

# POLITIQUE DE L'UNION AFRICAINNE SUR LA SÉCURITÉ ET L'AUTONOMISATION EN LIGNE DES ENFANTS







**POLITIQUE DE L'UNION AFRICAINE  
SUR LA SÉCURITÉ ET  
L'AUTONOMISATION EN LIGNE  
DES ENFANTS**

**Adoptée par la 44e session ordinaire du Conseil  
exécutif de l'Union Africaine**

Février 2024 - Addis-Abeba, Éthiopie

# TABLE DES MATIÈRES

<b>GLOSSAIRE DES DÉFINITIONS</b> .....	<b>2</b>
<b>I. INTRODUCTION</b> .....	<b>4</b>
<b>II. CONTEXTE</b> .....	<b>5</b>
II.I ACCES AU MONDE NUMERIQUE POUR LES ENFANTS D’AFRIQUE .....	5
II.II L’OPPORTUNITE.....	5
II.III LES RISQUES .....	6
II.IV FACTEURS INFLUENÇANT LA SECURITE EN LIGNE DES ENFANTS .....	7
II.V CADRES ET OUTILS EXISTANTS POUR LA PROTECTION EN LIGNE DES ENFANTS EN AFRIQUE .....	8
<b>III. PRINCIPES DIRECTEURS</b> .....	<b>10</b>
<b>IV. OBJECTIFS DE LA POLITIQUE</b> .....	<b>12</b>
<b>V. PLAN DE MISE EN ŒUVRE</b> .....	<b>13</b>

## GLOSSAIRE DES DÉFINITIONS

Terme	Définition
Agenda 2063 de l'UA	Le programme et le plan directeur visant à transformer l'Afrique en une puissance mondiale de l'avenir.
Stratégie continentale de l'éducation pour l'Afrique (CESA) 2016-2025 de l'UA	La stratégie vise à réorienter les systèmes d'éducation et de formation en Afrique afin de répondre aux besoins en termes de savoir, de compétences, d'aptitudes, d'innovation et de créativité nécessaires pour cultiver les valeurs fondamentales de l'Afrique et promouvoir le développement durable aux niveaux national, sous-régional et continental.
Stratégie de transformation numérique de l'UA	Une stratégie prospective globale sur dix ans (2020-2030) qui vise à exploiter le potentiel des technologies numériques, des données et de l'innovation afin d'accélérer la transformation de l'Afrique d'aujourd'hui en une Afrique en paix, intégrée et prospère.
Enfant	Toute personne âgée de moins de 18 ans, conformément à la Convention des Nations Unies relative aux droits de l'enfant.
Matériel relatif aux abus sexuels sur enfants (CSAM)	Images ou vidéos montrant un enfant de manière sexualisée, engagé ou représenté dans une activité sexuelle explicite.  NB : Cette terminologie remplace le terme utilisé précédemment « pédopornographie », qui est désormais largement reconnue comme inexacte et ne rend pas compte du préjudice intrinsèque à cet acte. <sup>1</sup>
Responsabilité sociale des entreprises	La responsabilité sociale des entreprises (RSE) est un modèle d'entreprise autorégulé qui permet à une société d'être socialement responsable vis-à-vis d'elle-même, de ses parties prenantes et du public.
Cyber-agression	Actes préjudiciables commis 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 un groupe.
Cyber-intimidation	Comprend l'envoi, la publication ou le partage de contenus négatifs, nuisibles, faux ou vicieux, notamment des informations personnelles ou privées sur un individu ou un groupe d'individus, dans le but de causer de l'embarras ou de l'humiliation.
Accessibilité numérique	L'accessibilité numérique est la capacité d'un site web, d'une application mobile ou d'un document électronique d'offrir une navigabilité et une compréhension faciles à un large éventail d'utilisateurs, notamment des personnes vivant avec des handicaps visuels, auditifs, moteurs ou cognitifs.

<sup>1</sup> Voir INHOPE : Qu'est-ce que le matériel relatif aux abus sexuels sur enfants ? <https://www.inhope.org/EN/articles/child-sexual-abuse-material>

Plate-forme numérique	Infrastructures en ligne basées sur un logiciel qui facilitent les interactions et les échanges entre les utilisateurs.
Compétences numériques	Ensemble de compétences, d'outils et de connaissances nécessaires pour utiliser les réseaux, les dispositifs numériques et différentes applications sur les médias en ligne qui facilitent la gestion de l'information conformément aux exigences spécifiques de l'environnement de travail, de l'environnement d'apprentissage et des situations de résolution de problèmes.
Environnement numérique	Tous les sites web, services, applications et autres formes d'espaces auxquels on accède à l'aide de la technologie.
Observation générale n° 25	Le Comité des droits de l'enfant des Nations Unies clarifie la manière dont la Convention relative aux droits de l'enfant s'applique à l'environnement numérique.
Préjudice	Impact négatif sur une personne, tel qu'un préjudice financier, physique ou émotionnel.
Exploitation sexuelle des enfants en ligne	L'utilisation de la technologie ou de l'internet pour faciliter les abus sexuels sur enfants, y compris la production et le partage de matériel d'abus sexuels sur enfants en ligne.
Données à caractère personnel	Toutes informations concernant une personne physique identifiée ou identifiable par lesquelles cette personne peut être identifiée, directement ou indirectement, en particulier par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, mentale, génétique, économique, culturelle ou sociale de cette personne.
Risque	Une situation ou un ensemble de facteurs susceptibles de causer un préjudice. L'identification des « risques » permet d'atténuer ou de prévenir les préjudices.

# I. INTRODUCTION

Le monde numérique est très prometteur pour l’Afrique et en particulier pour nos enfants, mais il présente aussi des risques à côté de ses multiples opportunités. Les enfants, définis comme toutes les personnes âgées de moins de 18 ans, ont des droits reconnus dans la Convention des Nations Unies relative aux droits de l’enfant<sup>2</sup> - ratifiée par chaque pays du continent africain - qui doivent être protégés, en ligne<sup>3</sup> et hors ligne de la même manière. Alors que de plus en plus d’enfants se connectent sur Internet en Afrique - une évolution soutenue par la campagne mondiale d’accès à la large bande pour tous et activée par les mesures de confinement et de couvre-feu en temps de Covid-19 - il importe de veiller à ce que l’environnement numérique soit un espace où les enfants puissent s’épanouir.

C’est dans ce contexte que la Commission de l’Union africaine (UA) pilote l’élaboration d’une Politique de l’UA sur la sécurité et l’autonomisation en ligne des enfants (la Politique). La Politique offrira un cadre solide pour la mise en œuvre des droits existants des enfants dans l’environnement numérique, notamment par le secteur privé et d’autres parties prenantes fabriquant des produits ou offrant des services auxquels les enfants pourraient avoir accès. Elle permettra aux États membres de maximiser les avantages tirés de l’utilisation des technologies de l’information et de la communication (TIC) par les enfants tout en minimisant les risques, en accordant toujours la priorité à l’intérêt supérieur de l’enfant.

La Politique de l’UA sur la sécurité et l’autonomisation en ligne des enfants vise à identifier les insuffisances et les domaines dans lesquels une harmonisation est nécessaire en vue de mettre en œuvre les droits de l’enfant et relever les défis transfrontaliers. Elle offrira aux autorités de régulation et aux décideurs nationaux un cadre garantissant que les fournisseurs de TIC respectent les droits de l’enfant ; elle dotera les enfants, les parents/tuteurs, les éducateurs, les agences/organisations de services sociaux, l’industrie et les responsables de l’application de la loi en Afrique des outils et des compétences nécessaires pour assurer la sécurité des enfants dans l’environnement en ligne ; et elle jette les bases d’une recherche et d’une collecte permanentes de données afin de garantir la contextualisation de la mise en œuvre dans le contexte africain. La présente Politique prévoit :

1. Un ensemble commun de principes, d’objectifs et de critères d’évaluation pour la COS, basé sur les meilleures pratiques internationales ;
2. Un cadre multipartite<sup>4</sup> pour décideurs nationaux afin de mettre en œuvre les politiques de COS ;
3. Un ensemble de mesures prioritaires à mettre en œuvre au niveau de l’UA.

La Politique devrait être comprise et mise en œuvre conjointement avec d’autres stratégies et législations connexes de l’UA, à savoir la Charte africaine des droits et du bien-être de l’enfant<sup>5</sup> et la Convention de l’Union africaine sur la cybersécurité et les données à caractère personnel.<sup>6</sup>

---

<sup>2</sup> Commission des droits de l’homme des Nations Unies, Convention relative aux droits de l’enfant, 7 mars 1990 : <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>

<sup>3</sup> La manière dont la Convention s’applique à l’environnement numérique est exposée dans l’Observation générale n° 25 (2021) de la CDE-NU : [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en)

<sup>4</sup> Conformément à l’UNSDG 2020, Common Minimum Standards for Multi-stakeholder Engagement (normes minimales communes pour l’engagement multipartite) : <https://unsdg.un.org/sites/default/files/2020-05/UNSDG-Common-Minimum-Standards-for-Multi-Stakeholder.pdf>

<sup>5</sup> <https://au.int/en/treaties/african-charter-rights-and-welfare-child>

<sup>6</sup> <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

## II. CONTEXTE

### II.I Accès au monde numérique pour les enfants d’Afrique

L’accès au monde numérique en Afrique se développe, et beaucoup de ceux qui se connectent à l’Internet sont des enfants. On estime qu’un internaute sur trois dans le monde est un enfant,<sup>7</sup> et que plus de 175 000 enfants se connectent pour la première fois chaque jour, soit un nouvel enfant chaque demi-seconde. En Afrique, on estime que 40 % des jeunes âgés de 15 à 24 ans peuvent accéder à l’internet.

Les enfants figurent parmi les explorateurs les plus enthousiastes de la technologie. Une étude réalisée en Afrique du Sud<sup>8</sup> en 2016 auprès d’enfants âgés de 9 à 17 ans et de leurs parents révèle que :

- 70,4 % des enfants interrogés utilisent l’internet, contre 65,8 % des parents interrogés ;
- 46,0 % de ceux qui l’ont utilisé ont pu accéder à l’internet quand ils le souhaitaient.

Pendant que l’expansion du monde numérique se poursuit, la nécessité pour l’Afrique de prendre en compte la sécurité des enfants dès la conception et par défaut devient de plus en plus urgente.

### II.II L’opportunité

L’accessibilité numérique offre aux enfants d’énormes opportunités et divers résultats en termes d’épanouissement, en fonction de l’utilisation qui en est faite. L’accès à l’internet peut aider les enfants à rester connectés, à améliorer leur culture numérique, à renforcer leur émancipation éducative et à diversifier leurs moyens de subsistance. Grâce à la numérisation croissante, les enfants peuvent désormais accéder à des outils de formation en ligne, se connecter avec leurs pairs et utiliser l’énorme potentiel que leur offre l’internet. L’environnement numérique peut contribuer positivement à la réalisation des droits de l’enfant, notamment le droit d’être entendu, de s’exprimer, de s’associer avec d’autres, de jouir de sa vie privée, de rechercher des informations et de jouer, comme le prévoit la Convention des Nations Unies relative aux droits de l’enfant. L’étude sud-africaine de 2016 révèle que la socialisation, en particulier à travers la messagerie instantanée, l’apprentissage et le travail scolaire sont des activités populaires chez les utilisateurs d’internet, 95,6 % d’entre eux déclarant qu’ils s’amuse parfois ou toujours lorsqu’ils se connectent à Internet.

L’utilisation de la technologie numérique est un facteur essentiel du changement qui facilite la réalisation de la Stratégie de transformation numérique de l’Union africaine,<sup>9</sup> les aspirations de l’Agenda 2063 de l’UA,<sup>10</sup> l’Agenda 2040 pour les enfants d’Afrique : Favoriser une Afrique digne pour les enfants ;<sup>11</sup> elle accompagne en partie la réalisation des Objectifs de développement durable (ODD).<sup>12</sup> Il est essentiel

---

<sup>7</sup> UNICEF, La situation des enfants dans le monde 2017: <https://www.unicef.org/reports/state-worlds-children-2017>

<sup>8</sup> Enfants du monde en ligne, Enfants sud-africains en ligne : Un aperçu de l'utilisation de l'internet et des activités en ligne des enfants (2016) : <http://globalkidsonline.net/southafrica/>

<sup>9</sup> <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>

<sup>10</sup> <https://au.int/en/agenda2063/goals>

<sup>11</sup> Comité africain d’experts sur les droits et le bien-être de l’enfant (CAEDBE), novembre 2016 : [https://au.int/sites/default/files/newsevents/agendas/africas\\_agenda\\_for\\_children-english.pdf](https://au.int/sites/default/files/newsevents/agendas/africas_agenda_for_children-english.pdf)

<sup>12</sup> <https://sdgs.un.org/goals>

d'améliorer l'accès des enfants à des données et à des dispositifs abordables pour la concrétisation de l'opportunité promise.

## II.III Les risques

L'accès des enfants au monde numérique s'accompagne d'une augmentation des risques qu'il leur fait courir. La pandémie de la Covid-19 a de plus en plus attiré les enfants africains vers le monde en ligne, certains accédant à l'internet pour la première fois. Les risques en ligne peuvent être présents 24 heures sur 24, 7 jours sur 7, à travers des dispositifs permettant d'accéder à l'internet. La situation peut s'aggraver pour les enfants présentant des besoins spéciaux et des handicaps.

La communauté internationale des droits de l'enfant classe les risques en ligne pour les enfants en quatre catégories : contenu, contact, comportement et risques liés à la consommation ou aux contrats, comme le montre la figure 1 ci-dessous :

<b>BASE</b>	<b>Contenu</b> L'enfant entre en contact avec un contenu potentiellement nuisible ou y est exposé	<b>Contact</b> L'enfant rencontre ou est ciblé par un contact <i>adulte</i> potentiellement nuisible	<b>Comportement</b> L'enfant est témoin, participe ou est victime d'un comportement potentiellement nuisible d'un <i>pair</i>	<b>Contrat</b> L'enfant est partie ou est exploité par un contrat potentiellement nuisible
<b>Agressive</b>	Information et communication violente, horrible, graphique, raciste, haineuse ou extrémiste	Harcèlement, filature, comportement haineuse, surveillance non désirée ou excessive	Intimidation, communication haineuse ou hostile ou activité d'un pair, exp. trolling, exclusion, humiliation	Vol d'identité, fraude, hameçonnage, arnaques, piratage, chantage, risques sécuritaires
<b>Sexuelle</b>	Pornographie (nuisible ou illégale), sexualisation de la culture, normes de l'image corporelle abusive	Harcèlement sexuel, sollicitation à caractère sexuel, sextorsion, génération et partage de matériels d'abus sexuels sur enfants	Harcèlement sexuel, messagerie à caractère sexuel non consensuel, pressions sexuelles délétères	Trafic à des fins d'exploitation sexuelle, diffusion/réception en flux (payée) d'abus sexuels sur enfants
<b>Valeurs</b>	Désinformation, marketing non adapté à l'âge ou contenu généré par l'utilisateur	Croyance ou manipulation idéologique, radicalisation et recrutement extrémiste	Communautés d'utilisateurs peut-être nuisibles, exp. automutilation, antivaccin, pressions négatives des pairs	Jeu de hasard, bulles de filtre, microciblage, persuasion ou achat de tracé de forme dans l'obscurité
<b>Transversale</b>	<b>Violations de la vie privée</b> (interpersonnelles, institutionnelles, commerciales) <b>Risques pour la santé physique et mentale</b> (Mode de vie sédentaire, usage abusif de l'écran, isolement, anxiété) <b>Inégalités et discrimination</b> (in/exclusion, exploitation de la vulnérabilité, préjugé algorithmique/analyses prédictives)			

Figure 1 : Les 4C, de Children Online : Recherche et preuves 2021<sup>13</sup>

L'étude de 2016 de l'Afrique du Sud montre que :

- Un enfant sur trois participant à l'étude a été exposé à des discours de haine (34,5 %) et à des images horribles (32,7 %) en ligne.

<sup>13</sup> <https://doi.org/10.21241/ssoar.71817>

- Plus d'un enfant sur cinq (21,9 %) de tous ceux qui utilisent l'internet, a déclaré avoir été traité de manière blessante ou méchante durant l'année écoulée (soit physiquement soit en ligne).
- Quelque 41,2 % ont déclaré avoir eu au moins une fois dans leur vie un contact en ligne avec une personne qu'ils n'avaient jamais rencontrée en personne auparavant.
- Près de 54,0 % des personnes ayant rencontré quelqu'un en ligne pour la première fois indiquent avoir été plus loin pour rencontrer physiquement la personne en question.
- À la question de savoir s'ils avaient vu des images à caractère sexuel en ligne au cours de l'année écoulée, 51,2 % des enfants interrogés ont répondu par l'affirmative et un sur trois a reçu un message à caractère sexuel (30,5 %). Un enfant sur cinq (20,5 %) participant à l'étude a reçu un message qu'il ne souhaitait pas, message contenant des publicités ou des liens vers des sites web classés X, 19,2 % avaient ouvert un message ou un lien dans un message montrant des images de personnes nues ou ayant des rapports sexuels qu'ils ne souhaitaient pas et 20,3 % avaient vu ou reçu un message, une image ou une vidéo à caractère sexuel qu'ils ne souhaitaient pas, concernant quelqu'un d'autre.

Les résultats d'une étude similaire réalisée au Ghana en 2017 rappellent ceux de l'étude sud-africaine.<sup>14</sup> D'autres études menées au Kenya mettent également en évidence les risques de santé mentale<sup>15</sup> et d'exploitation sexuelle<sup>16</sup> qui augmentent rapidement pour les enfants.

## II.IV Facteurs influençant la sécurité en ligne des enfants

De nombreux facteurs se combinent pour influencer la sécurité en ligne des enfants.

1. **Le caractère mondial de l'environnement numérique** s'accompagne de défis communs et d'opportunités d'action. Le secteur de la technologie opère simultanément dans plusieurs systèmes juridiques différents. L'élaboration d'approches internationales communes de la réglementation du secteur privé et d'une communauté transfrontalière de meilleures pratiques en matière d'éducation, d'application de la loi et d'aide aux victimes, entre autres, peut constituer une réponse efficace.
2. **La conception des produits et services TIC** est fondamentale, étant donné que les intérêts commerciaux, s'ils ne sont pas adaptés aux droits de l'enfant, peuvent créer ou renforcer les risques pour la sécurité des enfants. De par la conception, les stratégies de sécurité soutenues par la loi, se sont révélées être un facteur

<sup>14</sup> [Risques et opportunités liés aux pratiques en ligne des enfants, rapport-pays du Ghana 2017. Cette étude](https://www.unicef.org/ghana/media/1791/file/Risks_and_Opportunities_-_Child_Online_Protection.pdf) a porté sur 3 000 enfants âgés de 9 à 17 ans et 1 000 tuteurs/parents. [https://www.unicef.org/ghana/media/1791/file/Risks and Opportunities - Child Online Protection.pdf](https://www.unicef.org/ghana/media/1791/file/Risks_and_Opportunities_-_Child_Online_Protection.pdf)

<sup>15</sup> Kenya Paediatric, Adolescents in the Digital Age : <https://www.kenyapaediatric.org/wp-content/uploads/2018/05/Adolescents-in-the-digital-age-Dr.-Claire-Majisu.pdf>;

<sup>16</sup> Terre des Hommes, La face cachée de l'Internet pour les enfants. Exploitation sexuelle des enfants en ligne au Kenya - Rapport d'évaluation rapide (2018) : <https://www.datocms-assets.com/22233/1600704755-tdh-nl-ocse-in-kenya-research-report-feb-2018.pdf>

décisif de la sécurité des produits du secteur de la technologie, surtout en ce qui concerne les enfants.

3. **Le bien-être général des enfants** influe sur la manière dont ils entrent en contact avec l'internet. Il est prouvé que les enfants qui sont vulnérables hors ligne sont également plus susceptibles d'être vulnérables en ligne, de sorte que les facteurs de protection hors ligne peuvent également réduire l'exposition aux risques en ligne. Les facteurs hors ligne qui créent une vulnérabilité ou une protection influencent la manière dont les enfants entrent en contact avec l'environnement en ligne. Dès lors, les mesures locales hors ligne sont également nécessaires dans le cadre d'une stratégie globale.
4. De même, les **connaissances et le soutien des parents/tuteurs, des éducateurs et des pairs** peuvent aider les enfants à devenir des utilisateurs d'internet plus confiants.<sup>17</sup> Certaines études exploratoires laissent supposer que le soutien social et les relations positives des enfants avec les personnes qui les entourent peuvent agir comme des facteurs de protection, en soutenant que la protection des enfants en ligne est plus efficace lorsqu'elle est combinée à un soutien parental hors ligne.

## II.V Cadres et outils existants pour la protection en ligne des enfants en Afrique

Il existe des initiatives, des cadres et des outils nationaux, régionaux et continentaux relatifs à la sécurité en ligne des enfants en Afrique. Toutefois, ils sont largement axés sur les abus les plus odieux, notamment l'exploitation et les abus sexuels sur enfants, et surtout sur les droits des victimes. Le contexte plus large et en particulier le rôle des sociétés et la conception des systèmes constituent une brèche importante.

### 1. Niveau national

Environ 52 %<sup>18</sup> des pays africains disposent d'une forme de législation sur la protection des données et de la vie privée (y compris une protection limitée dans d'autres lois), mais la majorité de ces législations sont soit limitées dans leur champ d'application et leur applicabilité à l'environnement en ligne des enfants, soit ne sont pas encore totalement mises en œuvre. ***La réglementation sur la protection des données axée sur les enfants présente un fort potentiel pour répondre à de nombreux risques auxquels sont confrontés les enfants en ligne.***<sup>19</sup>

De nombreux pays traitent de manière générale la question de l'exploitation sexuelle ou interdisent la pornographie en général. Toutefois, ces lois ne suffisent pas puisqu'elles ne traitent pas spécifiquement des aspects criminels des différentes formes d'exploitation et d'abus sexuels en ligne sur enfants. En

---

<sup>17</sup> Voir l'[Étude sud-africaine](#) pour des statistiques sur les impressions des parents concernant les expériences des enfants sur l'internet, et sur la probabilité que les enfants communiquent avec leurs parents sur des questions liées à l'internet.

<sup>18</sup> Législation mondiale de la CNUCED en matière de protection des données et de la vie privée : <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

<sup>19</sup> L'impact positif de règles solides en matière de protection des données est mis en évidence par les changements apportés par les sociétés de technologie pour se conformer au code britannique de conception adaptée à l'âge, entré en vigueur en 2021 : « **Children are better protected online in 2022 than they were in 2021** » - [ICO marks anniversary of Children's code \(Les enfants sont mieux protégés en ligne en 2022 qu'ils ne l'étaient en 2021\)](#) - L'ICO marque l'anniversaire du Code de l'enfance) Bureau du Commissaire à l'information, 2 septembre 2022

outre, l'absence de définitions, d'approches et de mesures législatives harmonisées entre les États membres constitue un défi considérable pour garantir l'identification des infractions et la localisation des criminels - notamment en dehors des frontières nationales - et ensuite leur traduction en justice.

Il existe déjà plusieurs exemples d'initiatives de sécurité en ligne en faveur des enfants en Afrique dont on peut s'inspirer. Certains pays ont mis en place des initiatives documentées en matière de sécurité, tels que le Kenya,<sup>20</sup> le Ghana,<sup>21</sup> l'Ouganda<sup>22</sup> et la Zambie.<sup>23</sup> Des organisations d'experts existent dans toute l'Afrique pour encadrer la réflexion sur la sécurité en ligne, notamment le Centre africain des droits numériques<sup>24</sup> CIPESA<sup>25</sup> et Research ICT Africa<sup>26</sup>. Enfin, il existe en Afrique des exemples de législation pour orienter la prise de décisions : La loi ghanéenne sur la cybersécurité<sup>27</sup> criminalise les comportements à caractère sexuel en ligne avec des enfants et impose des obligations aux services de télécommunications. Le Rwanda dispose d'une politique bien conçue en matière de protection en ligne des enfants,<sup>28</sup> ainsi que d'un plan d'action quinquennal approfondi.

## 2. Niveau régional

Au niveau régional, plusieurs politiques et cadres juridiques de protection des enfants sont en place, entre autres : La politique de l'enfance de la CAE<sup>29</sup> et le cadre pour le renforcement des systèmes de protection des enfants au sein de la Communauté de l'Afrique de l'Est<sup>30</sup>, la loi type de la SADC sur l'éradication du mariage des enfants<sup>31</sup> et, en 2019, la CEDEAO a adopté une politique de l'enfance et son plan d'action stratégique (2019-2023). Une fois de plus, l'absence de cadres régionaux harmonisés constitue un obstacle majeur à une approche cohérente de la sécurité en ligne des enfants sur le continent et, au bout du compte, dans le monde entier.

Une fois de plus, ces lois traduisent des préoccupations antérieures à la question de sécurité numérique et ne vont pas dans le sens d'une approche plus intégrée et systémique de la sécurité en ligne des enfants.

## 3. Niveau continental

Au niveau continental, la Charte africaine des droits et du bien-être de l'enfant a été adoptée en 1990 et est entrée en vigueur en 1999. Il a été institué un Comité africain d'experts sur les droits et le bien-être de l'enfant (CAEDBE). Parmi les fonctions du Comité figurent la promotion et la protection des droits consacrés par la Charte. En 2019, le Comité a adopté une déclaration sur la prévention et l'élimination de l'exploitation sexuelle en ligne des enfants en Afrique.<sup>32</sup>

---

<sup>20</sup> UIT, Statut de l'initiative pour la sécurité en ligne des enfants au Kenya : [https://www.itu.int/en/ITU-D/Documents/ChildOnlineSafety/Initiative\\_Kenya.pdf](https://www.itu.int/en/ITU-D/Documents/ChildOnlineSafety/Initiative_Kenya.pdf)

<sup>21</sup> Ghana, Be cyber smart - Tips to keep children safe online (7-10 years) : <https://home.kpmg/gh/en/home/insights/2020/04/Be-cyber-smart-tips-to-keep-children-safe-online-7-10-years.html>

<sup>22</sup> [www.stopit.ug](http://www.stopit.ug)

<sup>23</sup> [www.stopit.ac.zm](http://www.stopit.ac.zm).

<sup>24</sup> <https://africadigitalrightshub.org>

<sup>25</sup> <https://cipesa.org>

<sup>26</sup> <https://researchictafrica.net>

<sup>27</sup> Loi ghanéenne sur la cybersécurité - Loi 1038, 2020

<sup>28</sup> [Politique de protection en ligne des enfants du Rwanda](#), 2019

<sup>29</sup> Politique de l'enfance de la CAE, 2016 : <http://repository.eac.int/bitstream/handle/11671/2013/EAC-Child-Policy.pdf?sequence=1&isAllowed=y>

<sup>30</sup> Cadre de la CAE pour le renforcement des systèmes de protection de l'enfance, 2017 : <file:///C:/Users/suliemana/Downloads/EAC-Framework-Child-Protection-2018.pdf>

<sup>31</sup> Loi type de la SADC sur l'éradication du mariage des enfants, 2016 : <https://www.childrenandaids.org/node/1139>

<sup>32</sup> <https://acerwc.africa/sites/default/files/2022-07/ACERWC-33nd-Session-Draft-Report-English-Final-1.pdf>

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo),<sup>33</sup> intègre dans ses articles des infractions liées au contenu de la pornographie infantile. Ainsi, il sera nécessaire d'introduire un amendement à la Convention pour soutenir la pleine réalisation des droits de l'enfant dans l'environnement numérique et protéger les enfants contre toutes les formes de violence et de préjudice en ligne.

Il existe également des guides pour assurer la sécurité en ligne des enfants, tels que ceux de Child Online Africa.<sup>34</sup>

### III. PRINCIPES DIRECTEURS

Lors de l'élaboration de politiques nationales en matière de protection en ligne des enfants, les décideurs politiques devraient garder à l'esprit certains principes directeurs afin d'orienter l'élaboration de ces politiques. Ces principes qui sous-tendent également cette politique continentale, se répartissent en deux catégories : l'application des droits reconnus de l'enfant et la prise en compte des questions transversales.

#### 1. Appliquer les droits reconnus de l'enfant

L'observation générale n° 25 (2021) du CDE-NU sur les droits de l'enfant en relation avec l'environnement numérique et l'observation générale n° 7 sur l'article 27 du Comité africain d'experts sur les droits et le bien-être de l'enfant (CAEDBE) partagent quatre principes directeurs :

- a) **Intérêt supérieur de l'enfant** : Les États membres sont encouragés à veiller à ce que, dans toutes les actions concernant la fourniture, la réglementation, la conception, la gestion et l'utilisation de l'environnement numérique, l'intérêt supérieur de chaque enfant constitue un facteur primordial. En considération de l'intérêt supérieur de l'enfant, tous les droits des enfants doivent être pris en compte, notamment leur droit de rechercher, de recevoir et de transmettre des informations, d'être protégés contre les préjudices et de voir leur opinion dûment prise en considération, et garantir la transparence de l'évaluation de l'intérêt supérieur de l'enfant et des critères qui ont été appliqués.
- b) **Non-discrimination** : Les États membres sont invités à prendre des mesures proactives pour prévenir la discrimination fondée sur la race, la couleur, l'origine nationale, la citoyenneté, l'appartenance ethnique, la profession, les opinions politiques et toutes autres opinions, ainsi que sur la santé, notamment le statut VIH, le handicap, l'âge, la religion, la culture, la situation matrimoniale, la situation socioéconomique, le statut de réfugié, de migrant ou tout autre statut, le sexe, le genre ou tout autre facteur susceptible d'entraîner une discrimination à leur encontre. Des mesures spécifiques seront nécessaires pour combler la fracture numérique liée au sexe pour les filles et veiller à ce qu'une attention particulière soit accordée à l'accès, à la culture numérique, à la vie privée et à la sécurité en ligne.

---

<sup>33</sup> Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel, 2014 :

[https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf). La Convention n'est pas encore entrée en vigueur, étant donné qu'à ce jour, 10 États membres sur les 15 requis ont ratifié la Convention de Malabo

<sup>34</sup> <https://toolkits.childonlineafrica.org>

- c) **Droit à la vie, à la survie et au développement** : Les États membres sont invités à prendre toutes les mesures appropriées pour protéger les enfants des risques qui pèsent sur leur droit à la vie, à la survie et au développement.
- d) **Participation des enfants** : Les États membres sont encouragés à promouvoir la sensibilisation et l'accès aux moyens numériques permettant aux enfants d'exprimer leur point de vue, et à proposer une formation et un soutien aux enfants pour qu'ils puissent participer sur un pied d'égalité avec les adultes, de manière anonyme si nécessaire. 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 membres sont invités à impliquer les enfants, à écouter leurs besoins et à tenir dûment compte de leurs opinions. Ils doivent veiller à ce que les processus consultatifs incluent les enfants qui n'ont pas accès à la technologie ou qui n'ont pas les compétences nécessaires pour l'utiliser.

## 2. Prendre en compte les questions transversales

En ce qui concerne les travaux de rédaction plus pratiques, les décideurs politiques doivent également évaluer les efforts déployés pour traiter des questions transversales suivantes :

- a) **Identifier les risques et atténuer les préjudices** : La première priorité en matière de protection en ligne des enfants doit être d'identifier clairement la source des préjudices subis en ligne par les enfants et de mettre en place des mécanismes efficaces pour limiter ces préjudices.
- b) **Promouvoir l'accès, l'accessibilité et l'inclusion** : Après avoir traité des préjudices, il est prudent et bénéfique pour la jouissance des droits des enfants d'élargir l'accès au monde en ligne - à un plus grand nombre d'enfants, aux enfants ayant des besoins spécifiques en matière d'accessibilité, et à tous les groupes d'enfants de manière égale.
- c) **Établir une chaîne de responsabilité et de collaboration** : Pour protéger et soutenir en permanence les enfants en ligne, il convient de confier à l'organisme approprié la responsabilité de gérer les efforts permanents des parties prenantes concernées.
- d) **Intégrer la conception centrée sur l'enfant** : Après avoir élaboré une politique visant à rendre l'environnement numérique existant plus sûr et plus favorable, les efforts peuvent porter sur l'amélioration de la réglementation de l'environnement numérique afin d'exiger que les droits et les besoins des enfants soient pris en compte dans le développement des services en ligne.
- e) **Garantir l'efficacité** : Enfin, la politique doit faire l'objet d'une évaluation permanente afin de s'assurer qu'elle fonctionne comme prévu et qu'elle répond aux préoccupations nouvelles et émergentes concernant les enfants dans le monde en ligne.

## IV. OBJECTIFS DE LA POLITIQUE

Prenant en compte les droits de l'enfant et les questions transversales, la Politique de l'Union africaine sur la sécurité et l'autonomisation en ligne des enfants fixe les objectifs suivants dans dix domaines d'action :

1. **Capacité institutionnelle** : Identifier et mobiliser les acteurs institutionnels (aux niveaux continental, régional et national) afin de diriger et de participer à un Comité de pilotage sur la sécurité en ligne des enfants ainsi qu'à un Groupe d'experts des parties prenantes pour couvrir tous les domaines de la politique de sécurité en ligne des enfants. Apporter les moyens, la capacité institutionnelle et l'encadrement adéquats pour garantir une action et une coopération efficaces.
2. **Cadres juridiques et réglementaires** : Renforcer et harmoniser de nouveau les systèmes juridiques et réglementaires continentaux, régionaux et nationaux relatifs à la sécurité en ligne des enfants, et renforcer les capacités des organismes d'application de la loi et des organes de réglementation dans le domaine de la sécurité en ligne des enfants, notamment leur capacité à collaborer avec d'autres secteurs, en particulier le secteur des TIC.
3. **Données à caractère personnel et identité** : Reconnaître les avantages de la vie privée, l'identité et la capacité d'agir des enfants et répondre aux menaces actuelles et émergentes inhérentes à l'utilisation des données dans le monde numérique, y compris les données personnelles, la biométrie et la prise de décision automatisée.
4. **Systèmes de réponse et de soutien** : Établir un cadre multilatéral coordonné pour lutter contre les risques auxquels sont exposés les enfants en ligne, en particulier l'exploitation et l'abus sur enfants (CSEA) : y compris des mécanismes juridiques et réglementaires efficaces d'application de la loi, la prévention, les recours et l'accès à des conseils d'experts sur la sécurité en ligne des enfants.
5. **Entreprises et droits de l'enfant** : Promouvoir une conception centrée sur l'enfant, des normes minimales, des accords sectoriels, l'adoption de meilleures pratiques, la sensibilisation culturelle et le financement de la sécurité en ligne des enfants à travers une réglementation et des cadres liés à la responsabilité d'entreprise.
6. **Formation** : Veiller à ce que toutes les personnes impliquées dans les services liés aux enfants, notamment le gouvernement, les forces de l'ordre, la justice, le monde de la santé et du bien-être, les hommes politiques et les fonctionnaires, ainsi que les concepteurs de technologies, comprennent bien la sécurité en ligne des enfants et l'intérêt supérieur de l'enfant.
7. **Éducation** : Promouvoir l'utilisation positive de la technologie numérique comme source de divertissement, d'information et d'apprentissage pour les enfants dans un environnement sûr.

8. **Sensibilisation du public et communication** : Sensibiliser tous les secteurs de la communauté aux questions de sécurité en ligne des enfants, afin de prévenir les risques et de promouvoir une utilisation positive de l'internet.
9. **Recherche et développement** : Garantir une approche intégrée, fondée sur des données probantes et actualisée de la sécurité en ligne des enfants.
10. **Coopération internationale** : Assurer une collaboration solide entre les partenaires, au niveau continental, ainsi qu'avec d'autres organisations et acteurs externes nationaux, régionaux et mondiaux, afin de partager les meilleures pratiques.

## V. PLAN DE MISE EN ŒUVRE

Le plan de mise en œuvre suivant définit des mesures pratiques pour progresser vers les objectifs susmentionnés. Il comprend des actions à mettre en œuvre au niveau de l'Union africaine, ainsi qu'un cadre permettant aux décideurs régionaux et nationaux de concevoir et de mettre en œuvre des mécanismes coordonnés et efficaces adaptés à leur contexte spécifique.<sup>35</sup> Le plan de mise en œuvre doit être considéré comme un complément aux efforts visant à améliorer l'accès aux données et aux dispositifs pour les enfants et ceux qui soutiennent la sécurité et l'autonomisation en ligne des enfants.

La réalisation du plan de mise en œuvre sera coordonnée par un Comité de pilotage de l'Union africaine sur la sécurité en ligne des enfants, nouvellement créé, qui sera également chargé d'évaluer et de mettre régulièrement à jour le plan, afin de l'adapter aux enseignements tirés dans le contexte de sa mise en œuvre et de l'évolution des meilleures pratiques internationales.

Pour chacun des domaines d'action, la Commission de l'Union africaine identifiera les insuffisances et élaborera des recommandations qui seront intégrées dans le plan de mise en œuvre de cette politique ou soumises à la Commission africaine pour suite à donner ; elle développera, partagera et tiendra à jour une base de données des meilleures pratiques et des moyens. Pour l'élaboration d'outils et de ressources, on veillera à prendre en considération les ressources existantes dans les environnements nationaux, internationaux ou multilatéraux qui peuvent être recentrées sur le contexte africain.

Afin d'assurer une mise en œuvre efficace et harmonieuse des actions clés contenues dans le plan de mise en œuvre, la Commission de l'Union africaine collaborera / coordonnera avec les institutions / organisations / partenaires africains et régionaux compétents pour mettre en œuvre les différents aspects du plan d'action.

Objet tif #	Gouvernance	
1	Affirmer l'engagement public au plus haut niveau en faveur de la sécurité en ligne des enfants	Déclaration ministérielle et événement de haut niveau pour le lancement de la politique de l'UA sur la sécurité et l'autonomisation en ligne des enfants [2023]

<sup>35</sup> Des outils pour l'élaboration de politiques régionales ou nationales plus détaillées et mieux adaptées sont disponibles dans le Guide sur la sécurité en ligne des enfants : <https://childonlinesafetytoolkit.org>

1	Créer un Comité de pilotage / surveillance de l'Union africaine sur la sécurité et l'autonomisation en ligne des enfants	Le Comité de pilotage / surveillance de l'Union africaine sur la sécurité et l'autonomisation en ligne des enfants sera chargé de coordonner la mise en œuvre et l'évaluation de la politique de l'Union africaine sur la sécurité et l'autonomisation en ligne des enfants, et servira de point focal pour la coopération régionale et internationale. Le Comité de pilotage / surveillance réunira les points focaux régionaux et nationaux désignés pour la COS ainsi que les représentants des autorités de l'UA responsables des domaines politiques suivants : éducation, santé, justice, protection des consommateurs, TIC, protection des données, cyber-sécurité, application de la loi, services à la famille et à l'enfance. Il comprendra une sélection d'experts africains et internationaux qui, entre eux, couvrent les dix domaines politiques, ainsi que les droits de l'enfant et les questions transversales. Il se réunira au moins une fois par trimestre. Le Secrétariat de l'UA assurera le secrétariat du Comité de pilotage.
1, 9	Créer le Groupe ou les groupes des partenaires de l'Union africaine sur la sécurité et l'autonomisation en ligne des enfants	Le Groupe des partenaires sur la sécurité et l'autonomisation en ligne des enfants apportera au Comité de pilotage son expertise et son soutien à la mise en œuvre. Il sera composé de professionnels et d'experts, notamment des professionnels de l'application de la loi, des entreprises, du secteur tertiaire, des organisations de défense des droits de l'enfant, des établissements d'enseignement, des parents/tuteurs et du monde universitaire. Il comprendra un groupe central de parties prenantes ainsi que des partenaires invités à participer pour un domaine politique donné. Sa fonction consultative peut être complétée par des appels à contribution ouverts. La participation des enfants doit être assurée dans toutes les activités. Ce Groupe est censé constituer une ressource d'experts pour le Comité de pilotage, et non un second groupe de pilotage dotés de pouvoir de décision.
1	Déterminer les indicateurs de performance et d'évaluation	La première réunion en présentiel du Comité de pilotage de l'Union africaine sur la sécurité et l'autonomisation en ligne des enfants adoptera la marche à suivre pour la mise en œuvre du présent Plan (y compris l'établissement de priorités et le financement des activités), les indicateurs clés de performance, les mécanismes d'évaluation, les modèles d'établissement de rapports ainsi que les mécanismes de révision pour le présent Plan et la Politique dans son ensemble. Le Comité de pilotage désignera une instance responsable (personne, institution, organe) pour chaque action du présent Plan et allouera les ressources humaines et financières nécessaires pour mener à bien la tâche envisagée.
Objet tif #	<b>Cadres juridiques</b>	
2, 3, 4, 5	Élaborer un cadre juridique harmonisé pour la protection de la vie privée et la sécurité en ligne des enfants par essence et par défaut, ainsi que des mécanismes d'application de la loi	La Commission de l'Union africaine identifie les insuffisances du système juridique et réglementaire actuel pour les enfants africains par rapport aux meilleures pratiques internationales et élabore un cadre juridique harmonisé pour la protection de la vie privée et de la sécurité en ligne des enfants, fondé sur les droits de l'enfant et la Charte africaine des droits et du bien-être de l'enfant. Ce cadre juridique définira (1) des protections solides pour les données des enfants, et (2) un système de sécurité par essence basé sur les résultats. Il couvrira tous les produits et services numériques auxquels les enfants peuvent avoir accès et garantira un niveau élevé de protection des données des enfants par essence et par défaut grâce à une conception adaptée à l'âge, notamment en exigeant des entreprises qu'elles mettent en œuvre la vérification de l'âge (si nécessaire), qu'elles procèdent à des évaluations des risques couvrant les 4 C, qu'elles adhèrent aux normes internationales et aux codes de pratique les plus élevés qui existent et qu'elles fassent preuve de transparence, notamment en assurant aux chercheurs l'accès aux données. L'application de la loi doit être assurée par une ou plusieurs instances de contrôle indépendantes, dotées de moyens suffisants pour exécuter la tâche requise.

2, 4	Renforcer les cadres de la justice pénale afin de lutter efficacement contre les infractions liées à la sécurité en ligne des enfants, notamment la CSEA	La Commission de l'Union africaine s'efforce de fournir des orientations sur la manière dont les lois et procédures pénales relatives à la sécurité en ligne des enfants (à savoir les enquêtes, les poursuites et les condamnations pour des délits en ligne qui violent les droits de l'enfant ou nuisent à leur développement physique, mental ou moral) peuvent être harmonisées et renforcées en conformité avec les normes et les meilleures pratiques internationales. Les lois pénales relatives à la sécurité en ligne des enfants devraient être élaborées eu égard à tous les droits des enfants, tels que leur droit d'être entendus et de participer, et devraient garantir la protection des enfants qui, eux-mêmes, entrent en conflit avec la loi. Les systèmes de justice pénale devraient garantir un accès rapide à la justice, notamment grâce à des mécanismes efficaces de soutien et d'information en faveur des victimes, et à des ressources suffisantes pour les services d'enquête et d'intervention.
2, 4, 5, 7	Élaborer et mettre en œuvre une classification harmonisée des classes d'âge	L'Union africaine encourage l'élaboration et l'adoption d'une classification harmonisée par âge pour les contenus commerciaux, les médias de service public ainsi que les jeux et activités en ligne, qui reflète l'évolution des capacités des enfants.
2, 10	Envisager la participation à des cadres juridiques internationaux pour la sécurité en ligne des enfants	La Commission de l'Union africaine identifie les insuffisances dans la contribution régionale et internationale aux instruments existants qui promeuvent la sécurité en ligne des enfants, et présente des recommandations à tous les États membres.
Objectif #	<b>Renforcement de capacités, formation et mutualisation des ressources</b>	
2, 3, 4, 5, 6, 10	Renforcer la capacité des autorités de régulation à superviser et à faire respecter les cadres juridiques relatifs à la protection de la vie privée et à la sécurité en ligne des enfants	La Commission de l'Union africaine encourage l'échange de meilleures pratiques, formule des recommandations pour le renforcement des capacités, développe et met en place un module de formation destiné aux autorités de régulation des TIC : (3) Les droits de l'enfant dans l'environnement numérique (en s'inspirant de l'observation générale n° 25 de la Convention des Nations Unies relative aux droits de l'enfant et des outils développés par l'UIT, par exemple) (4) Confidentialité des données (5) Sécurité par conception (couvrant les normes, processus et outils existants qui soutiennent la mise en œuvre et l'application de la loi) (6) Protections et normes d'acquisition pour les technologies de l'éducation et les technologies utilisées dans les écoles (7) Encadrement de l'IA (basé sur le modèle en quatre étapes des droits de l'enfant suivant l'encadrement de l'IA)
2, 4, 6, 10	Renforcer la capacité des agences d'application de la loi et de la justice pénale	La Commission de l'Union africaine encourage l'échange de meilleures pratiques, formule des recommandations pour le renforcement des capacités, développe des matériels de formation et met en œuvre des programmes ciblés de formation des formateurs pour l'application de la loi et autres spécialistes de la justice pénale pour la sécurité en ligne des enfants couvrant : (1) Les mécanismes de confidentialité et de protection des données (2) La protection des enfants et la prévention des infractions (3) La reconnaissance et l'instruction des comportements délictueux (4) Les poursuites et les condamnations (5) La gestion des criminels (6) Le soutien aux victimes

4, 6, 7, 10	Renforcer la capacité des professionnels travaillant directement avec les enfants	La Commission de l'Union africaine encourage l'échange de meilleures pratiques, formule des recommandations pour le renforcement des capacités, met au point le matériel de formation (et des cours pour les programmes d'études pertinents) et met en place des programmes ciblés de formation des formateurs pour les professionnels et les bénévoles qui travaillent avec les enfants dans les domaines tels que l'éducation, la santé et les services sociaux, couvrant : (1) L'établissement de lien entre la sécurité en ligne des enfants et leur rôle particulier (2) La manière d'élaborer et de mettre en œuvre une politique de sécurité en ligne pour les enfants dans un contexte donné (3) La nature du soutien aux enfants vulnérables (4) La reconnaissance et l'interprétation des comportements délictueux (5) La manière de signaler les infractions (6) La garantie de l'accès au soutien aux victimes
2, 3, 4, 5, 6, 9, 10	Développer et entretenir des bases de données pour la mutualisation des ressources et l'échange d'informations	La Commission de l'Union africaine met en place et entretient des bases de données pour le partage d'informations, de moyens et de bonnes pratiques, y compris le repérage des violations des droits de l'enfant et des préjudices identifiés, ainsi que pour la coopération en matière d'application de la loi. Ces bases de données seront renouvelées, révisées et partagées régulièrement.
Objectif #	<b>Sensibilisation, éducation et lignes téléphoniques d'assistance</b>	
3, 4, 5, 6, 7, 8, 10	Promouvoir et soutenir l'éducation numérique accessible dans les écoles	La Commission de l'Union africaine encourage l'échange de meilleures pratiques et élabore du matériel pédagogique ainsi qu'un programme d'éducation visant à promouvoir la sécurité et l'autonomisation en ligne des enfants dans les écoles. Le programme qui devrait être modulable en fonction des circonstances locales et introduit dans le cadre du programme scolaire standard, devrait avoir pour objectif d'aider les enfants à développer des compétences numériques et de leur donner les moyens de construire des communautés respectueuses. Il devrait être intégré et couvrir la culture des données et des médias, ainsi que les questions de sauvegarde. Il doit promouvoir l'utilisation positive de la technologie numérique, de la sexualité et du consentement, et prendre en compte les besoins de tous les enfants, indépendamment de leur sexe, de leur âge, de leur revenu ou de leur origine.
4, 5, 6, 7, 8	Promouvoir et soutenir l'éducation des parents, des tuteurs et des responsables communautaires	La Commission de l'Union africaine encourage l'échange de meilleures pratiques et élabore du matériel pédagogique ainsi que des programmes d'échange et de sensibilisation à l'intention des parents, des tuteurs et des responsables communautaires qui travaillent directement avec les enfants ou qui sont chargés de leur sécurité et de leur autonomisation en ligne. Des consultations avec les familles et les enfants sont nécessaires afin d'identifier les problèmes, les solutions et les moyens de sensibiliser efficacement la communauté à la sécurité en ligne des enfants.
7, 8	Développer et entretenir un portail public convivial pour les enfants sur la sécurité en ligne	La Commission de l'Union africaine encourage la création d'un portail public accessible et adapté aux enfants pour la sécurité en ligne et l'engagement numérique, couvrant l'ensemble des questions relatives à la sécurité en ligne des enfants, telles qu'elles sont exposées dans la présente politique. Les messages et le matériel ciblés doivent être conçus en consultation avec les enfants, les jeunes et les parents/tuteurs d'enfants.
7, 8	Campagne de sensibilisation autour de la Journée africaine pour un internet plus sûr	La Commission de l'Union africaine coordonne (notamment avec l'UIT) une campagne de sensibilisation du public aux questions soulevées dans la présente politique à l'occasion de la Journée africaine pour un internet plus sûr.
2, 4, 10	Soutenir et promouvoir les lignes téléphoniques d'assistance pour la dénonciation et le soutien aux victimes	La Commission de l'Union africaine encourage l'échange de meilleures pratiques (notamment avec les Centres à guichet unique), formule des recommandations pour le renforcement des capacités et soutient la mise en place et la promotion de structures intégrées d'assistance téléphonique (en ligne et par téléphone) pour la communication et le soutien aux victimes. Ces lignes d'assistance seront dotées de toutes les ressources et les bénévoles recevront une formation adéquate. L'idée est de s'appuyer sur les connaissances et les pratiques d'assistance téléphonique

		existantes sur d'autres territoires et de conclure des accords bilatéraux de « jumelage » qui assurent un soutien initial et permanent dans différents territoires.
5, 6	Promouvoir les meilleures pratiques du secteur en matière de COS	La Commission de l'Union africaine privilégie la sensibilisation des professionnels du secteur des TIC aux droits de l'enfant et aux questions couvertes par la présente politique, ainsi qu'aux meilleures pratiques et aux outils permettant de s'y conformer. La Commission encourage la promotion et le partage des meilleures pratiques en matière de COS par les États membres africains.
Objectif #	<b>Recherche</b>	
9, 10	Créer un fonds et un programme de recherche sur la COS africain	La Commission de l'Union africaine crée un fonds central de recherche et élabore un programme de recherche afin de fournir les données et les preuves nécessaires à la mise en œuvre et à la mise à jour de la présente politique. Le programme soutiendra la recherche et la collecte de données au niveau national, régional et continental afin de soutenir le suivi et l'évaluation des mesures de sécurité en ligne des enfants. Il encouragera des normes de recherche élevées, la création de centres d'excellence nationaux, le partage des données et des ressources ainsi que la coopération entre les chercheurs, y compris au niveau international. Une analyse initiale et régulière des insuffisances permettra de s'assurer que les ressources sont affectées en priorité aux domaines où les besoins sont les plus importants et d'éviter les doubles emplois inutiles. Les ressources de ce fonds devraient également permettre aux États membres de l'Union africaine de bénéficier des programmes de recherche des États multilatéraux, régionaux et autres, notamment en soutenant l'engagement des programmes de recherche nationaux avec des pairs et des programmes à travers le monde.
9, 10	Développer et entretenir une base de données de recherche	La Commission de l'Union africaine met en place et entretient une base de données centrale pour la recherche sur la sécurité en ligne des enfants. Cette base de données regroupera toutes les recherches menées dans le cadre du programme de recherche africain sur la COS et constituera un portail permettant aux chercheurs d'accéder aux travaux universitaires internationaux pertinents dans ce domaine. Il favorisera également le partage des meilleures pratiques en termes d'innovation, de recherche responsable, de ressources et de coopération entre les chercheurs africains en matière de COS. Cette base de recherche servira également de ressource pour les chercheurs internationaux afin de garder à l'esprit la perspective africaine.