur protection en ligne, dans le cadre de matières scolaires nouvelles ou existantes.

246. Young and eSafe (Jeune et en toute e-sécurité), Office of the eSafety Commissioner (Bureau du commissaire à la sécurité électronique).
247. Everything You Need to Teach Digital Citizenship (Tout le nécessaire pour enseigner la citoyenneté numérique), Common Sense Education.
248. Online safety activity book - Work with Sango (Cahier d'activités sur la protection en ligne : travailler avec Sango), Union internationale des télécommunications.
249. Online safety activity book - Teacher's Guide (Livre d'activités sur la protection en ligne : guide de l'enseignant), Union internationale des télécommunications.
250. Digiworld – An example of how the ITU Guidelines on Child Online Protection can be delivered in practice (Digiworld : un exemple de mise en pratique des lignes directrices de l'UIT sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.
251. Boîte à outils pour l'enseignement, Childnet.
252. Teaching online safety in school (Enseigner la protection en ligne à l'école), Department for Education (Ministère de l'éducation), 2019.

H. **Council of Europe EndOCSEA Kiko and the Manymes Booklet and Video (Livret et vidéo Kiko et les Manymes du Conseil de l'Europe EndOCSEA)**[253]
Ce livre d'histoires et cette vidéo, lancés par le Conseil de l'Europe, offrent des conseils aux personnes en charge d'enfants et aux jeunes enfants sur la manière d'utiliser Internet en toute sécurité.

8. **Sri Lanka: WebFighter campaign**[254]
Ce site Web fournit des conseils et des outils utiles aux soignants et aux éducateurs concernant la sécurité des enfants et des jeunes. Il propose des exemples d'ateliers sur la protection de l'enfance, sur la santé mentale et le bien-être, sur les normes de recrutement plus sûr, etc.

9. **Le programme Swipe Safe**[255]
Le programme Swipe Safe aide les jeunes à naviguer sur internet en toute sécurité en les informant des risques potentiels, tels que les escroqueries, le harcèlement ou les abus sexuels sur la toile, en leur proposant des stratégies pour se protéger. Le programme a été adapté par des organisations non gouvernementales au Vietnam, au Laos et en Birmanie. Swipe Safe mobilise les parents, les jeunes, les écoles et le secteur privé pour qu'ils jouent un rôle actif dans la protection en ligne des enfants. Le programme offre une formation aux propriétaires/gestionnaires de cybercafés afin qu'ils puissent identifier et traiter les risques et les éventuels événements indésirables qui pourraient arriver aux enfants, que ce soit en ligne ou hors ligne. Il assiste également les écoles dans l'élaboration de politiques adaptées aux enfants et de conseils sur la protection en ligne.

10. **Digital Literacy Package (DLP) (Kit d'habileté numérique)**[256]
Le kit ghanéen d'habileté numérique, produit par l'UNICEF, a été élaboré pour doter les enfants d'une habileté numérique et veiller à ce qu'ils restent en sécurité et résilients dans l'espace en ligne. Il comporte également des éléments destinés aux parents/personnes en charge d'enfants, leur donnant les moyens d'aider les élèves à rester en protection en ligne, surtout à l'heure de la COVID-19, où l'apprentissage à distance est devenu la norme.

253. EndOCSEA@Europe Activities - Kiko's exciting adventures continue in the digital age (Activités EndOCSEA@Europe - Les aventures passionnantes de Kiko se poursuivent à l'ère numérique), Conseil de l'Europe, 2020.
254. Goethe Institut.
255. ChildFund Swipe Safe, ChildFund Alliance, 2019.
256. Digital Literacy Package (DLP) (Kit d'habileté numérique), UNICEF, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications

> **Les États parties doivent diffuser des informations et mener des campagnes de sensibilisation sur les droits de l'enfant dans l'environnement numérique, en se concentrant en particulier sur ceux dont les actions ont un impact direct ou indirect sur les enfants. Ils doivent faciliter les programmes éducatifs destinés aux enfants, aux parents et aux personnes en charge d'enfants, au grand public et aux responsables politiques afin d'améliorer leur connaissance des droits de l'enfant en relation avec les opportunités et les risques associés aux produits et services numériques. De tels programmes doivent inclure des informations sur la manière dont les enfants peuvent bénéficier des produits et services numériques et développer leur habileté et leurs compétences numériques, sur la manière de protéger la confidentialité des enfants et de prévenir la victimisation, et sur la façon de reconnaître un enfant victime de dommages perpétrés en ligne ou hors ligne et de réagir de manière appropriée. Ces programmes doivent s'appuyer sur des recherches et des consultations avec les enfants, les parents et les personnes en charge d'enfants.**
>
> Source : Observation générale n° 25 (2021), par. 32[257]

Objectif :

Sensibiliser le public sur toutes les questions de protection en ligne des enfants dans tous les secteurs de la communauté, afin de prévenir les conséquences négatives probables et de promouvoir une utilisation positive d'Internet. Cette information sera largement diffusée, par des programmes spécifiques s'adressant à différents publics.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

8a. Créer un programme de sensibilisation du public

Les stratégies de sensibilisation aideront les personnes à comprendre et à gérer la question de la protection en ligne des enfants tout en profitant de l'espace virtuel. Les supports à produire doivent faire apparaître clairement les principes de la protection en ligne des enfants et les mesures à prendre pour comprendre les risques, limiter les dommages, signaler les infractions et demander réparation. Ces informations seront fournies en termes simples sur les sites Web officiels. Les messages et le matériel ciblés doivent être conçus en consultation avec les enfants, les jeunes et les parents/personnes en charge d'enfants. Ce plan doit prendre en compte les besoins spécifiques des parents/personnes en charge d'enfants et des enfants, en accordant une attention particulière aux enfants les plus jeunes et les plus vulnérables, y compris ceux qui ont des difficultés d'apprentissage ou ceux qui ne bénéficient pas de l'aide de leurs parents. L'enseignement de pair à pair est une stratégie bénéfique pour apprendre aux enfants de tous âges à connaître leurs droits et leurs responsabilités en ligne. Ce programme de messagerie publique peut aider les enfants et les adultes à comprendre les problèmes et à faire des choix judicieux au sujet de leurs interactions en ligne, mais ne remplace pas l'enseignement formel, la formation professionnelle, la conception sécuritaire ou la responsabilité de l'entreprise. Ces informations devront couvrir l'ensemble des questions de protection en ligne des enfants, telles que définies dans la présente politique.

257. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications

Les 5 thèmes transversaux

1. Identification des risques et atténuation des dommages
2. Promouvoir l'accès, l'accessibilité et l'inclusion
3. Instaurer une chaîne de responsabilité et de collaboration
4. Intégrer une conception axée sur l'enfant
5. Maintenir l'efficacité

Les dix domaines d'action politique

1. Capacité institutionnelle
2. Cadre juridique et réglementaire
3. Données personnelles, identité et autonomie
4. Systèmes de réponse et d'assistance
5. Responsabilité de l'entreprise
6. Formation
7. Enseignement
8. Sensibilisation du public et communications
9. Recherche et développement
10. Coopération internationale

8b. Fournir des informations accessibles et du matériel pédagogique

L'enseignement relatif à la protection en ligne commencera dès la petite enfance et se développera en fonction de l'évolution des besoins des enfants au fur et à mesure de leur croissance : des supports spécifiques seront produits pour guider et aider les enfants de tous âges, leurs familles et les personnes qui s'occupent d'eux. Les supports d'information encourageront l'utilisation positive de la technologie numérique, de la sexualité et du consentement, et tiendront compte des besoins de tous les enfants, quels que soient leur sexe, leur âge, leurs revenus ou leur origine. Les informations fournies par des tiers refléteront les droits et principes des enfants et viseront à aider les enfants de tous âges à se familiariser avec les risques et leurs droits en ligne. Les supports doivent indiquer clairement que les enfants et les utilisateurs ne sont pas responsables quand il leur arrive quelque chose de mal. Les groupes communautaires, les clubs de jeunes, les familles, les institutions religieuses et les plateformes numériques joueront tous un rôle déterminant dans la sensibilisation à la protection en ligne des enfants et l'enseignement informel au niveau communautaire.

8c. Sensibiliser les médias à la protection en ligne des enfants

Il convient de mettre à disposition des informations pour favoriser la couverture par les médias des questions de protection en ligne des enfants d'une manière adaptée à ces derniers. Les entreprises de médias et de divertissement devront être sensibilisées à la protection en ligne des enfants et être encouragées à soutenir les campagnes de sensibilisation du public, le cas échéant, de manière équilibrée, responsable et informative. Il est important d'encourager la prise en compte de l'ensemble des questions relatives à la protection en ligne des enfants, et pas seulement des gros titres les plus dramatiques à ce sujet.

8d. Faire participer les parents, les personnes en charge d'enfants et les enfants à des discussions sur la protection en ligne de ces derniers.

Les parents/les personnes en charge d'enfants et les familles doivent avoir les moyens de comprendre et d'agir sur la protection en ligne des enfants à leur domicile. Des consultations avec les familles et les enfants sont nécessaires pour identifier les problèmes, les solutions et les moyens de sensibiliser la communauté à la protection en ligne des enfants de manière efficace.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications

Feuille de route pour la mise en œuvre de la politique :

A **Créer un programme de sensibilisation du public**

Les stratégies de sensibilisation aideront les personnes à comprendre et à gérer la question de la protection en ligne des enfants tout en profitant de l'espace virtuel. Les supports à produire doivent faire apparaître clairement les principes de la protection en ligne des enfants et les mesures à prendre pour comprendre les risques, limiter les dommages, signaler les infractions et demander réparation. Ces informations seront fournies en termes simples sur les sites Web officiels.

Les messages et supports ciblés doivent être conçus en consultation avec les enfants, les jeunes et les personnes en charge d'enfants, et prendre en compte les besoins spécifiques des parents/personnes en charge d'enfants et des enfants, en accordant une attention particulière aux enfants les plus jeunes et les plus vulnérables, y compris ceux qui ont des difficultés d'apprentissage ou ceux qui ne bénéficient pas de l'aide de leurs parents. L'enseignement de pair à pair est une stratégie bénéfique pour apprendre aux enfants de tous âges à connaître leurs droits et leurs responsabilités en ligne. Ce programme de messagerie publique peut aider les enfants et les adultes à comprendre les problèmes et à faire des choix judicieux au sujet de leurs interactions en ligne, mais ne remplace pas l'enseignement formel, la formation professionnelle, la conception sécuritaire ou la responsabilité de l'entreprise. Ces informations devront couvrir l'ensemble des questions de protection en ligne des enfants, telles que définies dans la présente politique.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les publics clés et les interroger sur leurs perceptions et leurs questions.
2. Relever les messages essentiels à transmettre à chaque public. Voir l'outil d'assistance n° 1.
3. Réfléchir à la manière dont le message peut encourager une utilisation sûre du numérique, plutôt que de simplement choquer ou créer de l'anxiété.
4. Veiller à ce que les messages ne soient pas discriminatoires, par exemple en faisant croire que les filles ne devraient pas être connectées à Internet ou que les amitiés en ligne avec des personnes d'origines différentes sont dangereuses.
5. Collaborer avec les enfants et les parents/personnes en charge d'enfants pour développer ou tester votre message.
6. Analyser des exemples montrant que des publics différents requièrent des messages distincts.[258]

258. Voir par exemple Rwanda Child Online Protection Policy (Politique de protection en ligne des enfants au Rwanda), 5Rights Foundation, 2019.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

8 Sensibilisation du public et communications

B **Fournir des informations accessibles et du matériel pédagogique**

L'enseignement relatif à la protection en ligne commencera dès la petite enfance et se développera en fonction de l'évolution des besoins des enfants au fur et à mesure de leur croissance : des supports spécifiques seront produits pour guider et aider les enfants de tous âges, leurs familles et les personnes qui s'occupent d'eux. Les supports d'information encourageront l'utilisation positive de la technologie numérique et tiendront compte des besoins de tous les enfants, quels que soient leur sexe, leur âge, leurs revenus ou leur origine. Les informations fournies par des tiers refléteront les droits et principes des enfants et viseront à aider les enfants de tous âges à se familiariser avec leurs droits en ligne. Les supports doivent indiquer clairement que les enfants et les utilisateurs ne sont pas responsables quand il leur arrive quelque chose de mal. Les groupes communautaires, les clubs de jeunes, les familles, les institutions religieuses et les plateformes numériques joueront tous un rôle déterminant dans la sensibilisation à la protection en ligne des enfants et l'enseignement informel au niveau communautaire.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les publics clés.
2. Relever les messages essentiels à transmettre à chaque public.
3. Réfléchir à la manière dont le message peut encourager une utilisation sûre du numérique, plutôt que de simplement choquer ou créer de l'anxiété.
4. Veiller à ce que les messages ne soient pas discriminatoires, par exemple en faisant croire que les filles ne devraient pas être connectées à Internet ou que les amitiés en ligne avec des personnes d'origines différentes sont dangereuses.
5. Vérifier les exemples de différents publics et messages.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications

C **Sensibiliser les médias à la protection en ligne des enfants**

Il convient de mettre à disposition des informations pour favoriser la couverture par les médias des questions de protection en ligne des enfants d'une manière adaptée à ces derniers. Les entreprises de médias et de divertissement devront être sensibilisées à la protection en ligne des enfants et être encouragées à soutenir les campagnes de sensibilisation du public, le cas échéant, de manière équilibrée, responsable et informative. Il est important d'encourager la prise en compte de l'ensemble des questions relatives à la protection en ligne des enfants, et pas seulement des gros titres les plus dramatiques à ce sujet.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Veiller à ce que le ministère responsable et le comité de pilotage élaborent des messages clés et des indicateurs clés de performance sur la base de la boîte à outils pour la protection en ligne des enfants.
2. Développer une conscience et une intelligence des médias et développer une compréhension et une sensibilité au langage. Lorsque les ressources le permettent, entreprendre une formation aux médias.
3. Veiller à ce que ces messages soient partagés avec les médias grand public et spécialisés, afin d'encourager l'adhésion du public et d'assurer la transparence de la feuille de route, y compris ses succès et tout retard ou complication.
4. S'assurer que les principales parties prenantes et les dirigeants politiques sont prêts à promouvoir et à s'engager dans l'ensemble de la feuille de route pour la protection en ligne des enfants.[259]

259. Rwanda Child Online Protection Policy (Politique de protection en ligne des enfants au Rwanda), 5Rights Foundation, 2019.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications

D **Faire participer les parents, les personnes en charge d'enfants et les enfants à des discussions sur la protection en ligne de ces derniers.**

Les parents/les personnes en charge d'enfants et les familles doivent avoir les moyens de comprendre et d'agir sur la protection en ligne des enfants à leur domicile. Des consultations avec les familles et les enfants sont nécessaires pour identifier les problèmes et les moyens de sensibiliser la communauté à la protection en ligne des enfants de manière efficace.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les départements gouvernementaux, les ONG et les professionnels qui travaillent avec ou parlent directement aux enfants, aux familles et aux personnes en charge des enfants.
2. Leur offrir la possibilité de s'engager dans la feuille de route et de comprendre toute la portée et les possibilités qu'elle offre.
3. Faire entendre la voix des enfants, des parents et des personnes en charge d'enfants dans les documents d'information ou de supports de politique.
4. Fournir des messages clés destinés aux familles et aux personnes en charge d'enfants, qui répondent à leurs inquiétudes mais qui élargissent aussi leurs connaissances à une compréhension plus large de la sphère numérique ; recueillir les voix des enfants qui s'adressent directement aux parents et aux personnes en charge d'enfants.[260]

260. Our Rights in a Digital World (Nos droits dans un monde numérique), 5Rights Foundation, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications

Comment cela concorde avec les documents fondamentaux :

L'éventail des cibles des cyberattaques augmente rapidement. Les nouveaux internautes sont généralement peu sensibilisés à l'hygiène numérique. Plus de la moitié des attaques sont déjà dirigées contre des « objets » de l'Internet des Objets, qui relie tout, des téléviseurs intelligents aux babyphones en passant par les thermostats. Les réseaux 5G rapides intégreront davantage Internet aux infrastructures physiques, ce qui créera probablement de nouvelles vulnérabilités.

Source: The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation (L'ère de l'interdépendance numérique : rapport du Groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique) 2019[261]

Les États parties doivent veiller à ce que l'habileté numérique soit enseignée dans les écoles, dans le cadre des programmes d'enseignement de base, dès le niveau préscolaire et tout au long de la scolarité, et que ces pédagogies soient évaluées sur la base de leurs résultats. Les programmes d'études doivent inclure les connaissances et les compétences nécessaires pour manier en toute sécurité un large éventail d'outils et de ressources numériques, notamment ceux liés au contenu, à la création, à la collaboration, à la participation, à la socialisation et à l'engagement civique. Les programmes scolaires doivent également inclure une compréhension critique, des conseils sur la manière de trouver des sources d'information fiables et d'identifier l'information fausse ou trompeuse et d'autres formes de contenu biaisé ou faux, notamment sur les questions de santé sexuelle et reproductive, les droits de l'homme, y compris les droits de l'enfant dans l'environnement numérique, et les formes d'assistance et de recours disponibles. Ils doivent sensibiliser les enfants aux conséquences négatives possibles de l'exposition aux risques liés aux contenus, aux contacts, aux comportements et aux contrats, y compris les cyberagressions, la traite des êtres humains, l'exploitation et les abus sexuels et d'autres formes de violence, ainsi qu'aux stratégies d'adaptation permettant de réduire les dommages et aux stratégies visant à protéger leurs données à caractère personnel ainsi que celles d'autrui et à renforcer la résilience et les compétences sociales et émotionnelles des enfants.

Source : Observation générale n° 25 (2021), par. 104[262]

261. The Age of Digital Interdependence, UN Secretary-General's High-Level Panel on Digital Cooperation (L'ère de l'interdépendance numérique : groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique), 2019.
262. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

8 Sensibilisation du public et communications

Outils d'assistance :

1. Liste de contrôle pour s'assurer que le programme de sensibilisation est complet

Le processus A (« Générer un programme de sensibilisation du public ») nécessite l'élaboration d'un programme de sensibilisation générale capable de cibler certains publics très spécifiques. Cet outil est conçu pour vous aider à vous assurer que ces exigences sont respectées.

Groupe/public	Message principal pour les toucher
Enfants de moins de 12 ans	
Enfants de 12 à 18 ans	
Enfants vulnérables : - Sous protection - Avec des besoins supplémentaires - Avec des barrières linguistiques - Impliqués dans un contexte de justice pénale - Ceux qui sont en dehors du système d'enseignement ordinaire	
Familles ayant des problèmes d'accessibilité	
Familles rurales et éloignées	

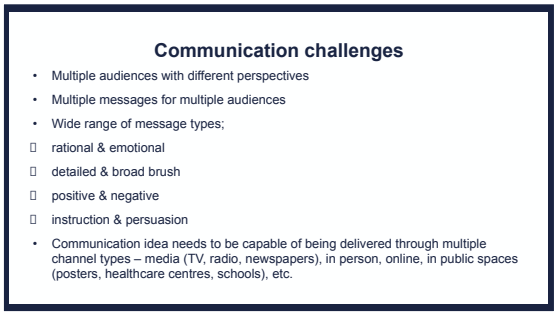
< SECTION PRÉCÉDENTE

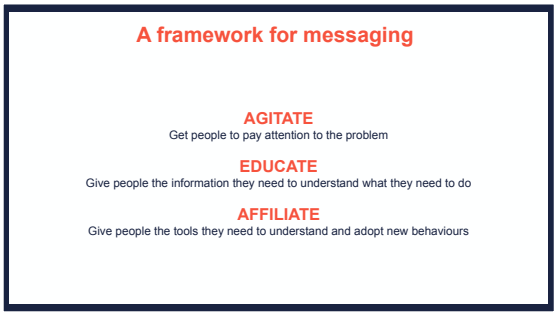
SECTION SUIVANTE >

8 Sensibilisation du public et communications

Autres ressources pour référence :

1. **Child Online Protection in Rwanda – Child Online Protection Communications (Protection en ligne des enfants au Rwanda : communications sur la protection en ligne des enfants)**[263]
   Travaillant pour le compte du gouvernement rwandais, 5Rights Foundation a préparé des supports de communication dans le cadre de la mise en œuvre de sa politique de protection en ligne des enfants.





263. Child Online Protection in Rwanda (Protection en ligne des enfants au Rwanda), 5Rights Foundation, 2019.

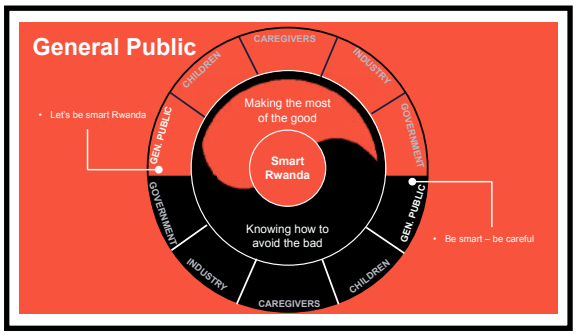
< SECTION PRÉCÉDENTE

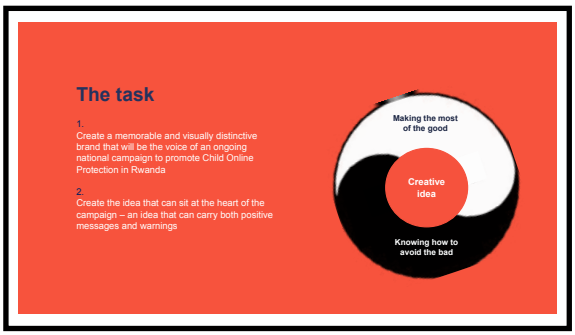
SECTION SUIVANTE >

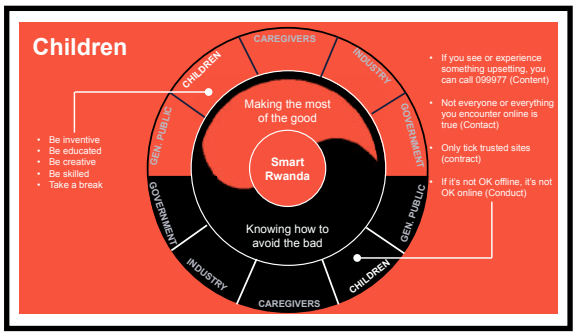
8 Sensibilisation du public et communication

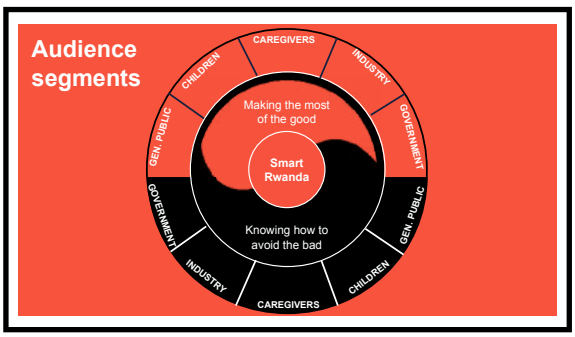
The right message will contain both silver lining and cloud

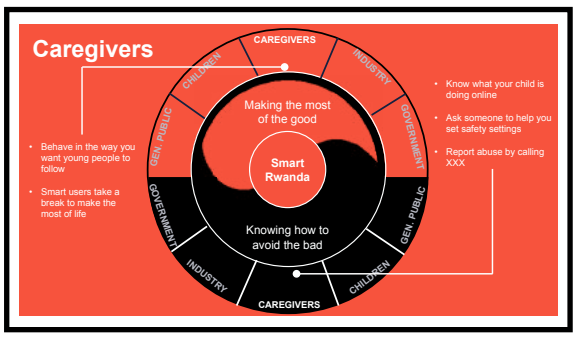
Messaging by segment (illustrative)







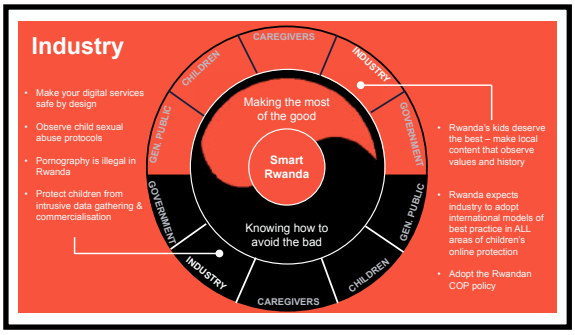


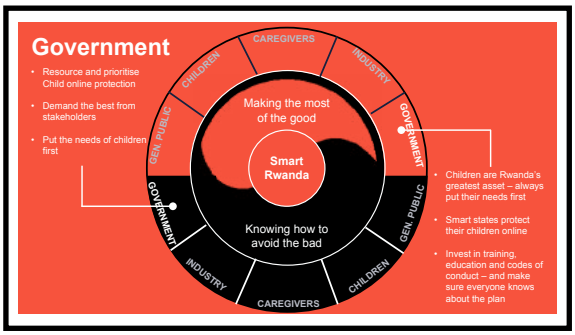


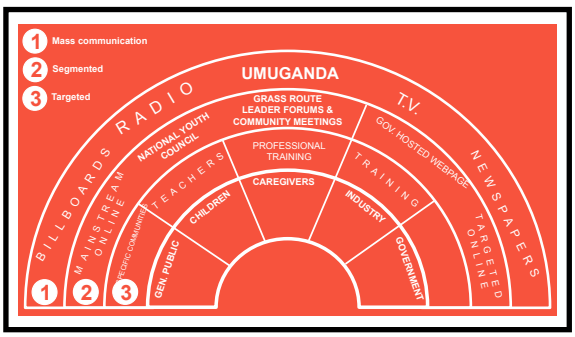
< SECTION PRÉCÉDENTE

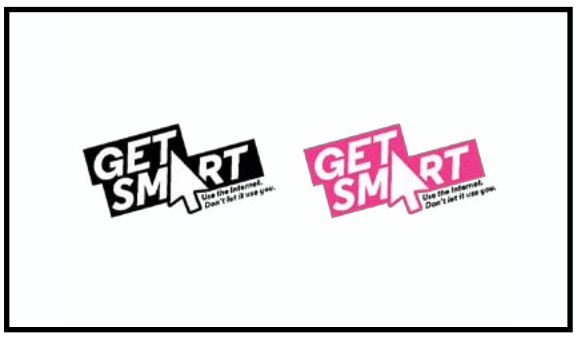
SECTION SUIVANTE >

8 Sensibilisation du public et communications



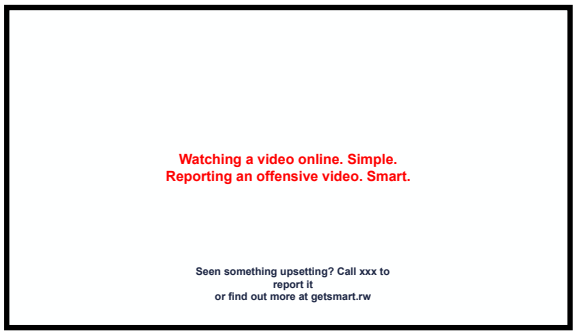






< SECTION PRÉCÉDENTE SECTION SUIVANTE >

8 Sensibilisation du public et communications



2. **Campagne Twisted Toys de 5Rights Foundation**[264]
   Cette campagne, lancée par la 5Rights Foundation, a permis de sensibiliser le public à tout type de surveillance et de danger auquel les enfants peuvent être confrontés lorsqu'ils explorent le monde numérique.

3. **Semaine mondiale de l'éducation aux médias et à l'information de l'UNESCO**[265]
   La Semaine mondiale de l'éducation aux médias et à l'information est un événement annuel qui permet de faire le point sur les progrès de l'habileté à utiliser les médias et l'information pour le public.

4. **Australian eSafety Commissioner's Global Tools for Parents (Outils mondiaux du commissaire australien à la sécurité électronique pour les parents)**[266]
   Ce document, préparé par le bureau du commissaire australien à la sécurité électronique, fournit des conseils aux personnes en charge d'enfants et aux parents pour les aider à protéger les enfants en ligne.

5. **The Council of Europe Digital Parenting Handbook (Le manuel de parentalité numérique du Conseil de l'Europe)**[267]
   Ce manuel, préparé par le Conseil de l'Europe, fournit des conseils aux personnes en charge d'enfants et aux parents pour assurer la protection en ligne des enfants, et notamment pour les protéger de l'exploitation et des abus sexuels.

6. **Goals of Africa Safer Internet Day 2021 with Sango the Mascot (Objectifs de la Journée africaine pour un internet plus sûr 2021 avec Sango la mascotte)**[268]
   Dans le but de créer un monde où les enfants peuvent être connectés et profiter pleinement des possibilités offertes par un environnement en ligne fiable et sûr, l'UIT a défini les objectifs suivants pour l'Afrique :

   - ☐ Promouvoir l'enseignement et la sensibilisation à l'échelle de l'Afrique sur l'importance de la protection en ligne des enfants.
   - ☐ Sensibiliser les gouvernements, l'industrie, les éducateurs, les enfants et les parents afin de garantir la sécurité de l'enfant africain en ligne.
   - ☐ Concevoir des stratégies visant à renforcer et à soutenir le développement de la résilience de l'enfant africain.
   - ☐ Développer, partager ou contextualiser les ressources disponibles pour soutenir l'apprentissage et l'enseignement des enfants.

264. Twisted Toys, 5Rights Foundation, 2021.
265. Global Media and Information Literacy Week (Semaine mondiale de l'éducation aux médias et à l'information), L'Organisation des Nations Unies pour l'éducation, la science et la culture, 2021.
266. Global Online Safety Advice for Parents and Carers (Conseils mondiaux de protection en ligne pour les parents et les personnes en charge d'enfants), eSafety Commissioner (Commissaire à la sécurité électronique), 2020.
267. Parenting in the Digital Age (Être parent à l'ère numérique), Conseil de l'Europe, 2017.
268. Positioning and Partnering for Child Online Protection (Positionnement et partenariat pour la protection en ligne des enfants), Bureau régional pour l'Afrique de l'Union internationale des télécommunications (UIT), 2021.

7. **Étude de cas : Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia**[269]
Le ministère colombien des technologies de l'information et des communications encourage le développement de compétences numériques pour faire face avec confiance aux risques liés à l'utilisation de l'internet et des TIC.

   Audience cible :

   - ☐ Enfants de 6 à 18 ans
   - ☐ Milieu académique de 11 à 28 ans
   - ☐ Adultes de 28 ans et plus

   Son site Web propose des liens vers des FAQ, des ressources de formation et d'enseignement ainsi que des informations accessibles sur le monde numérique.

8. **e-Learning course: Action to End Child Sexual Exploitation and Abuse (Cours e-Learning : action pour mettre fin à l'exploitation et aux abus sexuels des enfants)**[270]
Le cours Action to End Child Sexual Exploitation and Abuse (Action pour mettre fin à l'exploitation et aux abus sexuels des enfants) est un cours d'apprentissage en ligne conçu pour accroître la sensibilisation et les connaissances sur l'exploitation et les abus sexuels concernant les enfants, y compris les abus facilités par la technologie, et promouvoir des stratégies et des actions de prévention et de réponse fondées sur des données probantes. Le cours couvre la politique, la défense des intérêts et un large éventail d'aspects programmatiques. Cette étude et le cours d'apprentissage en ligne ont été produits avec le soutien financier du End Violence Fund (Fonds pour mettre fin à la violence).

9. **WeProtect Global Alliance How to talk about child sexual abuse in the digital world (Alliance mondiale WeProtect : comment parler de l'abus sexuel des enfants dans le monde numérique)**[271]
Cette note stratégique présente les défis à relever pour communiquer au sujet de l'exploitation et de l'abus sexuels concernant les enfants en ligne. Elle propose également des recommandations préliminaires à l'attention des communicateurs.

269. En TIC confío+, Ministère des technologies de l'information et des communications de Colombie, 2021.
270. Action to End Child Sexual Exploitation and Abuse (Action pour mettre fin à l'exploitation et aux abus sexuels des enfants), UNICEF, 2022.
271. How to talk about child sexual abuse in the digital world (Comment parler de l'abus sexuel des enfants dans le monde numérique ?), WeProtect Global Alliance, 2021.

« Aujourd'hui, à l'ère du numérique, les personnes... perdent leur vie privée. »

– Enfant vivant au Népal, 13 ans

« Les applications recueillent... vos données. Elles les vendent. Vous savez que vous êtes exposé, car vous recevez des publicités. »

– Enfant vivant en Norvège, 17 ans

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

9 Recherche et développement

> **Des données et des recherches régulièrement mises à jour sont essentielles pour comprendre les implications de l'environnement numérique sur la vie des enfants, évaluer son impact sur leurs droits et apprécier l'efficacité des interventions de l'État. Les États parties doivent veiller à recueillir des données fiables et complètes, dotées de ressources suffisantes et réparties en fonction de l'âge, du sexe, de la situation de handicap, de l'emplacement géographique, de l'origine ethnique et nationale et du contexte socio-économique. De telles données et recherches, y compris celles menées avec et par les enfants, devraient alimenter la législation, les politiques ainsi que les pratiques et devraient être disponibles dans le domaine public. Le recueil de données et la recherche concernant la vie numérique des enfants doivent respecter leur vie privée et répondre aux normes éthiques les plus élevées.**
>
> Source : Observation générale n° 25 (2021), par. 30[272]

Objectif :

Pour garantir une approche holistique et actualisée de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

Texte de politique modèle :

Établir et financer des cadres de recherche et de développement sur la protection en ligne des enfants efficaces et accessibles au public, à l'échelle nationale et régionale, afin de soutenir l'élaboration et la mise en œuvre de politiques relatives à la protection en ligne des enfants.

9a. Établir des cadres de recherche sur la protection en ligne des enfants
Les pays doivent établir un fonds de recherche central pour développer un programme de recherche avec des termes de référence clairement identifiés et des objectifs qui restent d'actualité, afin de permettre une recherche continue sur la protection en ligne des enfants sur une large gamme de questions pertinentes. Dans la mesure du possible, les pays doivent s'entraider et coopérer en matière de recherche et de développement sur la protection en ligne des enfants. L'analyse des lacunes doit permettre de garantir que les ressources sont affectées en priorité aux domaines où les besoins sont les plus importants et d'éviter les redondances inutiles. La recherche doit être mise à la disposition des partenaires régionaux ou internationaux, en particulier ceux qui ont le moins de ressources.

9b. Innovation continue
Les résultats de la recherche permettront de développer des produits et des services intégrant une conception sécuritaire, d'évaluer les pratiques de protection en ligne des enfants et de comprendre les expériences et les solutions en ligne des enfants dans le contexte national. ▶

272. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

9 Recherche et développement

9c. Créer des centres d'excellence en matière de recherche et de développement sur la protection en ligne des enfants
Les pays devront développer des centres d'excellence au sein des institutions existantes (universités, établissements de santé, centres d'innovation) qui peuvent partager et coopérer au développement d'outils, de services et de compétences liés à la protection en ligne des enfants par le biais d'un engagement national, régional et international.

9d. Établir des cadres éthiques solides en recherche et développement en matière de protection en ligne des enfants[273]
Les pays devront élaborer des lignes directrices à l'attention des chercheurs travaillant sur la protection en ligne des enfants, y compris la prise en compte effective des droits de l'enfant dans le cadre du processus de recherche. Cela doit inclure des conseils clairs sur le recueil des données et les implications éthiques et en termes de droits du traitement des données des enfants. L'intérêt de l'enfant doit être la principale préoccupation dans les cadres éthiques de recherche et de développement sur la protection en ligne des enfants, y compris dans les situations d'accès d'intérêt public.

9e. Établir des cadres pour la collecte d'informations
Les régulateurs travaillant dans le domaine de la protection en ligne des enfants doivent mettre en place des cadres pour la collecte d'informations qui leur permettront de suivre et d'évaluer l'efficacité de la protection en ligne des enfants dans différents contextes et l'impact qu'elle a sur différents groupes d'enfants. Le suivi et l'évaluation des actions en faveur de la protection en ligne des enfants doivent faire partie du processus de recherche et de développement.

9f. Permettre l'accès aux données des entreprises privées dans l'intérêt public
Il convient de créer des cadres dans lesquels les médias sociaux et autres entreprises doivent partager leurs données pour soutenir la recherche dans les meilleurs intérêts de l'enfant.

9g. Veiller à ce que les données et les statistiques soient pertinentes dans le contexte
Les modèles statistiques doivent refléter la situation locale, afin de favoriser le niveau de compréhension et de réponse aux problèmes nationaux. Ils doivent permettre le suivi des impacts transfrontaliers.

273. Children and the Data Cycle: Rights and Ethics in a Big Data World (Les enfants et le cycle des données : droits et éthique dans un monde de Big Data), Fonds des Nations Unies pour l'enfance, 2017.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

9 Recherche et développement

Feuille de route pour la mise en œuvre de la politique :

A **Établir des cadres de recherche sur la protection en ligne des enfants**

Les pays doivent établir un fonds de recherche central pour développer un programme de recherche avec des termes de référence clairement identifiés et des objectifs qui restent d'actualité, afin de permettre une recherche continue sur la protection en ligne des enfants sur une large gamme de questions pertinentes. Dans la mesure du possible, les pays doivent s'entraider et coopérer en matière de recherche et de développement sur la protection en ligne des enfants. L'analyse des lacunes doit permettre de garantir que les ressources sont affectées en priorité aux domaines où les besoins sont les plus importants et d'éviter les redondances inutiles. La recherche doit être mise à la disposition des partenaires régionaux ou internationaux, en particulier ceux qui ont le moins de ressources.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les fonds de recherche existants ou les institutions qui pourraient héberger ou financer des recherches sur la protection en ligne des enfants.
2. Définir le domaine de recherche requis.
3. Établir des critères stricts pour garantir que la recherche contribue à l'alphabétisation, à la sécurité et au bien-être des enfants.
4. Veiller à ce que les personnes qui entreprennent des recherches soient conscientes de tous les domaines de la feuille de route en matière de politique et ne se concentrent pas uniquement sur un seul aspect.
5. Faire dépendre tout financement de la recherche d'un large partage des résultats, notamment en conservant les résultats de la recherche dans un répertoire central et en dégageant des fonds pour la diffusion et la mise en œuvre des politiques.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

9 Recherche et développement

B **Innovation continue**

Les résultats de la recherche permettront de développer des produits et des services intégrant une conception sécuritaire, d'évaluer les pratiques de protection en ligne des enfants et de comprendre les expériences en ligne des enfants dans le contexte national.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Cartographier les changements, à l'échelle mondiale, apportés aux produits et services et les partager largement, afin de garantir que les progrès réalisés en matière de sécurité des enfants dans une partie du monde soient disponibles dans d'autres régions de la planète.
2. Dresser la carte des progrès accomplis et impliquer les ONG internationales ou les groupes d'experts pour faciliter leur diffusion.
3. Tirer parti des accords avec les organisations intergouvernementales, les entreprises privées et les ONG pour diffuser les bonnes pratiques. Par exemple, le don de matériel informatique doit être subordonné à l'intégration par défaut de fonctionnalités assurant la sécurité et le respect de la vie privée.

C **Créer des centres d'excellence en matière de recherche et de développement sur la protection en ligne des enfants**[274]

Les pays doivent mettre en place des pôles de protection en ligne pour les enfants qui peuvent partager et coopérer au développement d'outils, de services et de compétences relatifs à la protection en ligne des enfants par le biais d'un engagement national, régional et international.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Installer des pôles de protection en ligne pour les enfants dans les ministères ou les établissements universitaires existants.
2. Envisager la mise en place de pôles de protection en ligne pour les enfants dans les régions ayant des exigences culturelles et organisationnelles similaires, afin de partager les meilleures pratiques.

274. Child Safety Online Global Challenges and Strategies (Défis et stratégies mondiaux en matière de sécurité des enfants en ligne), Fonds des Nations Unies pour l'enfance, 2011.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

9 Recherche et développement

D **Établir des cadres éthiques solides en recherche et développement en matière de protection en ligne des enfants**[275]

Les pays devront élaborer des lignes directrices à l'attention des chercheurs travaillant sur la protection en ligne des enfants, y compris la prise en compte effective des droits de l'enfant dans le cadre du processus de recherche. Cela doit inclure des directives claires sur la collecte des données et les implications sur l'éthique et les droits de traitement des données des enfants. L'intérêt de l'enfant doit être la principale préoccupation dans les cadres éthiques de recherche et de développement sur la protection en ligne des enfants, y compris dans les situations d'accès d'intérêt public.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Établir des normes minimales de recherche responsable (voir les ressources ci-dessous, par exemple les lignes directrices d'ECPAT).
2. Veiller à ce que les normes soient intégrées dans le financement ou l'acceptation des résultats de la recherche. Voir les outils d'assistance n° 1 (page n° 156).
3. Veiller à ce que la formation à la sécurité des enfants soit obligatoire pour les chercheurs (voir le domaine d'action politique relatif à la Formation, page n° 144).

E **Établir des cadres pour la collecte d'informations**

Les régulateurs travaillant dans le domaine de la protection en ligne des enfants doivent mettre en place des cadres pour la collecte d'informations qui leur permettront de suivre et d'évaluer l'efficacité de la protection en ligne des enfants dans différents contextes et l'impact qu'elle a sur différents groupes d'enfants. Le suivi et l'évaluation des actions en faveur de la protection en ligne des enfants doivent faire partie du processus de recherche et de développement.

Dans l'affirmative, veuillez préciser :

Dans la négative, cela contribuera à garantir que les régulateurs exigent des cadres de collecte d'informations pour comprendre les éléments, les méthodes et les résultats. Toute exigence légale ou réglementaire doit inclure des pouvoirs de signalement, de transparence et de collecte d'informations. Le RGPD[276] et le projet de loi britannique sur la protection en ligne en sont des exemples.[277]

275. Children and the Data Cycle: Rights and Ethics in a Big Data World (Les enfants et le cycle des données : droits et éthique dans un monde de Big Data), Fonds des Nations Unies pour l'enfance, 2017.
276. Règlement général sur la protection des données, Union européenne, 2018.
277. Projet de loi sur la protection en ligne, Ministère du numérique, de la culture et des médias, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

9 Recherche et développement

F **Permettre l'accès aux données des entreprises privées dans l'intérêt public**

Il convient de créer des cadres dans lesquels les médias sociaux et autres entreprises doivent partager leurs données pour soutenir la recherche dans les meilleurs intérêts de l'enfant.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Mener des actions de sensibilisation auprès des entreprises de médias sociaux sur le territoire concerné, en requérant l'accès aux ensembles de données, le cas échéant.
2. Se joindre à des conversations régionales, nationales ou mondiales formulant des demandes similaires.

G **Veiller à ce que les données et les statistiques soient pertinentes dans le contexte**

Les régulateurs travaillant dans le domaine de la protection en ligne des enfants doivent mettre en place des cadres pour la collecte d'informations qui leur permettront de suivre et d'évaluer l'efficacité de la protection en ligne des enfants dans différents contextes et l'impact qu'elle a sur différents groupes d'enfants. Le suivi et l'évaluation des actions en faveur de la sécurité des enfants en ligne doivent faire partie du processus de recherche et développement.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Rechercher et trouver des statistiques provenant d'organismes bien documentés et réputés.
2. Collaborer avec les parties prenantes de ces agences pour valider et confirmer vos statistiques.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

9 Recherche et développement

Comment cela concorde avec les documents fondamentaux :

Capacité 2. Modèle de réponse nationale : recherche, analyse et suivi des bonnes pratiques en matière de respect de la loi :

Au minimum, une analyse devrait : évaluer la menace actuelle de l'exploitation et des abus sexuels sur mineur, comment elle se manifeste et qui est le plus à risque ; évaluer la vulnérabilité du pays à cette menace ; évaluer la réponse institutionnelle actuelle ; examiner et évaluer la mise en œuvre de la législation et des politiques applicables pour évaluer la conformité avec les normes internationales et les bonnes pratiques ; examiner la réponse actuelle de l'écosystème des TIC, y compris les mécanismes de signalement de la ligne d'assistance téléphonique et l'engagement de l'industrie ; cartographier l'activité des autres parties prenantes engagées dans cette question.

Pour éclairer une analyse, il est nécessaire d'avoir accès à un large éventail de données et d'informations relatives à l'exploitation et aux abus sexuels sur mineur provenant des organisations représentées au sein de l'organisme national et de toute autre partie prenante concernée. En outre, les données primaires doivent être recueillies auprès de diverses sources telles que les enfants, les parents, les éducateurs, les responsables de l'application de la loi et les fournisseurs de services.

Source : WeProtect Global Alliance Model National Response (Modèle de réponse nationale de WeProtect Global Alliance, MNR), pages 5-6[278]

278. Model National Response (Modèle de réponse nationale), WeProtect Global Alliance, 2016.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

9 Recherche et développement

Outils d'assistance :

1. Liste de contrôle des considérations relatives à l'éthique de la recherche

Le processus D (« Établir des cadres éthiques solides en recherche et développement en matière de protection en ligne des enfants ») souligne la nécessité de réfléchir de manière holistique à l'éthique de la recherche en matière de méthodologie, de financement et de recueil de données. Cette liste de contrôle est conçue pour vous aider à vous assurer que vos cadres d'éthique de la recherche abordent ces domaines.

La sélection des recherches à financer par le gouvernement tient-elle compte de la sécurité des enfants en ligne ?

Dans l'affirmative, veuillez préciser :

Dans la négative, comment cette question sera-t-elle traitée ?

Le financement de la recherche comprend-il une évaluation de l'impact sur l'enfant ou un contrôle éthique ?

Dans l'affirmative, veuillez préciser :

Dans la négative, comment cette question sera-t-elle traitée ?

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

9 Recherche et développement

Existe-t-il un cadre éthique pour les chercheurs et les développeurs incluant les perspectives des droits de l'enfant ?

Dans l'affirmative, veuillez préciser :

Dans la négative, comment cette question sera-t-elle traitée ?

Les chercheurs, les développeurs et les décideurs en matière de financement sont-ils formés à la sécurité des enfants en ligne et aux droits de l'enfant ?

Dans l'affirmative, veuillez préciser :

Dans la négative, comment cette question sera-t-elle traitée ?

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

9 Recherche et développement

Le principe de précaution s'applique-t-il à la recherche et au développement ?

Dans l'affirmative, veuillez préciser :

Dans la négative, comment cette question sera-t-elle traitée ?

Des données en libre accès sont-elles disponibles pour favoriser la recherche sur la sécurité des enfants en ligne ?

Dans l'affirmative, veuillez préciser :

Dans la négative, comment cette question sera-t-elle traitée ?

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

9 Recherche et développement

Autres ressources pour référence :

1. **University of Oxford – Framework for Responsible Research and Innovation in ICT (Université d'Oxford - Cadre pour une recherche et une innovation responsables dans le domaine des TIC)**[279]
   Financé par l'Engineering and Physical Sciences Research Council (EPSRC), ce cadre étudie les questions d'éthique dans la recherche sur les TIC. Préparé par l'Observatory for Responsible Research and Innovation in ICT (Observatoire pour la recherche et l'innovation responsables dans les TIC, ORBIT), il fournit des instructions claires sur la manière de mener une recherche pratique et éthique.

2. **End Violence Partnership – Disrupting Harm (Partenariat End Violence : Disrupting Harm)**[280]
   En partenariat avec ECPAT International, INTERPOL et le Bureau de la recherche de l'UNICEF, ainsi qu'avec le financement du Partenariat End Violence, Disrupting Harm est un projet de recherche qui examine comment la technologie numérique facilite l'exploitation et les abus sexuels des enfants dans 13 pays d'Afrique orientale et australe et d'Asie du Sud-Est.

3. **ECPAT Guidelines for Ethical Research on the Sexual Exploitation of Children (Lignes directrices d'ECPAT pour une recherche éthique sur l'exploitation sexuelle des enfants)**[281]
   Il s'agit d'un guide destiné aux chercheurs souhaitant mener des recherches sur des questions liées à l'exploitation et aux abus sexuels concernant des enfants, qui soulèvent certaines questions et certains dilemmes éthiques. Ces directives aident les chercheurs à élaborer leur projet de recherche de manière à réduire les dommages causés aux enfants au minimum.

4. **EU Fundamental Rights Agency Opinion (Avis de l'Agence des droits fondamentaux de l'UE)**[282]
   Avis 9 de l'Agence des droits fondamentaux : lorsqu'ils financent des activités de recherche et de développement, l'UE et ses États membres doivent exiger des contractants qu'ils fassent appel à des experts en matière de protection des données à caractère personnel et d'autres droits fondamentaux. Les chercheurs scientifiques et l'industrie doivent être attentifs à l'effet des caractéristiques phénotypiques, ainsi que de l'âge et du sexe, sur la composition des groupes témoins, afin d'éliminer tout risque de discrimination dans les résultats des tests.

5. **UN Office of the High Commissioner for Human Rights – Guidance on a Human Rights Based Approach to Data (Haut Commissariat des Nations Unies aux droits de l'homme : guide pour une approche des données fondée sur les droits de l'homme)**[283]
   Le présent guide fournit des recommandations et des principes aux parties prenantes et aux responsables politiques pour améliorer leur utilisation des données et des statistiques. Il garantit le respect, la protection et la réalisation des droits de l'homme sur la base de l'Agenda 2030 adopté lors du recueil ou de la désagrégation des données.

279. A Framework for Responsible Research and Innovation in ICT (Un cadre pour une recherche et une innovation responsables dans le domaine des TIC), University of Oxford, 2014.
280. Disrupting Harm, End Violence Partnership, 2019.
281. Guidelines for ethical research on sexual exploitation involving children (Lignes directrices pour une recherche éthique sur l'exploitation sexuelle concernant les enfants), ECPAT International, 2019.
282. Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights (Sous haute surveillance : biométrie, systèmes informatiques et droits fondamentaux de l'UE), Agence des droits fondamentaux de l'Union européenne, 2018.
283. A Human Rights-Based Approach to Data (Une approche des données basée sur les droits de l'homme), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2018.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

« Il est plus facile aujourd'hui de pirater les gens et d'obtenir des informations sensibles sans leur consentement grâce aux technologies numériques. »

– Enfant vivant au Pakistan, 12 ans

« Pourquoi [les sites Web et les médias sociaux] me demandent-ils mes informations personnelles si ces dernières ne sont utilisées à aucune fin ? »

– Enfant vivant aux Émirats arabes unis, 17 ans

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

10 Coopération internationale

La nature transfrontalière et transnationale de l'environnement numérique requiert une forte coopération internationale et régionale, afin de garantir que toutes les parties prenantes, y compris les États, les entreprises et les autres acteurs, respectent, protègent et appliquent effectivement les droits de l'enfant en relation avec l'environnement numérique. Il est donc essentiel que les États parties coopèrent bilatéralement et multilatéralement avec les organisations non gouvernementales nationales et internationales, les agences des Nations Unies, les entreprises et les organisations spécialisées dans la protection de l'enfance et les droits de l'homme en relation avec l'environnement numérique.

Les États parties doivent promouvoir et contribuer à l'échange international et régional d'expertise et de bonnes pratiques ainsi que mettre en place et promouvoir le renforcement des capacités, les ressources, les normes, les réglementations et les protections au-delà des frontières nationales qui permettent la mise en œuvre des droits de l'enfant dans l'environnement numérique par tous les États. Ils doivent encourager la création d'une définition commune de ce qui constitue un crime dans l'environnement numérique, l'assistance juridique mutuelle et la collecte et le partage conjoints de preuves.

Source : Observation générale n° 25 (2021), par. 123 et 124[284]

Objectif :

Collaborer avec les organisations et acteurs nationaux, régionaux et mondiaux pour partager les meilleures pratiques.

Texte de politique modèle :

Pour garantir une approche holistique de la protection en ligne des enfants, chacune des étapes ci-dessous est nécessaire.

10a. Établir des cadres de relations formels (par exemple, un mémorandum d'entente) avec les communautés régionales et mondiales de la sécurité des enfants en ligne
Le renforcement de la coopération internationale pour améliorer la protection en ligne des enfants dans le monde entier est essentiel pour garantir la sécurité mondiale. Les pays doivent formaliser des collaborations pour des investissements conjoints en partenariat public et privé dans des domaines liés à la cybersécurité, au renforcement des capacités en matière de sécurité des enfants en ligne, à l'innovation, à l'application de la loi, au système judiciaire et à l'enseignement, entre autres.

10b. Approuver les instruments juridiques régionaux et internationaux qui encouragent la coopération en matière de sécurité des enfants en ligne
Les pays doivent identifier les principaux instruments régionaux et internationaux qui leur permettront de coopérer avec d'autres pays en matière de sécurité des enfants en ligne. Cela concerne, entre autres, les accords internationaux sur la coopération en matière d'application de la loi, les meilleures pratiques internationales, les programmes internationaux susceptibles de fournir des ressources pour la coopération en matière de protection en ligne des enfants, et l'accès à tous les droits de l'homme ou normes connexes qui faciliteront la coopération entre les pays. ▶

284. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

10 Coopération internationale

10c. Identifier les pays et organisations partenaires qui peuvent fournir des modèles et une assistance appropriés pour le développement de la protection en ligne des enfants
Il n'est peut-être pas nécessaire de recommencer l'élaboration de la politique depuis le début. Les pays sont invités à rechercher des exemples pertinents de cadres et d'outils de protection en ligne pour les enfants qu'ils peuvent utiliser et adapter à leur propre contexte. Le partage d'informations sur les défis et les problèmes rencontrés dans le domaine de la protection en ligne des enfants peut s'avérer très précieux pour la planification, l'élaboration et la mise en œuvre des politiques de protection en ligne des enfants.

10d. Accompagner les autres pays dans l'élaboration de politiques de protection en ligne des enfants
Le cas échéant, partager des lois modèles, des cadres réglementaires, des leçons apprises ou d'autres supports qui peuvent être utilisés par d'autres pays pour développer leurs propres cadres et politiques de protection en ligne des enfants.[285]

Feuille de route pour la mise en œuvre de la politique :

A **Établir des cadres de relations formels (par exemple, un mémorandum d'entente) avec les communautés régionales et mondiales de la sécurité des enfants en ligne**

Le renforcement de la coopération internationale pour améliorer la protection en ligne des enfants dans le monde entier est essentiel pour garantir la sécurité mondiale. Les pays doivent formaliser des collaborations pour des investissements conjoints en partenariat public et privé (PPP) dans des domaines liés à la cybersécurité, au renforcement des capacités en matière de sécurité des enfants en ligne, à l'innovation, à l'application de la loi, au système judiciaire et à l'enseignement, entre autres.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier les accords et traités régionaux et mondiaux pertinents en matière de protection en ligne des enfants (voir Documents clés).
2. Prendre des dispositions pour adhérer et ajouter les étapes nécessaires à votre feuille de route pour la protection en ligne des enfants.
3. Vérifier que celles-ci comprennent, au minimum, toutes les actions requises telles que définies par :
   - ☐ Les objectifs de développement durable[286]
   - ☐ La convention relative aux droits de l'enfant et ses protocoles facultatifs[287]
   - ☐ L'observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique.[288]
   - ☐ Modèle de réponse nationale.[289] Voir l'outil d'assistance n° 1 (page n° 109).

285. Voir par exemple le Australian eSafety Commissioner's International Leadership and Collaboration Materials (Supports pour le leadership et la collaboration internationale du commissaire australien à la cybersécurité), 2021.
286. Transforming our world: the 2030 Agenda for Sustainable Development (Transformer notre monde : l'Agenda 2030 pour le développement durable), Nations Unies, 2021.
287. Convention on the Rights of the Child (Convention sur les droits de l'enfant), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 1989.
288. Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, Comité des droits de l'enfant des Nations Unies, 2021.
289. Model National Response (Modèle de réponse nationale), WeProtect, 2016.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

10 Coopération internationale

B **Approuver les instruments juridiques régionaux et internationaux qui encouragent la coopération en matière de protection en ligne des enfants**

Les pays doivent identifier les principaux instruments régionaux et internationaux qui leur permettront de coopérer avec d'autres pays en matière de sécurité des enfants en ligne. Cela concerne, entre autres, les accords internationaux sur la coopération en matière d'application de la loi, les meilleures pratiques internationales, les programmes internationaux susceptibles de fournir des ressources pour la coopération en matière de protection en ligne des enfants, et l'accès à tous les droits de l'homme ou normes connexes qui faciliteront la coopération entre les pays.

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Consulter les organismes internationaux chargés de faire respecter la loi, tels qu'INTERPOL[290] et Europol.[291]
2. Rechercher les meilleures pratiques auprès d'organisations mondiales telles que le National Center for Missing & Exploited Children[292] et Internet Watch Foundation.[293]

290. Qui nous sommes, INTERPOL.
291. About Europol, Europol.
292. Notre travail, National Center for Missing and Exploited Children (NCMEC).
293. À propos de nous, Internet Watch Foundation (IWF).

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

10 Coopération internationale

C **Identifier les pays et organisations partenaires qui peuvent fournir des modèles et une assistance appropriés pour le développement de la protection en ligne des enfants**

Il n'est peut-être pas nécessaire de recommencer l'élaboration de la politique depuis le début. Les pays sont invités à rechercher des exemples pertinents de cadres et d'outils de protection en ligne pour les enfants qu'ils peuvent utiliser et adapter à leur propre contexte. Le partage d'informations sur les défis et les problèmes rencontrés dans le domaine de la protection en ligne des enfants peut s'avérer très précieux pour la planification, l'élaboration et la mise en œuvre des politiques de protection en ligne des enfants.

Dans l'affirmative, veuillez préciser :

Dans la négative, il est utile de s'adresser à des organismes régionaux, tels que la Child Rights Coalition Asia[294], à des responsables nationaux, tels que la Fondation Alana au Brésil,[295] ou à des organisations spécialisées, telles que l'Internet Watch Foundation (fondation pour la surveillance d'Internet),[296] la 5Rights Foundation,[297] l'UNICEF,[298] INHOPE[299] ou l'initiative Safe Online du Partenariat mondial pour mettre fin à la violence contre les enfants.[300]Ces organisations disposent de ressources et d'informations et, dans de nombreux cas, peuvent vous aider à identifier des partenaires locaux ou pertinents.

294. À propos de nous, Child Rights Coalition Asia.
295. À propos de nous, Fondation Alana.
296. À propos de nous, Internet Watch Foundation (IWF).
297. 5Rights Foundation, 5Rights Foundation.
298. À propos de nous, UNICEF.
299. Notre histoire, INHOPE, 2021.
300. Safe Online, End Violence Against Children, 2022.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

10 Coopération internationale

D **Accompagner les autres pays dans l'élaboration de politiques de protection en ligne des enfants**

Le cas échéant, partager des lois modèles, des cadres réglementaires, des leçons apprises ou d'autres supports qui peuvent être utilisés par d'autres pays pour développer leurs propres cadres et politiques de protection en ligne des enfants.[301]

Dans l'affirmative, veuillez préciser :

Dans la négative, il sera utile de suivre ces mesures :

1. Identifier d'autres organisations ou ministères en charge dans votre région.
2. Examiner les meilleures pratiques d'autres régions, par exemple l'Association des nations de l'Asie du Sud-Est (ANASE) ou l'UE.
3. Partager généreusement vos ressources et vos solutions.
4. Réfléchir à la manière dont vous pourriez former des partenariats avec ceux qui ont moins de ressources.
5. Encourager les destinataires à partager leurs connaissances.
6. Se conformer aux meilleures pratiques internationales et chercher de manière proactive à partager avec les pays disposant de moins de ressources ou à leur donner les moyens de le faire : par exemple, en se jumelant avec un pays ou une région particulière, en offrant une assistance technique telle que la traduction juridique ou linguistique de certaines parties de la feuille de route, ou en organisant des ateliers destinés aux travailleurs de première ligne, y compris en ce qui concerne la mise en œuvre.

Comment cela concorde avec les documents fondamentaux :

Nous recommandons que, de toute urgence, le Secrétaire général de l'ONU facilite un processus de consultation souple et ouvert afin de développer des mécanismes actualisés pour la coopération numérique mondiale, avec les options discutées au chapitre 4 comme point de départ. Nous suggérons un objectif initial qui consisterait à marquer le 75e anniversaire des Nations Unies en 2020 par un « engagement mondial pour la coopération numérique » afin de concrétiser des valeurs, des principes, des compréhensions et des objectifs communs pour une architecture de coopération numérique mondiale améliorée. Dans le cadre de ce processus, nous croyons savoir que le Secrétaire général des Nations Unies pourrait nommer un Envoyé pour les technologies.

5B : nous encourageons une approche « systémique » multipartite de la coopération et de la réglementation, qui soit adaptative, souple, inclusive et adaptée à l'évolution rapide de l'ère numérique.

Source: The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation (L'ère de l'interdépendance numérique : rapport du Groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique) 2019[302]

301. Voir, par exemple, les Supports de leadership et de collaboration internationale du commissaire australien à la cybersécurité.
302. The Age of Digital Interdependence, UN Secretary-General's High-Level Panel on Digital Cooperation (L'ère de l'interdépendance numérique : groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique), 2019.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

10 Coopération internationale

Outils d'assistance :

1. Liste de contrôle des cadres internationaux à respecter

Le processus A (« Établir des cadres de relations formelles [par exemple, des mémorandums d'entente] avec les communautés régionales et mondiales de la protection en ligne des enfants ») indique que les exigences minimales d'une série de protocoles internationaux et de documents sur les meilleures pratiques doivent être respectées. Les ministères en charge doivent travailler à l'échelle du gouvernement avec l'aide de cet outil pour évaluer la conformité.

	Décrire la façon dont les exigences minimales sont respectées	**Lacunes en matière de conformité**	**Date à laquelle le ministère responsable est informé de ces lacunes**	**Date à laquelle le groupe de parties prenantes de la protection en ligne des enfants est informé de ces lacunes**
Objectifs de développement durable de l'ONU				
Convention des Nations Unies sur les droits de l'enfant				
CRC Optional Protocol: Involvement of children in armed conflict (Protocole facultatif de la CDE : implication des enfants dans les conflits armés)				
Vente d'enfants, prostitution des enfants et pornographie impliquant des enfants				
Procédure relative aux communications				

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

10 Coopération internationale

	Décrire la façon dont les exigences minimales sont respectées	Lacunes en matière de conformité	Date à laquelle le ministère responsable a été informé de ces lacunes ?	Date à laquelle le groupe de parties prenantes de la protection en ligne des enfants est informé de ces lacunes ?
Observation générale n° 25 (2021)	☑			
Réponse nationale modèle				
Luxembourg Guidelines (lignes directrices du Luxembourg) sur la terminologie pour la protection des enfants contre l'exploitation et les abus sexuels				

Autres ressources pour référence :

Cadres destinés à soutenir la coopération internationale

1. **Feuille de route des Nations Unies pour la coopération numérique**[303]
   La feuille de route du secrétaire général pour la coopération numérique,[304] soutenue par un groupe de haut niveau sur la coopération numérique, a été publiée en 2020. Elle fournit des recommandations aux différentes parties prenantes sur le renforcement de la coopération numérique mondiale.

2. **Ressource Web d'INTERPOL sur les crimes contre les enfants**[305]
   Le site Web d'INTERPOL propose une palette de ressources, notamment des informations sur le travail d'INTERPOL, ainsi que des informations sur la base de données en ligne en matière d'exploitation et d'abus sexuels sur mineur, le blocage et la catégorisation des contenus, et l'identification des victimes.

3. **Recommandation du Conseil de l'OCDE sur les enfants dans l'environnement numérique**[306]
   La Recommandation définit des principes et des orientations visant à guider les pays dans la recherche d'un équilibre entre la protection des enfants contre les risques en ligne et la promotion des opportunités et des avantages qu'offre le monde numérique.

303. Feuille de route du Secrétaire général des Nations Unies pour la coopération numérique, Nations Unies, 2020.
304. Groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique, Nations Unies, 2020.
305. Crimes contre les enfants, INTERPOL.
306. Recommandation du Conseil sur les enfants dans l'environnement numérique, OCDE, adoptée en 2012, modifiée en 2021.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

10 Coopération internationale

Autres ressources pour référence :

Cadres pour favoriser la coopération régionale

1. **African Union Malabo Convention on Cyber Security and Personal Data Protection (Convention de Malabo de l'Union africaine sur la cybersécurité et la protection des données personnelles) 2014**[307]
   Il s'agit de la convention de l'Union africaine visant à créer un « cadre crédible pour la cybersécurité en Afrique par l'organisation des transactions électroniques, la protection des données personnelles, la promotion de la cybersécurité, la gouvernance électronique et la lutte contre la cybercriminalité ».

2. **Agenda de l'Union africaine pour les enfants 2040**[308]
   L'agenda de l'Union africaine pour l'année 2040, l'Agenda 2063, définit des objectifs pour les enfants du continent. L'agenda s'appuie sur le paragraphe 53 qui stipule que « les enfants africains doivent être responsabilisés par la mise en œuvre intégrale de la Charte africaine des droits de l'enfant ».

3. **Stratégie de la Commission européenne Better Internet for Kids (Un Internet meilleur pour les enfants)**[309]
   Il s'agit de la stratégie européenne de la Commission européenne pour un meilleur Internet pour les enfants. La stratégie porte sur les compétences et les outils numériques destinés aux enfants et souligne également le potentiel du marché pour le développement de contenus en ligne interactifs, créatifs et éducatifs.

4. **WeProtect Global Alliance Model National Response (Réponse nationale modèle WeProtect Global Alliance, MNR)**[310]
   La réponse nationale modèle (MNR) vise à aider les pays à élaborer leur réponse à l'exploitation et à l'abus sexuels des enfants en ligne, mais elle indique que cette question ne peut être traitée de manière isolée. Un ensemble plus large de capacités de prévention et de lutte contre l'exploitation et les abus sexuels concernant des enfants doit être mis en place pour assurer une réponse nationale complète.

5. **Carte de politique de Better Internet for Kids (BIK)**[311]
   La carte de politique de Better Internet for Kids (BIK) offre un aperçu complet des stratégies et politiques BIK actuellement mises en œuvre dans les États membres de l'UE.

6. **ASEAN Regional Plan of Action on the Elimination of Violence Against Children (Plan d'action régional de l'ANASE sur l'élimination de la violence contre les enfants)**[312] **et Declaration on the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN (Déclaration sur la protection des enfants contre toutes les formes d'exploitation et d'abus en ligne dans l'ANASE)**[313]
   Le plan régional fournit une feuille de route pour aider les États membres à mettre en œuvre la déclaration de l'ANASE de 2013 sur la protection des enfants contre toutes les formes d'exploitation en ligne. ▶

307. African Union Convention on Cyber Security and Personal Data Protection (Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles), Union africaine, 2014.
308. Africa's Agenda for Children 2040 Fostering an Africa Fit for Children, African Committee of Experts on the Rights and Welfare of the Child (Agenda africain pour les enfants 2040 : promouvoir une Afrique adaptée aux enfants, Comité africain d'experts sur les droits et le bien-être de l'enfant.), 2016.
309. A European Strategy for a better Internet for our children (Une stratégie européenne pour un meilleur Internet au profit de nos enfants), Commission européenne, 2021.
310. Model National Response (Modèle de réponse nationale), WeProtect Global Alliance, 2016.
311. Better Internet for Kids Policy Map (Carte de politique de Better Internet for Kids), Better Internet for Kids, 2020.
312. ASEAN Regional Plan of Action on Elimination of Violence against Children (Plan d'action régional de l'ANASE sur l'élimination de la violence contre les enfants), Fonds des Nations unies pour l'enfance, 2019.
313. Ending violence against children in ASEAN Member States (Mettre fin à la violence contre les enfants dans les États membres de l'ANASE), UNICEF Asie de l'Est et Pacifique, 2019.

7. **Étude de cas : conventions du Conseil de l'Europe**
   La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, également connue sous le nom de « Convention de Lanzarote »,[314] exige la criminalisation de tous les types d'infractions sexuelles à l'encontre des enfants. Elle stipule que les États d'Europe et du reste du monde doivent adopter une législation spécifique et prendre des mesures pour prévenir la violence sexuelle, protéger les enfants victimes et poursuivre les auteurs.

   Le « Comité de Lanzarote »[315] (c'est-à-dire le Comité des Parties de la Convention de Lanzarote) est l'organe créé pour contrôler[316] si les Parties appliquent effectivement la Convention de Lanzarote. Le Comité est également chargé d'identifier les bonnes pratiques,[317] en particulier lors des activités de renforcement des capacités[318] (visites d'étude, conférences, etc.).

   Le Conseil de l'Europe contribue à protéger les sociétés du monde entier contre la menace de la cybercriminalité par le biais de la Convention de Budapest sur la cybercriminalité et de son Protocole sur la xénophobie et le racisme, du Comité de la Convention sur la cybercriminalité (T-CY) et des programmes de coopération technique sur la cybercriminalité.

   La convention est le premier traité international sur les infractions commises au moyen d'Internet et d'autres réseaux informatiques. Elle traite en particulier des atteintes aux droits d'auteur, de la fraude informatique, de la pédopornographie et des violations de la sécurité des réseaux. Elle contient également une série de pouvoirs et de procédures tels que la recherche de réseaux informatiques et l'interception.

8. **Organization of American States Preliminary Principles and Recommendations on Data Protection (Protection of Personal Data), Organisation des États américains : principes et recommandations préliminaires sur la protection des données (Protection des données personnelles)**[319]
   C'est le résultat d'une étude du Comité juridique interaméricain sur les cadres de protection des données. Les Principes représentent un modèle pour la législation interaméricaine sur l'accès à l'information publique. Ils représentent l'orientation du Secrétariat général pour assister les Etats membres dans la conception, l'exécution et l'évaluation de leurs cadres juridiques locaux concernant l'accès à l'information publique.

Coopération entre pays et cadres de soutien mutuel

9. **Luxembourg Guidelines (lignes directrices du Luxembourg) sur la terminologie pour la protection des enfants contre l'exploitation et les abus sexuels**[320]
   Ces lignes directrices sont une initiative de 18 partenaires internationaux visant à harmoniser les termes et définitions relatifs à la protection de l'enfance. Elles visent à apporter une plus grande clarté conceptuelle sur la terminologie afin de garantir une défense, une politique et des lois renforcées et plus cohérentes dans toutes les langues et dans toutes les régions du monde.

10. **Police Scotland support for development of a Child Online Policy in Rwanda (Assistance de Police Scotland pour l'élaboration d'une politique relative aux enfants en ligne au Rwanda)**[321]
    Il s'agit d'un partenariat entre Police Scotland et le gouvernement du Rwanda. 5Rights Foundation a publié un article de blog détaillé décrivant le partenariat.

314. Convention de Lanzarote, Conseil de l'Europe.
315. Comité de Lanzarote, Conseil de l'Europe.
316. Suivi de la Convention de Lanzarote, Conseil de l'Europe.
317. Bonnes pratiques de la Convention de Lanzarote, Conseil de l'Europe.
318. Convention de Lanzarote, Conseil de l'Europe.
319. Preliminary Principles and Recommendations on Data Protection (Principes et recommandations préliminaires sur la protection des données), Conseil permanent de l'Organisation des États américains, 2011.
320. Luxembourg Guidelines (Lignes directrices du Luxembourg), ECPAT, 2016.
321. Working with the Government of Rwanda and Police Scotland to support children online (Collaboration avec le gouvernement du Rwanda et Police Scotland pour protéger les enfants en ligne), 5Rights Foundation, 2020.

< SECTION PRÉCÉDENTE SECTION SUIVANTE >

10 Coopération internationale

11. La Déclaration universelle de protection en ligne des enfants[322]
Il s'agit de la déclaration de la Commission sur le large bande, qui vise à aligner toutes les parties prenantes sur la mission commune de défendre la cause de la protection en ligne des enfants.

Exemples de coopération entre les services chargés de l'application de la loi[323]

12. Le Virtual Global Taskforce (Groupe de travail virtuel mondial)[324]
Ce groupe de travail représente des organismes nationaux, régionaux et internationaux chargés de l'application de la loi qui ont uni leurs efforts pour lutter contre les abus sexuels d'enfants en ligne dans le monde entier. Il fournit également des liens vers les lignes d'assistance téléphonique régionales pour l'application de la loi et le signalement de matériel concernant l'abus sexuel sur mineur.

13. Lignes directrices du Conseil de l'Europe pour la coopération entre les services chargés de l'application de la loi et les fournisseurs de services Internet dans la lutte contre la cybercriminalité[325]
Il s'agit d'un ensemble de lignes directrices élaborées pour aider les fournisseurs de services et les services chargés de l'application de la loi de tout pays à établir des relations de travail efficaces. Elles sont proposées dans plus d'une douzaine de langues.

322. Déclaration universelle de protection en ligne des enfants, Commission sur le large bande, 2019.
323. Notice and Takedown: Company policies and practices to remove online child sexual abuse material (Notification et suppression : politiques et pratiques des entreprises en matière de retrait de matériel concernant l'abus sexuel sur mineur en ligne), Fonds des Nations Unies pour l'enfance et GSMA, 2016.
324. Virtual Global Taskforce (Groupe de travail virtuel mondial), Virtual Global Taskforce, 2016.
325. Law enforcement - Internet service provider Cooperation (Application de la loi - Coopération des fournisseurs de services Internet), Conseil de l'Europe, 2007.

« Vos données sont votre propriété. Vous avez le droit fondamental de savoir comment elles sont utilisées. Dans quelle mesure est-il facile d'utiliser mes données à mauvais escient et sont-elles monétisées ? »

– Enfant au Royaume-Uni, 17 ans

« Il est nécessaire que les jeunes connaissent leurs droits, afin de les protéger et de faire valoir ces droits. Grâce à Internet et à la technologie, c'est de plus en plus possible. »

– Enfant vivant en Roumanie, 16 ans

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 6

01	Introduction	6
02	Comment l'utiliser	9
03	Pourquoi les droits de l'enfant sont-ils importants	15
04	Cinq éléments que chaque responsable politique doit prendre en considération	25
05	Dix domaines d'action politique	37
06	**Documents clés**	169
07	Glossaire	174
08	Politique modèle	180

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Documents clés

La Convention des Nations Unies relative aux droits de l'enfant et les documents connexes :

1. **Convention des Nations Unies sur les droits de l'enfant**[326]
   Adoptée et ouverte à la signature, à la ratification et à l'adhésion par la résolution 44/25 de l'Assemblée générale du 20 novembre ; entrée en vigueur le 2 septembre 1990, conformément à l'article 49.

   Il existe également un texte et des illustrations adaptés aux enfants sur la Convention relative aux droits de l'enfant (voir également la section « Pourquoi les droits de l'enfant sont importants ») pour aider les enfants à comprendre leurs droits.

2. **Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pédopornographie**[327]
   Adopté et ouvert à la signature, à la ratification et à l'adhésion par la résolution de l'Assemblée générale A/RES/54/263 du 25 mai 2000 ; entré en vigueur le 18 janvier 2002.

3. **Protocole facultatif à la Convention relative aux droits de l'enfant, concernant l'implication d'enfants dans les conflits armés**[328]
   Adopté et ouvert à la signature, à la ratification et à l'adhésion par la résolution de l'Assemblée générale A/RES/54/263 du 25 mai 2000 ; entré en vigueur le 12 février 2002.

4. **Protocole facultatif à la Convention relative aux droits de l'enfant établissant une procédure de communications**[329]
   Résolution adoptée par l'Assemblée générale le 19 décembre 2011

5. **UNICEF Guidance: How We Protect Children's Rights with the UN Convention on the Rights of the Child (Guide de l'UNICEF : comment nous protégeons les droits des enfants avec la Convention des Nations Unies sur les droits de l'enfant)**[330]
   UNICEF's short guide to the Convention and its Optional Protocols (Petit guide de l'UNICEF sur la Convention et ses Protocoles facultatifs).

6. **L'observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique**[331]
   L'observation générale n° 25 fournit une analyse pratique de la manière dont les droits contenus dans la CIDE s'appliquent à la protection en ligne des enfants et au monde numérique.

7. **La version pour les jeunes de l'observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique**[332]
   Ce document présente les droits des enfants dans le monde numérique dans leurs propres mots et explique leurs droits de manière accessible.

326. Convention on the Rights of the Child (Convention sur les droits de l'enfant), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 1995.
327. The United Nations Convention on the Rights of the Child – The Children's Version (La Convention des Nations Unies relative aux droits de l'enfant - La version pour les enfants), Fonds des Nations Unies pour l'enfance.
328. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pédopornographie), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2002.
329. Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict (Protocole facultatif à la Convention relative aux droits de l'enfant concernant l'implication d'enfants dans les conflits armés), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2002.
330. Optional Protocol to the Convention on the Rights of the Child on a Communications Procedure (Protocole facultatif à la Convention relative aux droits de l'enfant concernant une procédure de communication), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2014.
331. How we protect Children's rights with the UN Convention on the Rights of the Child (Comment nous protégeons les droits des enfants avec la Convention des Nations Unies sur les droits de l'enfant), Fonds des Nations Unies pour l'enfance.
332. In Our Own Words – Children's Rights in the Digital World (Dans nos propres mots : les droits de l'enfant dans le monde numérique), 5Rights Foundation, 2021.

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Autres cadres et documents internationaux pertinents :

1. **La WeProtect Global Alliance *Model National Response* (Réponse nationale modèle WeProtect Global Alliance, MNR)**[333]
   La Réponse nationale modèle (MNR) est un élément clé de toute boîte à outils nationale pour la protection en ligne des enfants. La MNR vise à aider les pays à élaborer leur réponse à l'exploitation et à l'abus sexuels des enfants en ligne, mais elle indique que cette question ne peut être traitée de manière isolée. Un ensemble plus large de capacités de prévention et de lutte contre l'exploitation et les abus sexuels concernant des enfants doit être mis en place pour assurer une réponse nationale complète. Cette boîte à outils fournit des ressources qui soutiennent la mise en œuvre de la MNR. La Boîte à outils pour la protection en ligne des enfants peut aider les signataires de la MNR de la WeProtect Global Alliance à s'assurer qu'ils disposent de la capacité institutionnelle nécessaire pour atteindre les objectifs fixés, et que les obligations prévues par l'Observation générale n° 25 (2021) sont respectées.

2. **Lignes directrices de l'UIT sur la protection en ligne des enfants**[334]
   Les lignes directrices de l'UIT sur la protection en ligne des enfants constituent un ensemble complet de recommandations à l'attention de toutes les parties prenantes sur la manière de contribuer au développement d'un environnement en ligne sûr et stimulant pour les enfants et les jeunes.

   Les lignes directrices de la COP sont le fruit de la collaboration de 80 experts de différents secteurs, y compris des acteurs gouvernementaux, des organisations internationales, des ONG, des universités et le secteur privé. Rédigées pour la première fois en 2009, elles ont été mises à jour en 2020 et comprennent quatre séries d'orientations pour :

   - Les enfants
   - Les parents/personnes en charge d'enfants et éducateurs
   - L'industrie et
   - Les responsables politiques

3. **Les objectifs de développement durable de l'ONU (ODD)**
   La protection en ligne des enfants contribue à la réalisation de plusieurs des ODD et peut faire partie des programmes des responsables politiques pour respecter leurs engagements dans le cadre des ODD. Le Programme 2030 pour le développement durable,[335] adopté par tous les États membres des Nations unies en 2015, constitue un modèle commun de paix et de prospérité pour les populations et la planète, aujourd'hui et à l'avenir. Il est axé sur les 17 objectifs de développement durable (ODD),[336] qui constituent un appel urgent à l'action de tous les pays, développés et en développement, dans le cadre d'un partenariat mondial. Ils reconnaissent que l'éradication de la pauvreté et des autres privations doit aller de pair avec des stratégies visant à améliorer la santé et l'éducation, à réduire les inégalités et à stimuler la croissance économique, tout en s'attaquant au changement climatique et en œuvrant à la préservation de nos océans et de nos forêts.

4. **Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme**[337]
   « Ces Principes directeurs reconnaissent fondamentalement :

   (a) Les obligations existantes qui incombent aux États de respecter, protéger et mettre en œuvre les droits de l'homme et les libertés fondamentales ;
   (b) Le rôle dévolu aux entreprises en qualité d'organes spécialisés de la société remplissant des fonctions particulières, tenues de se conformer à toutes les lois applicables et de respecter les droits de l'homme ;
   (c) La nécessité que les droits et obligations s'accompagnent des voies de recours appropriées et efficaces en cas de violation.

   Ces Principes directeurs s'appliquent à tous les États et à toutes les entreprises commerciales, transnationales ou autres, indépendamment de leur taille, de leur secteur, de leur lieu d'implantation, de leur régime de propriété et de leur structure. »

333. Model National Response, WeProtect Global Alliance, 2015.
334. Guidelines on Child Online Protection (Lignes directrices sur la protection en ligne des enfants), Union internationale des télécommunications, 2021.
335. Transforming our world: the 2030 Agenda for Sustainable Development (Transformer notre monde : l'Agenda 2030 pour le développement durable), Département des affaires économiques et sociales des Nations Unies, 2021.
336. Les 17 objectifs, Département des affaires économiques et sociales des Nations Unies, 2015.
337. Principes directeurs relatifs aux entreprises et aux droits de l'homme, Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2011.

5. **INSPIRE de l'Organisation mondiale de la santé : sept stratégies pour mettre fin à la violence à l'encontre des enfants**[338]
   Il s'agit d'un « ensemble de mesures techniques fondées sur des données probantes visant à épauler les pays dans leurs efforts pour prévenir et combattre la violence à l'encontre des enfants âgés de 0 à 17 ans. Cet ensemble comprend le document de base décrivant les stratégies et les interventions d'INSPIRE, un manuel de mise en œuvre qui fournit des détails sur la façon de déployer les interventions, et une série d'indicateurs pour mesurer l'adoption d'INSPIRE et son impact sur les niveaux de violence contre les enfants. »

6. **Projet de directives de l'UNICEF sur l'IA pour les enfants**[339]
   Il s'agit de promouvoir les droits de l'enfant dans les politiques et pratiques d'IA des gouvernements et du secteur privé, et de sensibiliser à la manière dont les systèmes d'IA peuvent respecter ou compromettre ces droits. Les orientations politiques explorent l'IA et les systèmes d'IA, et examinent les façons dont ils ont un impact sur les enfants. Ce projet s'appuie sur la Convention relative aux droits de l'enfant pour présenter les trois fondements d'une IA respectueuse des droits de l'enfant :

   - Les politiques et systèmes d'IA doivent chercher à protéger les enfants.
   - Ceux-ci doivent répondre équitablement aux besoins et aux droits des enfants.
   - Ils doivent donner aux enfants les moyens de contribuer au développement et à l'utilisation de l'IA.

   Sur ces bases, les lignes directrices proposent neuf exigences pour une IA centrée sur l'enfant et fournissent des ressources indicatives pour rendre ces orientations opérationnelles.

7. **Luxembourg Guidelines (lignes directrices du Luxembourg) sur la terminologie pour la protection des enfants contre l'exploitation et les abus sexuels**[340]
   Ces lignes directrices sont une initiative de 18 partenaires internationaux visant à harmoniser les termes et définitions relatifs à la protection de l'enfance. Elles visent à apporter une plus grande clarté conceptuelle sur la terminologie afin de garantir une défense, une politique et des lois renforcées et plus cohérentes dans toutes les langues et dans toutes les régions du monde.

8. **Le principe de précaution**[341]
   L'UNESCO, en collaboration avec son organe consultatif, la Commission mondiale sur l'éthique des connaissances scientifiques et des technologies, a élaboré une définition de travail du « principe de précaution » que l'on retrouve dans de nombreux instruments internationaux relatifs aux développements scientifiques en général, et qui est applicable à la conception axée sur l'enfant dans le domaine technologique :

   « Lorsque des activités humaines peuvent causer un préjudice moralement inacceptable qui est scientifiquement plausible mais incertain, des mesures devront être prises pour éviter ou atténuer ce préjudice. Un préjudice moral inacceptable est un danger pour l'homme ou l'environnement qui est :

   1. une menace pour la vie ou la santé humaine, ou
   2. sérieux et effectivement irréversible, ou
   3. inéquitable pour les générations actuelles ou futures, ou
   4. imposé sans tenir suffisamment compte des droits de l'homme des personnes affectées. ▶

338. INSPIRE: Seven Strategies for Ending Violence Against Children (INSPIRE : sept stratégies pour mettre fin à la violence contre les enfants), Organisation mondiale de la santé, 2021.
339. Directives politiques sur l'IA pour les enfants, Fonds des Nations Unies pour l'enfance, 2020.
340. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016
341. The Precautionary Principle (Les principes de précaution), World Commission on the Ethics of Scientific Knowledge and Technology (Commission mondiale de l'éthique des connaissances scientifiques et des technologies), 2005.

Le jugement de plausibilité doit être fondé sur une analyse scientifique. L'analyse doit être continue afin que les actions menées fassent l'objet d'un examen. L'incertitude peut s'appliquer, mais sans s'y limiter, à la causalité ou aux limites du préjudice possible.

Les actions sont des interventions entreprises avant que le préjudice ne soit causé, dans le but d'éviter ou d'atténuer le préjudice. Il faudra choisir des actions qui sont proportionnelles à la gravité du préjudice potentiel, en tenant compte de leurs conséquences positives et négatives, et avec une évaluation des implications morales de l'action et de l'inaction. Le choix de l'action doit être le résultat d'un processus participatif. »

9. **Cadres régionaux pour la protection des droits de l'enfant**
   Par exemple, les lignes directrices du Conseil de l'Europe[342] pour le respect, la protection et la mise en œuvre des droits de l'enfant dans l'environnement numérique fournissent des orientations utiles dans le contexte européen. L'Union africaine a élaboré la Charte africaine des droits et du bien-être de l'enfant[343] pour décrire les droits des enfants dans le contexte africain.

10. **Développements novateurs au niveau national qui ont une importance mondiale**
    Par exemple, le Code britannique de conception adaptée à l'âge (Age Appropriate Design Code)[344] et la loi australienne sur la sécurité en ligne.[345]

342. Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (Lignes directrices pour le respect, la protection et la mise en œuvre des droits de l'enfant dans l'environnement numérique), Conseil de l'Europe, 2018.
343. Charte africaine des droits et du bien-être de l'enfant, Union africaine, 1990.
344. Introduction to the Age Appropriate Design Code (Introduction au code de conception adapté à l'âge), Bureau du Commissaire à l'information.
345. Consultation on a Bill for a new Online Safety Act (Consultation sur un projet de loi pour une nouvelle loi sur la sécurité en ligne), Ministère des infrastructures, des transports, du développement régional et des communications.

DOSSIER SYSTÈME

8 ÉLÉMENTS | 105 MO SUR DISQUE | SECTION 7

01 Introduction 6

02 Comment l'utiliser 9

03 Pourquoi les droits de l'enfant sont-ils importants 15

04 Cinq éléments que chaque responsable politique doit prendre en considération 25

05 Dix domaines d'action politique 37

06 Documents clés 169

07 Glossaire 174

08 Politique modèle 180

< SECTION PRÉCÉDENTE

SECTION SUIVANTE >

Glossaire

À sa 86e session, le Comité des droits de l'enfant a adopté son Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique. Ce glossaire terminologique, qui n'est pas exhaustif, a également été inclus dans le cadre de ce projet.

Analyses émotionnelles
Le recueil de données pour déterminer ou déduire l'humeur d'un individu, souvent effectué en évaluant les communications vidéo, vocales et écrites, ou les données personnelles, pour identifier des marqueurs tels que l'expression du visage ou le ton de voix qui sont corrélés à des émotions spécifiques en utilisant des techniques d'apprentissage automatique, y compris des algorithmes.

Ciblage comportemental
Analyse de l'activité en ligne des utilisateurs afin de les cibler avec de la publicité, des messages, des suggestions de contenus supplémentaires ou des contacts avec d'autres utilisateurs sur la base de leurs préférences antérieures, souvent dans l'intention de modifier leur comportement futur.

Conception sécuritaire
La pratique consistant à concevoir des services en ligne dans le but d'assurer autant que possible la sécurité des utilisateurs, par exemple en définissant des paramètres de sécurité par défaut pour les comptes des utilisateurs mineurs ou en empêchant les adultes de contacter les utilisateurs mineurs.

Cyberagression
Actes préjudiciables perpétrés par des individus ou des groupes, en ligne ou par le biais de la technologie numérique, souvent dans l'intention d'offenser ou de blesser un autre individu ou groupe.

Désinformation
Lorsque de fausses informations sont sciemment partagées.

Filtrage des informations
L'utilisation d'un programme pour filtrer le contenu numérique et identifier ou cacher le contenu qui correspond à des critères définis. Parmi les utilisations courantes du filtrage des informations, citons le masquage des contenus choquants dans les résultats des moteurs de recherche ou le tri des résultats qui apparaissent en premier.

Habileté numérique
La capacité d'utiliser les technologies de l'information et de la communication pour trouver, évaluer, créer et communiquer. Les termes apparentés comprennent, entre autres, « éducation aux médias », « éducation à l'information » ou « éducation aux médias et à l'information ».

Information fausse ou trompeuse
Lorsque de fausses informations sont partagées, mais sans intention de nuire.

Minimisation des données
Le principe consistant à ne collecter que le minimum de données personnelles pertinentes nécessaires à la finalité pour laquelle elles sont traitées, et à ne conserver ces données que dans la mesure où elles sont nécessaires à cette finalité.

Modération des contenus
Pratique consistant à surveiller et à analyser le contenu généré par les utilisateurs en fonction de règles prédéterminées afin de supprimer le contenu jugé inadmissible, soit automatiquement, soit en faisant appel à des modérateurs humains. La modération des contenus peut être effectuée simultanément à la génération des contenus, comme dans les services de chat, ou en différé, comme dans les forums.

Neuromarketing
L'étude de la façon dont le cerveau des gens réagit au contenu marketing, et l'application de cette information pour développer des campagnes marketing plus efficaces. Les réactions peuvent être mesurées de nombreuses façons, de l'analyse de l'activité cérébrale au temps d'engagement, en passant par les clics et le temps passé sur un site Web.

Numérisation
L'adaptation des environnements, des pratiques, des entreprises et de la vie quotidienne pour inclure les services et les infrastructures numériques et en tirer parti. Il s'agit également de la conversion d'informations dans un format numérique.

Profilage
La pratique consistant à utiliser les données personnelles de l'individu pour déduire, prédire ou analyser les caractéristiques de cette personne, par exemple ses goûts, ses préférences, ses points de vue, ses opinions ou son comportement, dans le but de recommander du contenu, des produits ou des services sur la base du profil de données de la personne.

Protection de la vie privée dès la conception
La pratique consistant à concevoir des services en ligne dans le but de protéger autant que possible la vie privée des utilisateurs, par exemple en paramétrant les comptes des utilisateurs mineurs comme étant privés par défaut ou en limitant la quantité de données recueillies.

Risques liés au contact
Préjudice potentiel créé par la possibilité pour les utilisateurs d'entrer en contact les uns avec les autres en utilisant des services en ligne, par exemple en permettant à des inconnus ou à des personnes cachant leur identité de contacter des enfants.

Publicité ciblée
La pratique consistant à montrer des publicités particulières aux utilisateurs en fonction des données recueillies à leur sujet, par ex

Publicité immersive
L'intégration harmonieuse de publicités dans le contenu en ligne ou les services numériques, permettant aux utilisateurs de rester immergés dans les caractéristiques du contenu et des services tout en étant exposés au marketing et aux messages de la marque.

Recherche automatisée
Le processus d'évaluation des données des utilisateurs pour filtrer le contenu auquel ils accèdent en ligne, principalement pour des intérêts commerciaux. Le contenu est généralement choisi en fonction de la perception de la réaction de l'utilisateur à d'autres contenus, ou en fonction du contenu que d'autres utilisateurs ayant agi de la même manière ont recherché par la suite.

Risques contractuels
Préjudice potentiel lorsqu'un utilisateur est exposé à des relations contractuelles ou à des pressions commerciales inappropriées, telles que l'utilisation compulsive, les jeux de hasard, la publicité ciblée, les coûts cachés, les conditions générales inéquitables et la perte de contrôle des données personnelles.

Risques liés au contenu
Préjudice potentiel pour les utilisateurs en fonction de la nature du contenu en ligne, y compris le contenu inapproprié pour l'âge (par exemple, la pornographie), non fiable (comme l'information fausse ou trompeuse ou la désinformation) ou certaines autres catégories de contenu (par exemple, la promotion de comportements à risque ou de méthodes d'automutilation ou de suicide).

Risques liés à la conduite
Préjudice potentiel fondé sur le comportement ou la conduite de l'utilisateur ou de ses pairs, par exemple l'utilisation délibérée de plateformes en ligne pour menacer ou harceler d'autres utilisateurs, y compris le cyberharcèlement, le « sexting » et les commentaires haineux, parfois aussi involontairement par la divulgation d'informations privées d'autres utilisateurs.

Systèmes automatisés
Logiciel et matériel programmés pour exécuter une fonction automatiquement sans qu'une intervention humaine soit nécessaire pour fournir des informations et des instructions pour chaque opération.

Technologie des implants
Une micro-puce qui peut être implantée sur une personne pour stocker, suivre ou récupérer des informations contenues dans une base de données externe, telles que l'identification personnelle ou des informations médicales, policières ou de contact.

Technologie d'assistance
Technologie développée pour favoriser ou améliorer l'indépendance d'un individu, y compris les systèmes d'adaptation et de réadaptation, ainsi que les dispositifs destinés aux personnes en situation de handicap, tels qu'un lecteur d'écran ou une reconnaissance vocale.

Traitement automatisé
Le processus de prise de décision par des moyens automatisés, c'est-à-dire en utilisant un logiciel configuré pour analyser les données fournies et suivre des règles définies pour parvenir à des décisions basées sur des algorithmes, sans intervention humaine.

Traitement des données
Comprend les processus de recueil, d'enregistrement, de conservation, d'analyse, de diffusion et d'utilisation des données.

Vol d'identité
L'usurpation frauduleuse de l'identité d'une autre personne, par exemple pour accéder à son patrimoine, porter atteinte à sa réputation, avoir accès à ses contacts en ligne ou en tirer un quelconque profit.

Réalité virtuelle et Réalité augmentée

Réalité augmentée :
Une simulation du monde physique avec des caractéristiques modifiées ou des éléments supplémentaires, généralement vécue à travers un écran pour permettre la superposition d'objets virtuels sur une image en direct ou une vidéo de la réalité.

Réalité virtuelle :
La simulation par ordinateur d'une image ou d'un environnement tridimensionnel avec lequel une personne peut interagir de manière apparemment réelle ou physique à l'aide d'un équipement numérique spécial, tel qu'un casque avec un écran incorporé ou des gants équipés de capteurs.

Pour d'autres termes concernant spécifiquement les abus sexuels sur les enfants, veuillez vous référer aux Luxembourg Guidelines (Lignes directrices du Luxembourg) de l'ECPAT.[346]

346. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016.

Postface

Faire de la protection des enfants en ligne une réalité est le travail de nombreuses personnes : les dirigeants mondiaux, la communauté internationale, les responsables politiques, les autorités chargées de l'application de la loi, les professionnels de la santé, les enseignants, les parents, les personnes en charge d'enfants et les enfants eux-mêmes.

« Le jeu numérique est en fait bénéfique car il évite de s'ennuyer... Internet procure du bonheur aux enfants en réalisant des vidéos amusantes. »

– Enfant vivant au Ghana, 17 ans

« Dans quelle mesure [mes données] sont-elles sécurisées et comment les médias les protègent-ils des pirates informatiques ? Je veux savoir où [mes données sont stockées] et dans quelle mesure leur sécurité est assurée. Je veux savoir si mes informations... sont également partagées avec leurs autres contacts de confiance ? »

– Enfant vivant au Canada, 15 ans

DOSSIER SYSTÈME

8 ÉLÉMENTS	105 MO SUR DISQUE	SECTION 8

01	Introduction	6
02	Comment l'utiliser	9
03	Pourquoi les droits de l'enfant sont-ils importants	15
04	Cinq éléments que chaque responsable politique doit prendre en considération	25
05	Dix domaines d'action politique	37
06	Documents clés	169
07	Glossaire	174
08	**Politique modèle**	180

Projet de politique modèle

Le texte suivant est un projet de politique modèle, regroupant toutes les sections de cette boîte à outils. Chaque pays a son propre point de départ lorsqu'il conçoit sa politique de sécurité en ligne pour les enfants. Ce modèle permet d'aborder la dimension numérique des droits de l'enfant.

Introduction

Pourquoi les droits de l'enfant sont importants

Les droits de l'enfant constituent le fil conducteur de toutes les politiques qui affectent la vie des enfants, tant en ligne qu'hors ligne. L'objectif d'une politique de sécurité en ligne pour les enfants est, fondamentalement, de faire en sorte que les droits des enfants à la protection et à la participation soient réels et effectifs lorsqu'ils s'engagent dans le monde numérique.

Les enfants et leurs familles ont des droits fondamentaux en vertu de la Charte internationale des droits, notamment la Déclaration universelle des droits de l'homme de 1948, le Pacte international relatif aux droits civils et politiques de 1966 et le Pacte international relatif aux droits économiques, sociaux et culturels de 1966, ainsi que des structures régionales et nationales des droits de l'homme.

En ce qui concerne les enfants, la Convention des Nations Unies relative aux droits de l'enfant de 1989 (« la Convention » ou CDE)[1] et ses protocoles facultatifs relatifs à la vente d'enfants[2] et aux enfants dans les conflits armés[3] fournissent un cadre pratique pour comprendre comment les droits de l'homme s'appliquent aux enfants. La Convention est le traité sur les droits de l'homme le plus largement ratifié de l'histoire et son protocole facultatif relatif à une procédure de communication contribue à la rendre exécutoire afin que les droits des enfants soient réels et effectifs.

Tous les droits contenus dans la CDE sont utiles pour assurer la protection en ligne des enfants, et il est essentiel de consulter les enfants pour comprendre ce que ces droits signifient dans la pratique. Par exemple, les droits des enfants au jeu, à la participation et à la vie de famille dans l'espace en ligne doivent être pris en compte. Toutes les personnes impliquées dans la réalisation des consultations doivent être correctement formées aux droits de l'enfant et aux implications pratiques de la voix et de l'inclusion des enfants.

5 considérations principales

1. Identification des risques et atténuation des dommages

Les stratégies de protection en ligne des enfants doivent être élaborées avant tout pour maximiser les avantages que les enfants peuvent tirer des technologies numériques. Cela implique nécessairement la responsabilité première d'atténuer les risques, de limiter au maximum la probabilité qu'un dommage se produise, de remédier aux dommages lorsqu'ils se sont produits et de prendre en compte l'impact que les produits et services peuvent avoir sur l'utilisateur final, si cet utilisateur est (ou est susceptible d'être) un enfant. Il est essentiel de concevoir des produits et des services qui anticipent la participation des enfants en toute sécurité.

Si certains enfants subissent un préjudice grave, des millions d'autres sont victimes d'un préjudice en ligne sous une forme ou une autre. Par exemple, il existe un large éventail de risques liés à la surveillance ou à l'exploitation commerciale, à l'exposition à de fausses informations ou à des arnaques, à des prédateurs ou à du harcèlement, tandis qu'un nombre moins important d'entre eux subissent le préjudice extrême d'un abus sexuel sur un enfant. De nombreux risques sont cumulatifs. Ils affectent les enfants de différentes manières et une forme de préjudice peut ouvrir la voie à d'autres formes de préjudice.[4]

La nature internationale du monde en ligne implique que les enfants sont confrontés aux mêmes risques en ligne, quelle que soit leur situation géographique. Mais des contextes différents peuvent également soulever des préoccupations spécifiques. Dans certains cas, un enfant peut être désavantagé par un manque d'accès à l'environnement en ligne ; dans d'autres cas, il peut y avoir un lien entre le préjudice subi en ligne et l'expérience hors ligne d'un enfant. Les risques et les préjudices spécifiques se chevauchent souvent les uns les autres. Il existe très peu de grandes lignes ou de divisions nettes.

---

1. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
2. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
3. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989.
4. Building the digital world that young people deserve (Construire le monde numérique que les jeunes méritent), 5Rights Foundation, 2020.

Des facteurs tels que le sexe, l'âge, les circonstances familiales, le statut socio-économique, le lieu, les expériences et la disponibilité de la technologie numérique peuvent modifier les risques et les façons dont les enfants subissent des préjudices. Certains risques et préjudices affectent des communautés et des catégories d'enfants entières : par exemple, les filles sont plus exposées aux abus, tandis que les garçons ont tendance à être davantage maltraités.[5] Les normes culturelles entourant la masculinité aggravent également le problème de la sous-détection et du sous-signalement des abus sexuels sur les enfants de sexe masculin.[6] Les risques et les préjudices peuvent également être amplifiés par des plateformes conçues de manière à encourager le partage de contenus choquants et sensationnels, ou encore par le profilage ou la promotion de certains types de comportements d'utilisateurs parce qu'ils suscitent un engagement rentable.

Les responsables politiques doivent prendre en compte tous les risques auxquels sont exposés les enfants et prendre des mesures pour les atténuer. Un outil clé pour identifier les risques est le cadre des 4C.

La classification des 4C de CO:RE reconnaît que les risques en ligne apparaissent lorsqu'un enfant :

- Accède à et est exposé à des **contenus** potentiellement dangereux
- Subit ou est visé par des **contacts** potentiellement dangereux
- Est témoin, participe ou est victime d'un **comportement** potentiellement dangereux
- Est partie à ou exploité par un **contrat** potentiellement nuisible.

2. Promouvoir l'accès, l'accessibilité et l'inclusion

Aujourd'hui, l'accès au monde en ligne est crucial pour que les enfants puissent exercer leurs droits et réaliser pleinement leur potentiel. Une politique de sécurité en ligne pour les enfants doit être inclusive, à la fois dans ses objectifs et dans sa pratique.[7] Cela signifie qu'elle doit être assortie de ressources adéquates et qu'elle doit s'appuyer sur les meilleures pratiques et les cadres existants, en particulier dans les situations où les ressources sont limitées. Que la mise en œuvre d'une politique de sécurité des enfants en ligne implique d'adapter la législation existante (par exemple en matière de protection de l'enfance, de protection des consommateurs ou de réglementation des télécommunications) au contexte de la protection en ligne des enfants ou de créer de nouveaux corps de loi, elle doit promouvoir l'inclusion et l'égalité pour tous les enfants, quels qu'ils soient et où qu'ils soient.

Les enfants ne constituent pas un groupe homogène. Les politiques de protection en ligne des enfants doivent être accessibles et inclusives pour atteindre tous les enfants, quels qu'ils soient et où qu'ils soient. Une « fracture numérique » risque fort d'apparaître lorsque certains enfants ont facilement accès à l'espace en ligne, tandis que d'autres en sont effectivement exclus. Les cadres doivent être adaptés à l'âge des enfants et convenir à tous les enfants, quels que soient leur sexe, leur race, leur religion, leur nationalité, leur origine ethnique, leur handicap ou toute autre caractéristique. La langue doit être accessible et inclusive et, le cas échéant, les supports doivent être disponibles dans un éventail de langues différentes. Les supports relatifs à la protection en ligne des enfants doivent être élaborés en consultation avec les enfants et les personnes qui s'occupent d'eux : au minimum, ils doivent être adaptés à l'âge, neutres du point de vue du sexe et facilement accessibles aux enfants d'âges différents et à leurs parents/aux personnes qui s'en occupent. Lorsque l'alphabétisation est limitée, les supports visuels permettent souvent de faire passer les messages de manière beaucoup plus efficace. L'utilisation de termes cohérents entre les différentes plateformes contribue à rendre la protection en ligne des enfants plus facilement compréhensible et accessible pour les enfants, leurs familles et les personnes qui s'en occupent.[8]

Les responsables politiques doivent s'assurer qu'ils favorisent l'accès des enfants en ligne et qu'ils les incluent dans leur démarche pour rendre les environnements numériques sûrs.

---

5. Safe Online Investment Portfolio Results 2020 (Résultats du portefeuille d'investissement en ligne sécurisé 2020), Global Partnership to End Violence against Children (Partenariat mondial pour mettre fin à la violence à l'encontre des enfants), 2020. p. 2.
6. Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse (Rompre avec le mal au Kenya : données sur l'exploitation et l'abus sexuels des enfants en ligne), Global Partnership to End Violence against Children (Partenariat mondial pour mettre fin à la violence à l'encontre des enfants), 2021. p. 68.
7. Par exemple : les enfants en situation de handicap ou les enfants issus de groupes minoritaires marginalisés, les enfants des rues, les enfants réfugiés et les enfants migrants, entre autres. Cette question est abordée dans les thèmes transversaux ci-dessous. Vous trouverez plus d'informations sur le modèle et la liste de contrôle dans 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child (La « voix » ne suffit pas : conceptualiser l'article 12 de la Convention des Nations Unies relative aux droits de l'enfant), Laura Lundy, 2013.
8. Voir l'introduction sur l'importance du langage et des définitions ainsi que la section du glossaire.

3. Instaurer une chaîne de responsabilité

La responsabilité de la protection en ligne des enfants implique de nombreuses personnes, spécialités et organisations, notamment le gouvernement, les services de police, les entreprises, les éducateurs, l'aide psychosociale, les familles et les enfants. Certains maillons de la chaîne portent un plus grand poids de responsabilité.[9] Par exemple, un service qui est susceptible d'être consulté par des enfants ou d'avoir un impact sur eux doit examiner si l'une de ses caractéristiques présente un risque pour les enfants. Il doit le faire avant tout contact avec les enfants utilisateurs. On parle souvent de « conception sécuritaire » ou de « conception axée sur l'enfant ». La sécurité par défaut doit être la norme.

Assumer la responsabilité de la protection en ligne des enfants, c'est à la fois prévenir le mal avant qu'il ne se produise et prendre des mesures lorsque les choses tournent mal. Les mécanismes de plainte et de signalement doivent être accessibles et clairement signalés afin que les enfants, les personnes qui s'en occupent et les professionnels qui en ont besoin puissent les trouver et les utiliser facilement. Dans le cadre des systèmes professionnels en ligne, il convient de mettre en place des mécanismes permettant de suivre et d'évaluer les rapports de plaintes afin d'identifier et de traiter rapidement les sujets de préoccupation.

Les lois et les règlements doivent établir des cadres clairs en matière de prévention, de responsabilité et de réparation lorsque les choses tournent mal. Cela inclut le recueil de données concernant les rapports et les plaintes, afin qu'ils soient suivis et analysés pour améliorer le système. Les enfants et les parents/les personnes qui s'en occupent ne doivent pas être rendus responsables de la prévention ou de la prise en charge de risques et de préjudices qu'ils ne comprennent ou ne contrôlent que très peu. Le consentement ne peut être utilisé pour décharger les organisations publiques ou privées de leurs responsabilités en matière de protection en ligne des enfants. L'intégration de la protection en ligne des enfants dans les cadres existants pour la sécurité des produits[10], la protection des enfants[11], les droits des enfants[12] et les droits des consommateurs[13] peut contribuer à éviter les lacunes en matière de responsabilité et la duplication des ressources, des rôles et des responsabilités. Il ne doit pas y avoir de failles juridiques qui compromettent la protection en ligne des enfants.

Il est crucial que la protection en ligne des enfants soit intégrée dans tous les domaines politiques connexes, des plans nationaux pour le large bande aux programmes d'enseignement, d'une manière transparente, responsable et applicable. La création de silos peut conduire à des conflits réglementaires et à une fragmentation de l'élaboration et de la mise en œuvre des politiques.

4. Intégrer une conception axée sur l'enfant

La protection en ligne des enfants doit être intégrée dans la conception et le développement des technologies. La conception axée sur l'enfant intègre dès le départ la protection en ligne des enfants dans les services et les produits. Il s'agit notamment de veiller à ce que la protection en ligne des enfants soit prise en compte dans les exigences réglementaires en matière de conception et dans l'octroi de licences pour les nouvelles technologies[14]. La conception axée sur l'enfant est souvent appelée sécurité/droits/vie privée/éthique dès la conception.

L'application du principe de précaution[15] aux technologies susceptibles d'avoir un impact sur les enfants et les jeunes garantit que la sécurité des enfants en ligne est prise en compte dès le début. La Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST) de l'UNESCO a proposé une « définition de travail » du principe de précaution :

« Lorsque des activités humaines peuvent entraîner un dommage moralement inacceptable, scientifiquement plausible mais incertain, des mesures doivent être prises pour éviter ou réduire ce dommage.

---

9. Voir par exemple les Principes directeurs de l'ONU sur les entreprises et les droits de l'homme.
10. Centre de protection de l'enfance, Commission européenne, 2021.
11. Stratégie pour les droits de l'enfant, Conseil de l'Europe, 2021.
12. Directive sur les droits des consommateurs, Commission européenne, 2014.
13. Guidelines for policy-makers on Child Online Protection (Lignes directrices à l'attention des responsables politiques sur la protection en ligne des enfants), Union internationale des télécommunications, 2020.
14. Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes fondamentaux visant à lutter contre l'exploitation et les abus sexuels sur mineur en ligne), GOV.UK, 2021.
15. Voir Communication from the Commission on the precautionary principle (Communication de la Commission sur le principe de précaution), EUR-Lex, 2000 ; The precautionary principle: Definitions, applications and governance (Le principe de précaution : définitions, applications et gouvernance), Parlement européen, 2015.

Un préjudice moral inacceptable est un danger pour l'homme ou l'environnement qui est :

- Une menace pour la vie ou la santé humaine, ou
- Sérieux et effectivement irréversible, ou
- Inéquitable pour les générations actuelles ou futures, ou
- Imposé sans tenir suffisamment compte des droits de l'homme des personnes affectées. »[16]

Le principe de précaution doit orienter un cadre pour la sécurité et le respect de la vie privée dès la conception, afin de garantir que la protection en ligne des enfants et les droits des enfants soient intégrés dans la technologie dès la phase de conception. La conception axée sur l'enfant ne doit pas seulement être un concept éthique, mais une obligation légale.[17] Elle doit également être intégrée dans les critères de financement de la recherche et du développement qui peuvent affecter les droits en ligne des enfants.

La technologie et l'intelligence artificielle (IA) ont le potentiel d'améliorer la protection en ligne des enfants et de protéger leurs droits. Encourager le développement d'outils technologiques permettant de concrétiser les droits de l'enfant et d'améliorer la protection en ligne des enfants est un aspect important de la politique de protection en ligne des enfants. L'impact plus large de l'IA ou d'autres technologies conçues pour protéger les enfants doit être évalué à la lumière de tous les droits de l'enfant,[18] afin d'éviter de porter atteinte à d'autres droits tels que la vie privée et la non-discrimination.

Les enfants eux-mêmes sont extrêmement différents et l'ensemble des caractéristiques, des origines et des contextes des enfants doivent être pris en compte dans l'élaboration, la mise en œuvre et le contrôle de l'efficacité des politiques dans ce domaine. Une action efficace en matière de sécurité des enfants en ligne doit tenir compte des tensions perçues. Par exemple, dans les débats sur le chiffrement, les défenseurs de la protection contre l'exploitation et les abus sexuels sur mineur (CSEA) peuvent voir leurs arguments se heurter à ceux liés à la vie privée et à la protection des données. Ces conflits doivent être résolus dans la mesure où une issue pratique est possible, afin d'éviter de nombreuses années de débats cycliques alors que des enfants sont mis en danger ou subissent des préjudices. Dans de tels cas, « l'intérêt supérieur » de l'enfant doit primer.[19]

Il existe plusieurs cadres et processus qui favorisent l'application de la conception axée sur l'enfant dans l'élaboration des politiques, notamment le principe de précaution, les évaluations de l'impact sur l'enfant[20] et la consultation avec l'enfant.[21]

En outre, l'Association de normalisation de l'Institut des ingénieurs électriciens et électroniciens (IEEE-SA) a introduit une norme contenant des étapes pratiques que les entreprises peuvent suivre pour concevoir des produits et services numériques adaptés à l'âge des enfants,[22] et la Commission sur l'avenir numérique a indiqué comment le droit des enfants à jouer librement pourrait être renforcé dans un monde numérique en améliorant la conception des produits et services numériques. Les responsables politiques doivent toujours chercher à s'assurer que les produits et services minimisent les risques avant d'être mis à la disposition des enfants.

La conception sécuritaire et la définition des droits sont systémiques par nature et visent donc à protéger des millions d'enfants dès le départ, et non après coup.

5. Maintenir l'efficacité

La sécurité en ligne et les droits des enfants dans l'environnement numérique ne peuvent être véritablement efficaces que par des actions politiques concrètes, des ressources adéquates et leur application.

---

16. The Precautionary Principle (Les principes de précaution), World Commission on the Ethics of Scientific Knowledge and Technology (Commission mondiale de l'éthique des connaissances scientifiques et des technologies), 2005.
17. Voir par exemple l'article 25, Règlement général sur la protection des données, Union européenne, 2018.
18. Voir par exemple Observation générale n° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique, CIDE, 2021.
19. Convention relative aux droits de l'enfant, Haut-Commissariat des Nations Unies aux droits de l'homme, 1989. (Voir en particulier l'article 3, section 1, sur les droits de l'enfant).
20. Child Rights Impact Assessment (Évaluation de l'impact sur les droits de l'enfant), Digital Futures Commission (Commission sur l'avenir du numérique), 2021.
21. Child Rights Impact Assessment (Évaluation de l'impact sur les droits de l'enfant), Digital Futures Commission (Commission sur l'avenir du numérique), 2021.
22. IEEE 2089-2021 Standard for Age-Appropriate Digital Services Framework (Norme pour un cadre de services numériques adaptés à l'âge), IEEE SA, 2021.

La protection en ligne des enfants concerne un large éventail de domaines politiques, notamment les technologies de l'information et des communications (TIC), l'enseignement, la justice pénale, la santé, la réglementation de l'industrie, l'aide sociale et familiale, les entreprises, les droits de l'homme et l'égalité, le développement international, et bien d'autres encore. La coopération entre les différents ministères et agences travaillant dans des sphères politiques est donc essentielle pour une action efficace en matière de protection en ligne des enfants. Il convient d'établir un budget afin d'allouer des ressources à la politique, tant au sein des différents départements qu'entre eux. Une politique avec des fonds insuffisants, ou un partenariat sans capacité, c'est-à-dire qui n'existe que sur le papier, n'aboutira pas à une protection efficace en ligne des enfants.

Comprendre l'efficacité signifie examiner l'impact des politiques de protection en ligne des enfants. La surveillance, l'évaluation et le recueil de données sont essentiels à l'élaboration de bonnes politiques. Apprendre et partager les leçons de l'élaboration efficace des politiques au-delà des frontières est un moyen efficace de maximiser l'efficacité. Pour vérifier l'efficacité de la politique de protection en ligne des enfants, il faut consulter non seulement les principaux acteurs concernés, mais aussi les enfants, afin de comprendre comment les actions les affectent ou pourraient les toucher à l'avenir.[23] Il s'agit d'un processus continu.

Les politiques doivent être fondées sur des données et des preuves. Aussi bien les autorités compétentes que les entreprises privées doivent être tenues de recueillir et de partager des données pour faciliter la compréhension des problèmes de protection des enfants en ligne, dans le respect des lois et des principes relatifs à la protection des données. La protection en ligne des enfants est un domaine d'action relativement nouveau, de sorte que lorsque les preuves ne sont pas disponibles ou contestées, les responsables politiques doivent adopter une approche de précaution, ou se tourner vers d'autres contextes et adopter une approche « qui fonctionne ». Par exemple, avec les principes de santé et de sécurité, ou des cadres tels que INSPIRE: Seven Strategies for Ending Violence Against Children (INSPIRE : sept stratégies pour mettre fin à la violence contre les enfants).[24]

La protection en ligne des enfants n'est pas une question isolée. L'efficacité de la politique de protection en ligne des enfants dépendra de l'efficacité globale des institutions clés et de leur capacité à collaborer en vue d'une protection efficace. La responsabilisation effective en matière de protection en ligne des enfants en général, et de prévention de l'exploitation et des abus sexuels sur mineur en particulier, repose sur des systèmes judiciaires nationaux solides. La Réponse nationale modèle (RNM) présente des orientations sur cette question.

Les approches efficaces de la protection en ligne des enfants reposent également sur l'octroi de ressources adéquates aux institutions qui les soutiennent, notamment dans des domaines tels que l'aide psychosociale et la réglementation des TIC et des domaines connexes. Le respect effectif des droits de l'enfant par le biais d'une politique de sécurité en ligne dépend d'une législation efficace en matière de droits de l'homme, ainsi que d'une législation et d'une réglementation spécifiques, assorties d'organes de surveillance, afin de garantir les droits de l'enfant dans l'environnement en ligne et hors ligne.

Les responsables politiques doivent s'assurer que la capacité institutionnelle, les ressources et les mécanismes de responsabilité sont en place pour soutenir les politiques de protection en ligne des enfants. En cas de conflit, « l'intérêt supérieur » de l'enfant doit primer. Sans cela, même les meilleures politiques seront inefficaces.

Domaines d’action politique

1. Capacité institutionnelle

1a. Affirmer l’engagement public en faveur de la protection en ligne des enfants au plus haut niveau
Les dirigeants nationaux, notamment le Premier ministre ou le Président, doivent s’engager en faveur de la protection en ligne des enfants, tant sur la scène nationale qu’internationale.

23. Digital Futures Commission (Commission sur l'avenir du numérique), 5Rights Foundation, 2021.
24. INSPIRE Indicator Guidance and Results Framework (Guide des indicateurs et cadre des résultats d'INSPIRE), Organisation mondiale de la santé, 2018.

1b. Désigner un ministère ou un organisme chargé de diriger l'élaboration de la politique nationale de protection en ligne des enfants

Dans le monde entier, une série d'organismes et de ministères différents sont responsables de la politique de protection en ligne des enfants, et le choix de l'organisme ou du ministère peut affecter la manière dont la politique de protection en ligne des enfants évolue et donne la priorité à différents aspects de la protection en ligne des enfants. La protection en ligne des enfants est susceptible de relever de plusieurs ministères, mais il est important qu'un organisme responsable s'approprie le programme. Dans certains pays, la politique de protection en ligne des enfants est dirigée par le ministère responsable des TIC, dans d'autres par le ministère responsable de l'enfance et de la famille, et dans d'autres encore par le ministère de la justice. Il se peut que les groupes existants qui travaillent sur la violence à l'encontre des enfants (VEE) ou la cybersécurité puissent être élargis pour inclure l'expertise nécessaire afin d'éviter le travail en silo. L'organisme responsable peut être choisi pour son autorité, son expertise, ses ressources, sa capacité ou sa motivation, mais tout organisme responsable devra collaborer avec d'autres. Quel que soit le ministère qui assume la direction des opérations, il doit s'engager à adopter une approche holistique qui reflète les besoins primordiaux en matière de protection en ligne des enfants.

1c. Publier un manuel des définitions et du langage

Le ministère responsable désigné devra publier une liste complète des définitions et du langage qui reflète les définitions utilisées dans les meilleures pratiques internationales.[25]

1d. Mettre en place un Comité directeur national chargé de la protection en ligne des enfants

Le Comité directeur national chargé de la protection en ligne des enfants sera responsable de la mise en œuvre des politiques et du développement, et servira de point focal pour la coopération nationale et régionale. Il sera responsable de la boîte à outils pour la protection en ligne des enfants et de l'élaboration d'une stratégie pour la mettre en œuvre, ce que l'on pourrait appeler le plan d'action. Le Comité se penchera sur un large éventail de compétences couvrant divers domaines d'action, notamment l'enseignement, la santé, la justice, la protection des consommateurs, la protection des données, l'application de la loi, les TIC et les services à la famille et à l'enfance, entre autres, et supervisera la mise en œuvre et le respect des normes. Le Comité sera formellement tenu de coopérer avec tous ceux qui sont chargés de la sécurité des enfants ou de la cybersécurité, et rendra régulièrement compte au ministère responsable.

1e. Comprendre les acteurs de la protection en ligne des enfants

Les organismes chargés de l'application de la loi, les entreprises, le secteur tertiaire, les organisations de défense des droits de l'enfant, les établissements d'enseignement, les parents et les personnes en charge d'enfants, ainsi que les universités, ont tous des idées utiles et des intérêts importants en matière de sécurité en ligne des enfants. Dans certains contextes, la création d'un groupe de partenaires peut être utile pour soutenir le Comité dans ses activités et ancrer son plan d'action dans des scénarios réels. Dans d'autres contextes, des discussions informelles ou des appels aux preuves émanant d'un réseau ouvert d'acteurs peuvent être plus efficaces. Quoi qu'il en soit, le Comité directeur national pour la protection en ligne des enfants doit chercher à s'engager auprès des principaux acteurs susceptibles de soutenir ses activités. La coopération entre organismes doit être encouragée. L'objectif de l'engagement des partenaires est de se concentrer sur la mise en œuvre, et non sur l'élaboration de politiques.

1f. Définir les rôles et les responsabilités des partenaires

Il doit y avoir un cadre de corégulation qui définit les rôles et les responsabilités de tous les organismes développant et gérant les infrastructures numériques, les réseaux et les services, ainsi que les fonctions des ministères. Des normes minimales doivent être établies pour tous les participants à la chaîne de valeur, y compris les responsables de l'infrastructure, du matériel, des produits et services numériques et ceux qui les gèrent ou les utilisent quand ils interagissent avec les enfants. Ces normes doivent se concentrer sur la sécurité des enfants et la pleine réalisation des droits des enfants dans le monde numérique. La participation de la société civile et la consultation des enfants doivent être assurées dans les groupes de partenaires.

---

25. Voir par exemple Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminologie universelle : directives terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels), ECPAT International, 2016

1g. Définir les indicateurs de performance et l'évaluation
Chaque aspect du plan de mise en œuvre doit être associé à une autorité responsable (personne, institution, organisme) et à des ressources humaines et financières pour mener à bien la tâche envisagée. Il se peut que la même autorité soit responsable de plus d'un domaine politique, ou d'un seul domaine d'expertise. Des indicateurs clés de performance (ICP), des mécanismes d'évaluation et des structures de signalement claires doivent être introduits pour permettre au Comité directeur de superviser et de gérer les progrès. L'environnement numérique évoluant rapidement, les indicateurs clés de performance devront être régulièrement réévalués.

1h. Assurer l'intégration de la protection en ligne des enfants dans les domaines de la politique publique.
Tout plan national pertinent, tel qu'un Plan national pour le large bande ou un cadre d'habileté numérique, doit inclure une politique de sécurité en ligne pour les enfants dans le cadre de la stratégie de déploiement. Les plans qui se déroulent sur plusieurs années doivent être vérifiés à des étapes clés.

2 Cadre juridique et réglementaire

2a. Renforcer et appliquer les lois qui interdisent les infractions liées à la protection en ligne des enfants
Les lois et les procédures pénales facilitent les enquêtes et la poursuite des infractions en ligne qui violent le droit des enfants à la protection et devront être renforcées et modifiées conformément aux normes et aux meilleures pratiques internationales. Elles doivent inclure l'introduction de l'évaluation obligatoire des risques pour atténuer le potentiel de dommages, alourdir les sanctions et les cadres de fixation des peines lorsque cela est nécessaire. Elles doivent également inclure la possibilité de procédures de notification et de retrait. Les lois pénales relatives à la protection en ligne des enfants doivent être élaborées à la lumière de tous les droits des enfants, y compris leur droit d'être entendu et leur droit à la participation.[26]

2b. Adopter une réglementation sur la protection des données et instaurer des autorités de contrôle indépendantes, veiller à ce que les données des enfants soient adéquatement protégées et recueillies uniquement lorsque c'est nécessaire, avec des niveaux élevés de sécurité et d'attention
Une telle réglementation générale doit inclure un statut de catégorie spéciale applicable aux données relatives aux enfants, exigeant des niveaux plus élevés de protection et de garanties par défaut, ainsi que des protections contre l'utilisation commerciale inappropriée des données relatives aux enfants. Lorsque le consentement des enfants, ou des parents/personnes qui s'occupent d'eux, est demandé pour le recueil et le traitement en ligne des données des jeunes enfants, il doit être éclairé et significatif. Le recueil de données à des fins de protection doit faire l'objet d'une attention particulière dans des circonstances exceptionnelles, lorsque cela est dans l'intérêt supérieur de l'enfant.

2c. Renforcer les enquêtes pénales, les poursuites et les peines pour l'exploitation sexuelle ou les abus en ligne des enfants[27]
Les organismes de justice pénale responsables des infractions liées à la protection en ligne des enfants doivent être formés aux questions de protection en ligne des enfants afin de favoriser une meilleure prévention, des poursuites efficaces et des condamnations appropriées, ainsi qu'une meilleure compréhension de l'impact sur les victimes. Les capacités des équipes d'enquête et d'intervention concernées doivent être évaluées et renforcées pour détecter, prévenir et répondre aux menaces de cybersécurité, en particulier celles liées à la protection en ligne des enfants. Les systèmes de justice pénale doivent être en mesure d'assurer un accès rapide à la justice.

2d. Revoir et renforcer les systèmes de justice pour les jeunes
Veiller à ce que la loi soit claire et proportionnée afin de réduire au minimum le risque que des enfants ne se retrouvent dans une situation de conflit avec la loi dans le contexte de la protection en ligne des enfants. Lorsque des enfants font l'objet de sanctions pénales liées à la protection en ligne des enfants, par exemple en cas de cyberharcèlement ou d'abus sexuel basé sur l'image, le système judiciaire doit tout mettre en œuvre pour éviter que les enfants ne soient criminalisés et fournir un soutien et une représentation juridique adéquats aux enfants qui se retrouvent en conflit avec la loi afin de protéger leurs droits.

---

26. Par exemple, les cadres juridiques qui ne précisent pas clairement si les images sexuelles autogénérées échangées entre enfants sur une base consensuelle seront considérées comme du matériel illégal concernant l'abus sexuel sur mineur. Même si les enfants ne sont pas poursuivis dans la pratique, cette incertitude juridique avec une criminalisation potentielle peut porter atteinte à la confiance, au contrôle et aux droits d'autonomie.
27. L'exploitation et abus sexuels sur mineur (CSEA) consiste en ce qu'un enfant est forcé ou persuadé de prendre part à des activités sexuelles. Cela peut impliquer un contact physique ou à des activités sans contact et peut se produire en ligne ou hors ligne.

2e. Identifier et ratifier les traités et protocoles internationaux relatifs à la protection en ligne des enfants
La création d'un écosystème durable pour la protection en ligne des enfants exige une approche multipartite et une participation à l'échelle mondiale. Chaque pays doit identifier et ratifier les protocoles et traités internationaux et régionaux pertinents et prendre des mesures pour mettre en œuvre leurs dispositions.

2f. Renforcer la capacité des organismes de maintien de l'ordre public
Les lacunes dans l'application de la loi et le système judiciaire doivent être identifiées, et des mesures doivent être mises en place pour accroître la sensibilisation, le signalement et la mise en œuvre des poursuites. La formation internationale et le partage des compétences doivent être recherchés dans la mesure du possible, et la coordination et la collaboration intersectorielles entre l'industrie et les services chargés de l'application de la loi doivent être encouragées.

3 Données personnelles et identité

3a. Mettre en place ou s'assurer que les cadres de protection des données existants sont efficaces pour assurer une protection spécifique des données relatives aux enfants
Les droits des enfants dans l'environnement en ligne sont intimement liés à la façon dont leurs données sont recueillies, sauvegardées et utilisées. La législation et la réglementation en matière de protection des données relatives aux enfants doivent être accessibles, efficaces et capables d'évoluer pour faire face aux risques émergents.[28]Cela suppose non seulement d'établir le cadre juridique et réglementaire, mais aussi de s'assurer qu'il fonctionne dans la pratique et qu'il est appliqué en conséquence.

3b. Établir des protocoles et des limites à l'utilisation de la prise de décision automatisée qui peut affecter les enfants
Les normes, lois et codes de pratique doivent garantir que les enfants bénéficient des systèmes automatisés et ne sont pas pénalisés par la prise de décision automatisée.[29] Il est particulièrement important d'éviter le risque de discrimination dans la prise de décision automatisée. Ces protocoles et ces limites peuvent s'appliquer dans le cadre de la justice pénale, la protection sociale, la santé et la médecine, l'enseignement et le secteur privé, entre autres.

3c. Garantir des protections juridiques et réglementaires adéquates concernant les données biométriques des enfants
Les pouvoirs publics et les organismes de réglementation doivent établir des protocoles juridiques et réglementaires appropriés pour l'utilisation des données biométriques des enfants, ainsi que des limites à cette utilisation, à la lumière des principes des droits de l'enfant, de la limitation des objectifs et des exigences de la politique de protection en ligne des enfants.

3d. Établir des directives, des lois et des règlements clairs sur les pratiques susceptibles d'affecter la représentation des enfants
Créer des cadres juridiques empêchant le ciblage et le suivi personnalisés des enfants à des fins commerciales sur la base de leurs données à caractère personnel. Établir des codes relatifs à l'utilisation de systèmes de recommandation et d'autres processus ou technologies de prise de décision automatisée susceptibles d'orienter le comportement des enfants, de modeler leurs préférences et leurs opinions, de porter atteinte à leur réputation ou de limiter leur expérience.[30]

3e. Mettre en place une surveillance et un suivi efficaces
Créer des organismes et des systèmes capables de recueillir des informations relatives à la protection en ligne des enfants et de garantir la transparence et la mise en œuvre effective des droits et des protections des enfants par les entreprises, les gouvernements et d'autres organisations.

3f. Établir des cadres pour assurer la transparence
La surveillance doit être assurée par un organisme de réglementation désigné, disposant de ressources suffisantes, de la capacité et de l'expertise nécessaires pour comprendre les systèmes utilisés et leur impact sur les droits de l'enfant. L'organisme de contrôle doit également avoir accès à des chercheurs et des experts indépendants.

---

28. Règlement général sur la protection des données, Union européenne, 2018.
29. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert (Un expert des droits de l'homme de l'ONU met en garde contre la dérive du monde vers une dystopie de l'aide sociale numérique), Bureau du Haut Commissariat des Nations Unies aux droits de l'homme, 2019.
30. Voir, par exemple, YouTube Data Breach Claim (Réclamation pour violation de données sur YouTube), McCann contre Google, 2021.

4 Systèmes de réponse et d'assistance

4a. Avis et retrait

Les institutions gouvernementales collaboreront avec des experts, la communauté chargée de l'application de la loi et l'industrie afin d'établir et de contrôler des protocoles efficaces pour la notification et le retrait de contenu illégal et nuisible. Cela nécessitera, entre autres, l'élaboration de protocoles pour garantir que les fournisseurs de services Internet (FSI) locaux soient autorisés à restreindre l'accès aux hôtes qui ne retirent pas les contenus signalés ou qui enfreignent de manière persistante les lois ou autres exigences réglementaires relatives à la protection en ligne des enfants.

4b. Établir des processus pour la gestion du risque des délinquants en relation avec l'exploitation et les abus sexuels sur mineur

Il convient de mettre en place un processus efficace de gestion des délinquants associant plusieurs acteurs, en s'inspirant des normes internationales de bonne pratique. Les forces de l'ordre et les autres praticiens de la justice pénale doivent être formés à reconnaître les comportements délinquants et à enquêter à leur sujet. La gestion des risques des délinquants est un élément essentiel de la protection en ligne des enfants, car des personnes individuelles ou des groupes de délinquants peuvent toucher en ligne un grand nombre d'enfants victimes.

4c. Fournir des ressources suffisantes pour le soutien psychosocial des enfants victimes primaires et secondaires et de leurs familles

Les organisations formant des praticiens dans les domaines de la santé mentale, de la psychologie et du travail social qui travaillent avec des enfants vulnérables doivent être tenues d'avoir une compréhension de base des questions de protection en ligne des enfants.[31] La protection en ligne des enfants doit être intégrée dans des systèmes plus larges de sécurité et de protection des enfants, tels que la sauvegarde dans les écoles ou la violence à l'encontre des enfants (VEE).

4d. Mettre en place des cadres de détection et de protection des victimes

Un objectif clé de la prévention du préjudice causé en ligne sera de prendre en compte les besoins des enfants vulnérables et de savoir comment les soutenir de manière optimale. Les centres One Stop font office d'institution de coordination pour les victimes d'abus : ils permettent d'accéder à une série de services essentiels, de l'aide médicale à l'aide juridique, en un lieu centralisé. Ils offrent un cadre pour les procédures de sauvegarde et de protection des enfants, apportent un soutien aux victimes et transmettent rapidement les signalements de crimes en ligne aux autorités compétentes.[32]

4e. Veiller à ce que les cadres pertinents ne criminalisent pas les enfants

Il est important d'établir des cadres appropriés pour gérer les enfants qui peuvent se trouver eux-mêmes en conflit avec la loi dans le contexte de la protection en ligne des enfants, par exemple, dans les cas de cyberharcèlement, de diffusion d'informations malveillantes ou de piratage. Dans la mesure du possible, les enfants devraient être orientés hors du système de justice pénale, et les possibilités de conseil ou de justice réparatrice devraient être privilégiées. Il convient de veiller tout particulièrement à ce que la situation de l'enfant soit parfaitement comprise. Par exemple, le comportement d'un enfant peut être le résultat d'une intimidation, d'une sollicitation sexuelle ou d'une autre forme de coercition.

---

31. What Works to Prevent Violence Against Women and Girls Evidence Reviews Paper 3: Response mechanisms to prevent violence (Ce qui marche pour prévenir la violence contre les femmes et les filles, Document d'analyse 3 : mécanismes d'intervention pour prévenir la violence), What Works, 2015. p. 28.
32. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prévenir et combattre l'exploitation et les abus sexuels sur mineurs (CSEA) : un modèle de réponse nationale), WeProtect Global Alliance, 2016.

5 Les entreprises et les droits de l'enfant :

5a. Mettre en œuvre la sécurité, les droits et l'éthique dès le stade de la conception

Des normes et des codes de pratique devront être élaborés pour exiger des concepteurs de produits, des fabricants et des fournisseurs de services qu'ils respectent les droits de l'enfant et contribuent à la sûreté et à la sécurité en ligne des enfants. Les conditions générales devront refléter l'intérêt supérieur de l'enfant. Entre autres, les normes et les codes de pratiques auront pour objectif d'empêcher qu'on propose aux enfants du contenu ou des contacts nocifs ou inappropriés ; de protéger la vie privée en ligne des enfants dans le système ou au niveau du périphérique ; de répondre aux préoccupations de sécurité soulevées par l'Internet des objets, les jouets et les services liés à la fonction de streaming, afin de garantir que les entreprises privées ont envisagé, par le biais d'une évaluation de l'impact sur les enfants, un processus de réduction des risques et d'atténuation des effets qui conduit à proposer aux enfants un service adapté à leur âge.

5b. Adoption de normes minimales[33]

L'industrie a la responsabilité de veiller à ce que les enfants bénéficient d'une protection en ligne. Cela oblige à créer un espace en ligne sûr et accessible aux enfants, et pas seulement à empêcher l'accès à des contenus nocifs. Les entreprises seront tenues de montrer quelles procédures et considérations spéciales elles ont adoptées pour assurer la sécurité et le respect des droits des enfants (en utilisant le cadre de risque 4C[34]) lorsqu'elles élaborent et établissent leurs services en ligne.[35] Un code doit être créé par le ministère ou l'organisme responsable, supervisé par le Comité directeur. Ces normes seront obligatoires et exécutoires.

5c. Application d'une classification par tranche d'âge

L'application de la classification cohérente par âge des contenus commerciaux, des médias de service public, des jeux et des activités en ligne propose une approche transparente et efficace pour gérer le contenu et les services qui ont un impact sur les enfants. Une telle démarche peut être nécessaire pour les biens et les services concernés et pour le contenu adapté aux différentes tranches d'âge. Un système de vérification de l'âge ou la création d'espaces réservés aux adultes seront nécessaires pour des contenus interdits ou des activités qui ne conviennent pas aux enfants. Cela peut inclure notamment des filtres de contenu pour bloquer les contenus indésirables.[36]

5d. Mettre en place des systèmes de modération et de notification

Des mécanismes permettant d'identifier des contenus choquants ou inappropriés seront requis de la part des fournisseurs de services, et des systèmes de contrôle transparents et robustes doivent être mis en place pour tous les services en ligne, y compris des mécanismes de retrait. Une ligne d'assistance téléphonique publique gratuite sera disponible pour les notifications et l'accès à un soutien et des conseils spécialisés. Les mécanismes de notification doivent être aisément accessibles aux enfants. Des systèmes de signalement devront être envisagés comme outil supplémentaire.

5e. Assurer la protection des enfants contre les pressions commerciales

Les efforts déployés pour protéger les enfants contre les pressions commerciales comprennent : la promotion d'une conception appropriée à l'âge ; la désactivation de la publicité ciblée ; le partage avec des tiers ; la sensibilisation au contexte dans lequel les enfants grandissent. Les produits et les services qui renforcent les droits et la protection en ligne des enfants peuvent être certifiés, et des mesures peuvent être prises contre les créateurs de produits et de services qui ne respectent pas ces valeurs.

5f. Veiller à ce que les principes de conception axée sur l'enfant soient appliqués pour réduire au minimum les risques liés à la protection en ligne des enfants

Cette démarche inclut, par exemple, la possibilité de mettre des adultes étrangers en contact avec des enfants, la publicité ciblée pour les jeux de hasard ou encore la recommandation de contenus nocifs.
La protection en ligne des enfants doit être intégrée au stade de la conception pour éviter que des problèmes ne surgissent plus tard.

---

33. Voir, par exemple, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principes volontaires visant à lutter contre l'exploitation et les abus sexuels sur mineur en ligne), GOV.UK, 2020.
34. Voir la section sur l'atténuation des risques et des dommages.
35. Les droits de l'enfant dans les évaluations d'impact, Fonds des Nations Unies pour l'enfance, 2013.
36. But how do they know it is a child? (Mais comment savent-ils que c'est un enfant ?), 5Rights Foundation, 2021.

6 Formation

6a. Offrir une formation, le perfectionnement des compétences et un mentorat à tous les acteurs de la protection en ligne des enfants

Des premiers intervenants aux juges, tous les acteurs de la chaîne de maintien de l'ordre public et les professionnels qui travaillent avec les enfants dans d'autres milieux tels que l'enseignement ou la santé doivent être conscients de la protection en ligne des enfants. Ils devront bénéficier d'une formation complète, y compris sur la façon dont la protection en ligne des enfants concerne leur rôle particulier, comment comprendre le comportement choquant, et comment assurer l'accès à l'aide aux victimes.

6b. Offrir une formation spécialisée pour le soutien psychosocial et l'identification des signes de toute la gamme des questions de protection en ligne des enfants

Pour être efficaces, les praticiens concernés doivent bénéficier d'une formation en ligne sur la sécurité des enfants, une formation sur les politiques de protection et de sauvegarde des enfants ainsi qu'une formation sur les conseils destinés aux enfants et aux familles. La sensibilisation à la protection en ligne des enfants devra être intégrée dans les cadres existants pour la protection des enfants. Les professionnels qui travaillent avec des enfants dans l'enseignement, la santé, les services communautaires et d'autres paramètres doivent être formés à reconnaître les signes et les symptômes de problèmes de protection en ligne des enfants.

6c. Développer des programmes d'enseignement supérieur

Les sessions relatives à la protection en ligne des enfants devront obligatoirement faire partie de l'enseignement, du travail social, de la santé, de la psychologie et d'autres programmes d'études pertinents dans les universités ou les établissements d'enseignement publics et privés. Il convient de réexaminer régulièrement l'efficacité de cet enseignement à la lumière des progrès réalisés en matière de formation à la protection en ligne des enfants et des questions émergentes. Les programmes scolaires doivent couvrir tous les aspects de la protection en ligne des enfants, tels que définis dans la présente politique.

6d. Encourager le perfectionnement professionnel

Des programmes de formation continue sur la protection en ligne des enfants et la protection des enfants pour les professionnels travaillant dans les domaines pertinents seront établis, revus régulièrement et mis à jour pour suivre le rythme des nouvelles technologies et aborder les nouveaux obstacles ainsi que les nouvelles préoccupations à mesure qu'ils apparaissent.

7 Enseignement

7a. Désigner des responsables de la protection de l'enfance

Chaque école doit désigner un responsable de la protection de l'enfance.[37] Chaque responsable doit recevoir une formation sur les procédures de protection des enfants et une formation spécifique à la protection en ligne des enfants. Les responsables seront chargés de veiller à ce que les politiques de protection en ligne des enfants (y compris les procédures de protection et les systèmes de signalement anonyme) soient adoptées, mises en œuvre et appliquées dans les écoles. Le responsable de la protection de l'enfance sera le point de contact concernant les préoccupations liées à la protection de l'enfance et à la protection en ligne des enfants, et transmettra les préjudices signalés aux autorités compétentes. Les responsables doivent également faciliter les plans d'intervention, afin de protéger les enfants contre tous les dangers qui les menacent.

7b. Promouvoir un enseignement numérique accessible

Promouvoir les contenus, y compris les programmes de pair à pair, qui sont conçus et montrés pour aider les enfants à développer des compétences numériques et leur donner les moyens de bâtir des communautés respectueuses qui favorisent la sécurité en ligne des enfants. Le système d'enseignement numérique devra être holistique et couvrir l'éducation aux données et aux médias, ainsi que les questions de protection, en particulier les questions de sexualité et de consentement. L'enseignement sera également étendu aux parents/personnes en charge d'enfants afin de les aider à promouvoir la protection en ligne des enfants.

---

37. Il peut s'agir d'un membre du comité de sécurité de l'école, d'un éducateur ou d'un membre du comité de protection de l'enfance d'un village ou d'une communauté où les écoles sont représentées.

7c. Promouvoir le contenu pédagogique
Au rythme de la généralisation de l'adoption numérique, les élèves et les enseignants apprendront les compétences nécessaires pour interagir avec les systèmes numériques et tirer pleinement profit du contenu des programmes, tant dans les langues locales qu'internationales.

7d. Promouvoir l'habileté numérique
Un programme d'habileté numérique sera introduit dans les programmes scolaires. Le programme sensibilisera les enfants à la manière dont leurs données peuvent être utilisées et leur fournira une compréhension de base de l'économie des données. Il mettra l'accent sur l'utilisation positive, autonome et créative des technologies numériques par les enfants et l'encouragera ; il définira clairement les risques, les avantages et les conséquences sociales de l'utilisation des technologies ; il visera à garantir que les mesures de protection et de prévention sont largement diffusées, comprises et appliquées. L'enseignement de l'habileté numérique devra préciser clairement les différentes parties prenantes responsables de la sécurité en ligne.

7e. Promouvoir la pensée critique
L'enseignement destiné aux enfants et aux parents/personnes en charge d'enfants sur la pensée critique ainsi que la sensibilisation aux risques de la désinformation en ligne devront être intégrés dans l'enseignement de l'habileté numérique. Cette démarche doit inclure un enseignement plus large pour promouvoir la compréhension et la sensibilisation aux droits de l'homme, en particulier les droits de l'enfant, et la manière dont ils fonctionnent en ligne et hors ligne.[38]

7f. Introduire des procédures formelles de protection en ligne pour les enfants dans les écoles
La formation à la protection en ligne des enfants doit faire partie intégrante des diplômes d'enseignement, tant au niveau de l'école primaire que de l'école secondaire, et faire l'objet d'une formation continue en service. Tous les enseignants doivent suivre une formation obligatoire sur la protection en ligne des enfants, connaître la politique de l'école en matière de protection en ligne des enfants et donner des cours sur la protection en ligne des enfants aux élèves. Toutes les écoles doivent nommer un responsable de la protection en ligne des enfants, chargé de défendre les normes de protection en ligne des enfants et d'assumer la responsabilité de l'application de la politique de l'école en matière de protection en ligne des enfants.

8 Sensibilisation du public et communications

8a. Créer un programme de sensibilisation du public
Les stratégies de sensibilisation aideront les personnes à comprendre et à gérer la question de la protection en ligne des enfants tout en profitant de l'espace virtuel. Les supports à produire doivent faire apparaître clairement les principes de la protection en ligne des enfants et les mesures à prendre pour comprendre les risques, limiter les dommages, signaler les infractions et demander réparation. Ces informations seront fournies en termes simples sur les sites Web officiels. Les messages et le matériel ciblés doivent être conçus en consultation avec les enfants, les jeunes et les parents/personnes en charge d'enfants. Ce plan doit prendre en compte les besoins spécifiques des parents/personnes en charge d'enfants et des enfants, en accordant une attention particulière aux enfants les plus jeunes et les plus vulnérables, y compris ceux qui ont des difficultés d'apprentissage ou ceux qui ne bénéficient pas de l'aide de leurs parents. L'enseignement de pair à pair est une stratégie bénéfique pour apprendre aux enfants de tous âges à connaître leurs droits et leurs responsabilités en ligne. Ce programme de messagerie publique peut aider les enfants et les adultes à comprendre les problèmes et à faire des choix judicieux au sujet de leurs interactions en ligne, mais ne remplace pas l'enseignement formel, la formation professionnelle, la conception sécuritaire ou la responsabilité de l'entreprise. Ces informations devront couvrir l'ensemble des questions de protection en ligne des enfants, telles que définies dans la présente politique.

38. Voir l'article 29 de la Convention relative aux droits de l'enfant, et les articles pertinents d'observation générale.

Les cinq thèmes transversaux
1. Identification des risques et atténuation des dommages
2. Promouvoir l'accès, l'accessibilité et l'inclusion
3. Instaurer une chaîne de responsabilité et de collaboration
4. Intégrer une conception axée sur l'enfant
5. Maintenir l'efficacité

Les dix domaines d'action politique
1. Capacité institutionnelle
2. Cadre juridique et réglementaire
3. Données personnelles, identité et autonomie
4. Systèmes de réponse et d'assistance
5. Responsabilité de l'entreprise
6. Formation
7. Enseignement
8. Sensibilisation du public et communications
9. Recherche et développement
10. Coopération internationale

8b. Fournir des informations accessibles et du matériel pédagogique
L'enseignement relatif à la protection en ligne commencera dès la petite enfance et se développera en fonction de l'évolution des besoins des enfants au fur et à mesure de leur croissance : des supports spécifiques seront produits pour guider et aider les enfants de tous âges, leurs familles et les personnes qui s'occupent d'eux. Les supports d'information encourageront l'utilisation positive de la technologie numérique, de la sexualité et du consentement, et tiendront compte des besoins de tous les enfants, quels que soient leur sexe, leur âge, leurs revenus ou leur origine. Les informations fournies par des tiers refléteront les droits et principes des enfants et viseront à aider les enfants de tous âges à se familiariser avec les risques et leurs droits en ligne. Les supports doivent indiquer clairement que les enfants et les utilisateurs ne sont pas responsables quand il leur arrive quelque chose de mal. Les groupes communautaires, les clubs de jeunes, les familles, les institutions religieuses et les plateformes numériques joueront tous un rôle déterminant dans la sensibilisation à la protection en ligne des enfants et l'enseignement informel au niveau communautaire.

8c. Sensibiliser les médias à la protection en ligne des enfants
Il convient de mettre à disposition des informations pour favoriser la couverture par les médias des questions de protection en ligne des enfants d'une manière adaptée à ces derniers. Les entreprises de médias et de divertissement devront être sensibilisées à la protection en ligne des enfants et être encouragées à soutenir les campagnes de sensibilisation du public, le cas échéant, de manière équilibrée, responsable et informative. Il est important d'encourager la prise en compte de l'ensemble des questions relatives à la protection en ligne des enfants, et pas seulement des gros titres les plus dramatiques à ce sujet.

8d. Faire participer les parents, les personnes en charge d'enfants et les enfants à des discussions sur la protection en ligne de ces derniers.
Les parents/les personnes en charge d'enfants et les familles doivent avoir les moyens de comprendre et d'agir sur la protection en ligne des enfants à leur domicile. Des consultations avec les familles et les enfants sont nécessaires pour identifier les problèmes, les solutions et les moyens de sensibiliser la communauté à la protection en ligne des enfants de manière efficace.

9 Recherche et développement

9a. Établir des cadres de recherche sur la protection en ligne des enfants
Les pays doivent établir un fonds de recherche central pour développer un programme de recherche avec des termes de référence clairement identifiés et des objectifs qui restent d'actualité, afin de permettre une recherche continue sur la protection en ligne des enfants sur une large gamme de questions pertinentes. Dans la mesure du possible, les pays doivent s'entraider et coopérer en matière de recherche et de développement sur la protection en ligne des enfants. L'analyse des lacunes doit permettre de garantir que les ressources sont affectées en priorité aux domaines où les besoins sont les plus importants et d'éviter les redondances inutiles. La recherche doit être mise à la disposition des partenaires régionaux ou internationaux, en particulier ceux qui ont le moins de ressources.

9b. Innovation continue
Les résultats de la recherche permettront de développer des produits et des services intégrant une conception sécuritaire, d'évaluer les pratiques de protection en ligne des enfants et de comprendre les expériences et les solutions en ligne des enfants dans le contexte national.

9c. Créer des centres d'excellence en matière de recherche et de développement sur la protection en ligne des enfants
Les pays devront développer des centres d'excellence au sein des institutions existantes (universités, établissements de santé, centres d'innovation) qui peuvent partager et coopérer au développement d'outils, de services et de compétences liés à la protection en ligne des enfants par le biais d'un engagement national, régional et international.

9d. Établir des cadres éthiques solides en recherche et développement en matière de protection en ligne des enfants[39]
Les pays devront élaborer des lignes directrices à l'attention des chercheurs travaillant sur la protection en ligne des enfants, y compris la prise en compte effective des droits de l'enfant dans le cadre du processus de recherche. Cela doit inclure des directives claires sur la collecte des données et les implications sur l'éthique et les droits de traitement des données des enfants. L'intérêt de l'enfant doit être la principale préoccupation dans les cadres éthiques de recherche et de développement sur la protection en ligne des enfants, y compris dans les situations d'accès d'intérêt public.

9e. Établir des cadres pour la collecte d'informations
Les régulateurs travaillant dans le domaine de la protection en ligne des enfants doivent mettre en place des cadres pour la collecte d'informations qui leur permettront de suivre et d'évaluer l'efficacité de la protection en ligne des enfants dans différents contextes et l'impact qu'elle a sur différents groupes d'enfants. Le suivi et l'évaluation des actions en faveur de la protection en ligne des enfants doivent faire partie du processus de recherche et de développement.

9f. Permettre l'accès aux données des entreprises privées dans l'intérêt public
Il convient de créer des cadres dans lesquels les médias sociaux et autres entreprises doivent partager leurs données pour soutenir la recherche dans les meilleurs intérêts de l'enfant.

9g. Veiller à ce que les données et les statistiques soient pertinentes dans le contexte
Les modèles statistiques doivent refléter la situation locale, afin de favoriser le niveau de compréhension et de réponse aux problèmes nationaux. Ils doivent permettre le suivi des impacts transfrontaliers.

10 Coopération internationale

10a. Établir des cadres de relations formels (par exemple, un mémorandum d'entente) avec les communautés régionales et mondiales de la protection en ligne des enfants
Le renforcement de la coopération internationale pour améliorer la protection en ligne des enfants dans le monde entier est essentiel pour garantir la sécurité mondiale. Les pays devraient formaliser des collaborations pour des investissements conjoints en partenariat public et privé dans des domaines liés à la cybersécurité, au renforcement des capacités en matière de protection en ligne des enfants, à l'innovation, à l'application de la loi, au système judiciaire et à l'enseignement, entre autres.

10b. Approuver les instruments juridiques régionaux et internationaux qui encouragent la coopération en matière de sécurité en ligne des enfants
Les pays doivent identifier les principaux instruments régionaux et internationaux qui leur permettront de coopérer avec d'autres pays en matière de protection en ligne des enfants. Cela doit inclure, entre autres choses : les accords internationaux sur la coopération en matière d'application de la loi ; les meilleures pratiques internationales ; les programmes internationaux susceptibles de fournir des ressources pour la coopération en matière de protection en ligne des enfants ; l'accès à tous les droits de l'homme ou normes connexes qui faciliteront la coopération entre les pays.

---

39. Children and the Data Cycle: Rights and Ethics in a Big Data World (Les enfants et le cycle des données : droits et éthique dans un monde de Big Data), Fonds des Nations Unies pour l'enfance, 2017.

10c. Identifier les pays et organisations partenaires qui peuvent fournir des modèles et une assistance appropriés pour le développement de la protection en ligne des enfants
Il n'est peut-être pas nécessaire de recommencer l'élaboration de la politique depuis le début. Les pays sont invités à rechercher des exemples pertinents de cadres et d'outils de protection en ligne pour les enfants qu'ils peuvent utiliser et adapter à leur propre contexte. Le partage d'informations sur les défis et les problèmes rencontrés dans le domaine de la protection en ligne des enfants peut s'avérer très précieux pour la planification, l'élaboration et la mise en œuvre des politiques de protection en ligne de ces derniers.

10d. Accompagner les autres pays dans l'élaboration de politiques de protection en ligne des enfants
Le cas échéant, partager des lois modèles, des cadres réglementaires, des leçons apprises ou d'autres supports qui peuvent être utilisés par d'autres pays pour développer leurs propres cadres et politiques de protection en ligne des enfants.[40]

40. Voir par exemple le Australian eSafety Commissioner's International Leadership and Collaboration Materials (Supports pour le leadership et la collaboration internationale du commissaire australien à la cybersécurité), 2021.

5RIGHTS FOUNDATION

End Violence Against Children