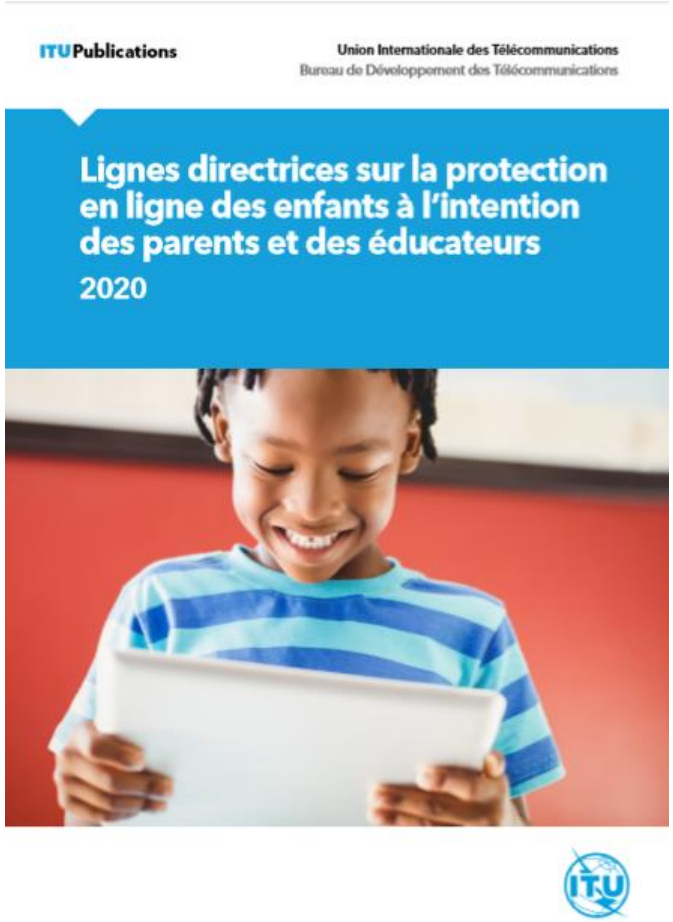


Lignes directrices en ligne des enfants à l'intention des professionnels d'Industrie

OBJECTIFS

Domaines clés pour l'industrie	• **Expliquez cinq domaines clés que les directives soulignent pour que les entreprises promeuvent COP**
Lignes directrices pour l'industrie	• Les lignes directrices en détail • Les listes de contrôle spécifiques aux fonctionnalités • Le travail avec l'industrie pour préciser les directives pour l'Afrique
Sécurité par la conception	• Les principes de la sécurité dès/par la conception ou de la sécurité par défaut • L'importance avec l'étude de cas de l'application de conférence Zoom.
La voie à suivre	• Couvrir les plans et les objectifs de la COP en Afrique d'ici à 2023 • Mettre en évidence les jalons
Récapitulation	• Le lancement officiel vendredi • Formulaire d'évaluation

RECAPUTILATION DU JOUR 1

Les Décideurs Politiques:

à partir les Directives COP, soutenir le **développement**, la **rédaction, l'adoption** et la **mise en œuvre de stratégies nationales COP** basées sur une approche multipartite /multisectorielle.

1. Élaboration d'une **Législation Nationale** adéquate
2. Le **Cadre Juridique et les Stratégies** axés liés sur la Sécurité dès la Conception, entre autres.
3. **Harmonisation des Lois au niveau international** en tant qu'étape clé pour la Protection des Enfants En Ligne.

Pour les parents:

Soutenir les enfants et les jeunes ainsi que leurs familles en les informant et en les engageant lors de la sensibilisation sur les questions liées à la COP ainsi qu'en soutenant le développement des compétences numériques et la littératie numérique

a. Les **parents discutent avec leurs enfants** et essaient de faire des activités en ligne avec eux.
b. **Identifiez la technologie, les appareils** et les services dans la famille / le ménage.
c. Déterminez si **les programmes de filtrage et de blocage ou de surveillance** peuvent aider et soutenir leurs familles.
d. **Mettez-vous d'accord** en tant que famille sur l'utilisation d'Internet et des appareils personnels.
e. Soyez **conscient des services en ligne et mobiles** utilisés par leurs enfants.

Pour les éducateurs

Dans leur rôle en veillant à ce que **les enfants et les jeunes dispensent leurs leçons conformément aux protocoles standard** qui placent la sécurité des enfants au cœur de son mandat d'enseigner les CTI/ICT avec un mélange de sensibilisation sur la COP ainsi que sur les compétences numériques et l'alphabétisation.

Les lignes directrices pour les éducateurs comprennent:

1. S'assurer que tous les appareils sont **sécurisés et protégés par mot de passe.**
2. Installation d'un **logiciel antivirus et de pare-feu**.
3. S'assurer qu'il **existe une politique** qui détaille comment la technologie peut être utilisée.
4. Examiner comment gérer **la prise et le stockage des images** des élèves.
5. S'assurer que les flux Internet fournis par l'école sont **filtrés et surveillés**.

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

Les technologies en ligne offrent aux enfants et aux jeunes de nombreuses **possibilités de communiquer**, **d'acquérir de nouvelles compétences**, de **donner libre cours** à leur **créativité** et de contribuer à **l'édification d'une société meilleure**

Mais, elles amène de **nouveaux risques**, comme l'exposition aux atteintes à la **vie privée**, à des **contenus illicites**, au **harcèlement**, à la **cyberintimidation**, à l'utilisation abusive des **données personnelles**, à la **manipulation psychologique** et même aux **abus sexuels** sur les enfants

- une **approche générale** visant à répondre à toutes les **menaces et préjudices potentiels** que les enfants et les jeunes peuvent rencontrer au cours de l'acquisition de compétences numériques.

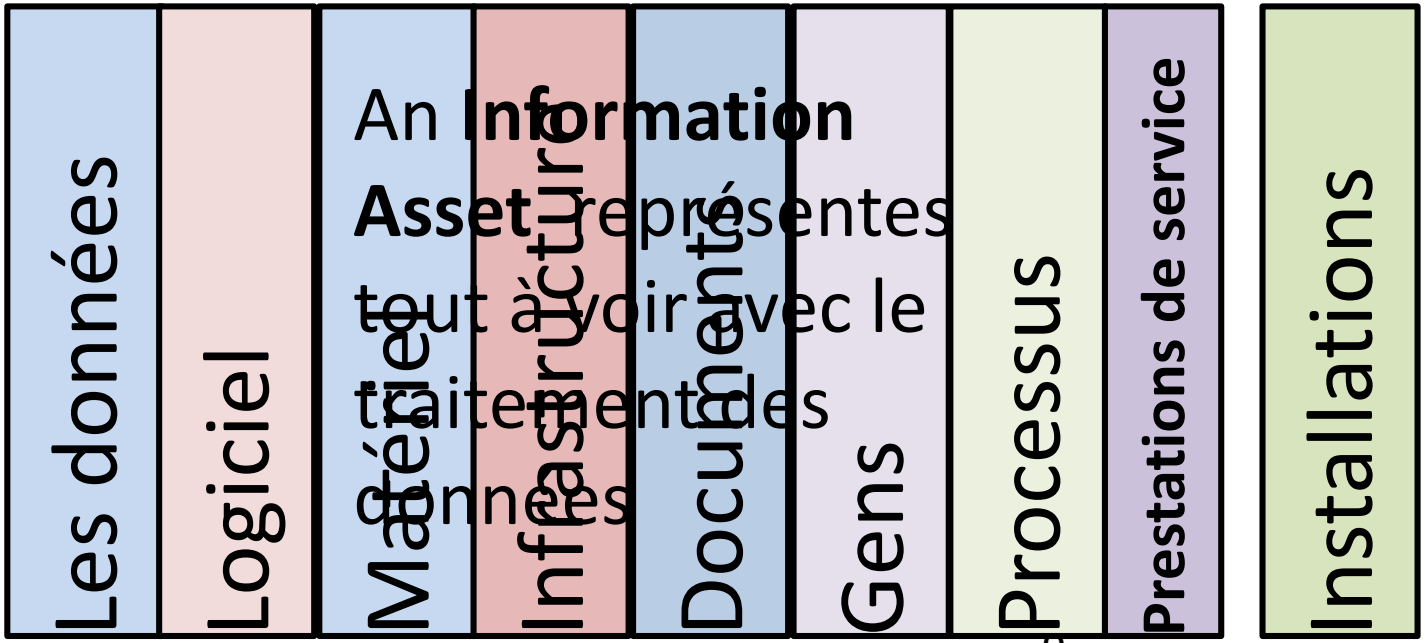
- **leur résilience numérique** et leur **bien-être** et **protection** en ligne, lorsqu'ils profitent des possibilités offertes par l'Internet

- est une **responsabilité commune** - , les décideurs, le secteur privé, les parents, les personnes s'occupant d'enfants, les éducateurs et autres acteurs doivent veiller à ce que les enfants puissent réaliser tout leur potentiel – en ligne et hors ligne.

ÉDUCATION AUX MÉDIAS

Le but de « **l'éducation aux médias** » est pour aider les personnes de **tous âges** de **développer les habitudes d'enquête et les compétences** d'expression qu'ils doivent être **des penseurs critiques, des communicateurs efficaces et des citoyens actifs** dans le monde d'aujourd'hui.

Actifs d'information



Sondage – Jour 3

ITU Publications

International Telecommunication Union
Development sector

Guidelines for industry on Child Online Protection

2020

Sécurité par Conception (SbD)

Les principes de sécurité par/dès la conception (SbD) que le eSafety Commissioner (eSafety), Australie

Le SbD souligne l'importance de **considérer de manière proactive la sécurité des utilisateurs comme une atténuation standard des risques au cours du processus de développement.**
La sécurité de mise à niveau est autorisée, mais au lieu de cela, **permettre aux utilisateurs de subir des dommages avant de s'attaquer au problè**me.
SbD insiste sur la **nécessité de lutter contre les préjudices en ligne**, aux côtés de la sécurité et des droits des utilisateurs.

La sécurité par conception

Ces principes

- fournir des conseils **pour intégrer, améliorer et évaluer les considérations de sécurité** des utilisateurs tout au long des phases de conception, de développement et de déploiement d'un cycle de vie de service typique.
- Les principes **placent fermement la sécurité** des utilisateurs comme un **principe de conception** fondamental qui doit **être intégré dans le développement** des innovations technologiques dès le départ.

Principe SbD: **responsabilités des prestataires de services**

En son cœur se trouvent les principes SbD, d'un modèle pour l'industrie de toutes tailles et de tous **stades de maturité, fournissant des conseils pour intégrer**, évaluer et améliorer la sécurité des utilisateurs. Les trois principes clés sont les suivants:

- Le fardeau de la sécurité ne devrait **jamais incomber uniquement à l'utilisateur final**. Les prestataires de services peuvent **prendre des mesures préventives pour s'assurer que leur service est moins susceptible** de faciliter, enflammer ou encourager des comportements illégaux et inappropriés.

SbD

Principe SbD 2: Autonomisation et l’autonomie des utilisateurs

La dignité des utilisateurs est d’une importance capitale, **l’intérêt supérieur des utilisateurs** étant une considération primordiale, à travers des fonctionnalités, et une approche de conception inclusive qui garantit l'autonomie et l'autonomie des utilisateurs dans le cadre de l'expérience en service

Principe SbD 3: Transparence et responsabilité

La transparence et la responsabilité sont les **caractéristiques d'une approche robuste** de la sécurité. Ils fournissent non seulement **l'assurance que les services fonctionnent conformément à leurs objectifs** de sécurité publiés, mais contribuent également à **éduquer et responsabiliser les utilisateurs sur les mesures** qu'ils peuvent prendre pour résoudre les problèmes de sécurité.

Assurez-vous qu'il existe des **protocoles internes clairs pour interagir** avec les forces de l'ordre, les services d'assistance et les lignes d'assistance téléphonique pour les contenus illégaux
.

Fournir des mesures et **des outils techniques qui permettent aux utilisateurs de gérer leur propre sécurité** de manière adéquate et qui sont définis par défaut sur les **niveaux de confidentialité et de sécurité** les plus sûrs.

Intégrer les considérations, la **formation et les pratiques relatives à la sécurité** des utilisateurs dans les **rôles, fonctions et pratiques de travail** de toutes les personnes qui travaillent avec, pour ou au nom du produit ou du service.

Développer des **normes communautaires**, des **conditions de service et des procédures de modération** qui sont mises en œuvre de manière équitable et cohérente.

Fournissez aux utilisateurs des **fonctions de support intégrées et des boucles de rétroaction qui informent** les utilisateurs de l'état de leurs **rapports, des résultats obtenus** et offrent une opportunité d'appel.

Mener un **engagement ouvert avec** une large base d'utilisateurs, y compris des experts et des parties prenantes clés, sur le développement, l'**interprétation et l'application des normes de sécurité** et leur efficacité ou leur pertinence.

Mettre en œuvre **les contrats sociaux** au moment de l'inscription; ceux-ci décrivent les **devoirs et responsabilités du service,** de l'utilisateur et des tiers pour la sécurité de tous les utilisateurs.

Tirez parti de l'utilisation des **fonctionnalités techniques pour atténuer les risques et les préjudices**, qui peuvent être **signalés aux utilisateurs au point de pertinence**, et qui incitent et optimisent des interactions plus sûres.

S'engager à **innover constamment et à investir dans des technologies améliorant la sécurité** de manière continue et à collaborer et partager avec d'autres outils, meilleures pratiques, processus et technologies améliorant la sécurité.

Zoom Case: Comment la technologie adhère aux principes de conception de sécurité

Selon l'annonce d'Avril de Zoom, un certain nombre de mesures ont été introduites par la société pour résoudre les problèmes de sécurité et de confidentialité. Zoom a annoncé **immédiatement un gel du développement** de nouvelles fonctionnalités et a **transféré toutes les ressources d'ingénierie pour résoudre** les problèmes de sécurité et de confidentialité.
La société a mené un **examen approfondi avec des experts tiers** et mis en place un conseil RSSI (CISO).

- Zoom a **offert une série de sessions de formation, de didacticiels, de webinaires quotidiens** interactifs gratuits aux utilisateurs et a pris des mesures pour minimiser les temps d'attente pour que les clients puissent être autorisés à **utiliser les différents paramètres proposés dans le produit pour organiser des réunions plus sécurisées.** Ces caractéristiques comprennent:
- - Limitez la participation aux participants qui sont connectés à la réunion à l'aide de l'adresse e-mail indiquée dans la réunion invitée.

Cont’

- **Configurer une fonction de salle d'attente**
- **Mot de passe protéger l'accès aux réunions**
- **Verrouiller les réunions une fois qu'elles commencent**
- **Couper le son des participants qui ne présentent pas**
- **Supprimer les participants indésirables**
- **Désactiver le chat privé**

Zoom prépare un rapport de transparence **pour détailler les informations liées aux demandes de données, d'enregistrements et de contenu**. Le **PDG de la société a organisé des webinaires** hebdomadaires pour répondre aux questions de la communauté.

Les principaux défis de Zoom en matière de conception éthique et de confidentialité

- Une série de **failles de sécurité et de violations de la vie privée ont été découvertes sur Zoom.**
- Le 30 mars 2020, le **FBI a publié un avertissement public** concernant un problème nommé d'après Zoom - **«Zoom-Bombing».**
- L'entreprise était également dit **avoir partagé des données utilisateur avec des tiers et faire de fausses déclarations** sur l'algorithme de chiffrement il utilise.

- En juin, Zoom a **fermé les comptes des dissidents Chinois après une réunion Zoom** en ligne sur l'anniversaire du mouvement social de la place Tiananmen en 1989.
- Le 1er Avril, Zoom a publié un article un blog pour **répondre à une liste de critiques et a présenté un plan de 90 jours**. Le 29 juin, l'entreprise **a nommé un nouveau responsable de la sécurité de l'information**.

Les mêmes erreurs continuent d'exposer les enfants à des préjudices en ligne.

Le retraitement pour la sécurité est acceptable, **mais qu'est-ce qui fonctionnerait le mieux dans notre situation particulière?**

- **Autorégulation**
- **Co-régulation**
- **Réglementation complète**
- **Quelle direction?**

Lignes directrices pour l'industrie

Cinq domaines clés pour l'industrie

- 1. Intégrer les préoccupations relatives aux droits de l'enfant dans toutes les politiques et processus de gestion appropriés de l'entreprise
- 2. Développer des processus standard pour traiter le matériel d'abus sexuel d'enfants (CSAM)
- 3. Créer un environnement en ligne plus sûr et adapté à l'âge
- 4. Éduquer les enfants, les soignants et les éducateurs à la sécurité des enfants et à l’utilisation responsable des TIC
- 5. Promouvoir la technologie numérique en tant que moyen d'accroître l'engagement civique

Intégrer les préoccupations relatives aux droits de l'enfant dans toutes les politiques d'entreprise et processus de gestion appropriés

Intégrer les droits de l'enfant

- Appelé par les Principes directeurs des Nations Unies relatifs aux entreprises et **aux droits de l'homme**
- La **vie privée et la liberté** d'expression sont particulièrement importantes à protéger
- Respecter les **réglementations nationales**, mais aller au-delà au moins des normes internationales
- Veillez à éviter toute **compromission involontaire** des droits de l'enfant

Élaborer une politique de protection de l'enfance

- Mettre en place une **équipe de gestion de la politique de protection de l'enfance avec une supervision** et une autorité sur la COP
- **Consulter les parties prenantes** (y compris les enfants) sur la meilleure façon d'autonomiser et de protéger les droits des enfants
- S'assurer que la **politique respecte ou dépasse les normes** internationales
- Diligence raisonnable de la COP: évaluer si l'entreprise peut contribuer à des effets néfastes sur les enfants

Caractéristiques et évaluation

- Système de signalement des plaintes
- Conception adaptée à l'âge
- Dépistage automatisé des activités et contenus inappropriés
- Ventilez les évaluations d'impact par sous-groupe, tel que l'âge

Développer des processus standard pour gérer CSAM

Matériel d'abus sexuel d'enfants

- **Problème généralisé:** Internet Watch Foundation a trouvé plus de 100 000 sites avec en 2019
- Efforts d'éradication étendus de la part des **gouvernements et des organisations (ONG)** à but non lucratif, mais l'industrie a également un rôle à jouer

Reporting CSAM

- Avoir un service de reporting
- Faire connaître les hotlines pour les rapports CSAM: application de la loi, organismes à but non lucratif pour la sécurité des enfants (par exemple, IWF, ICMEC - INHOPE a une liste complète)
- Transmettre les rapports aux forces de l'ordre et aux organisations internationales de sécurité des enfants
- Veiller à ce que le processus minimise l’exposition des personnes au matériel et fournir un soutien pour la santé mentale du personnel

Gestion du CSAM

- Créer une équipe pour intégrer les efforts de lutte contre le CSAM dans le produit et rendre compte des progrès
- Bloquer le matériel signalé mais ne pas supprimer
- Coopérer avec les forces de l'ordre
- Créer un système de conservation des données pour faciliter les enquêtes

Outils technologiques

- PhotoDNA: numérisation de photos et de vidéos préservant la confidentialité de Microsoft
- Projet Artemis: analyse les chats pour trouver des signes de toilettage, également de Microsoft
- IWF dispose d'outils de détection et de blocage CSAM et de listes de noms de domaine pour les FAI
- Utilisez régulièrement ces outils pour rechercher des CSAM

Créer un environnement en ligne plus sûr et adapté à l'âge

Réduire les risques

- Récapitulatif: les risques sont le c**ontenu, le contact et la conduite, et peuvent être agressifs, sexuels, basés sur des valeurs ou commerciaux** sur le sujet
- Le risque ne sera **pas éliminé, mais peut être réduit**
- L'action des enfants crée des comportements à risque, ce qui contribue à **développer l'autonomie et la résilience**
- Là où le risque est encore important, les utilisateurs peuvent être informés
- Les TIC destinées aux enfants sont tenues à un niveau plus élevé

Communication ouverte

- Communiquez de **manière professionnelle et claire** avec les enfants
- Lorsque le contenu peut **être inapproprié pour les enfants** (par exemple, le contenu généré par l'utilisateur), **indiquez-le au préalable**
- Soyez **transparent sur la manière** dont les contrôles parentaux empiètent sur les droits des enfants à la vie privée
- Fournir des **précisions sur les produits ou services** disponibles
- Indiquez le groupe d'âge cible, éventuellement en utilisant **des systèmes de classification du contenu** local

Environnement positif

- Utilisez un code de conduite pour indiquer les attentes comportementales
- Espaces sociaux modérés pour éviter le harcèlement, l'usurpation d'identité, etc.
- Expliquez clairement les possibilités de signalement
- Traiter les rapports en temps opportun et autoriser un appel
- Communiquer avec le journaliste et le journaliste sur l’état du rapport

Contrôle de la confidentialité et du contenu

- Réduisez au minimum la collecte de données auprès des enfants, en respectant la confidentialité dès la conception
- Utilisez des technologies préservant la confidentialité lorsque cela est possible
- Envisagez de fournir des outils de contrôle parental, y compris les achats et les limites de temps
- Envisagez la vérification de l'âge pour diriger les enfants vers des espaces adaptés à leur âge
- Faites attention de ne pas restreindre leur liberté d'expression ou de violer leur vie privée

Interactions avec l'industrie

- Prenez soin des personnes qui travaillent pour vous et prennent soin des enfants
- Assurez-vous que la publicité est sécurisée pour les enfants

Collaborez avec d'autres entreprises pour partager des informations sur la COP

Éduquer les enfants, les Parents et les éducateurs à la sécurité des enfants et à l’utilisation responsable des TIC/ICT

Le rôle de l'industrie dans l'éducation

- **Sensibilisation** et éducation vitales
- Responsabilité **partagée** avec **les écoles et les parents**
- Peut être plus efficace en **travaillant indirectement**

- Les parents et les enseignants connaissent mieux la situation de l’enfant, mais peuvent eux-mêmes avoir besoin d’éducation

Thèmes éducatifs

- Promouvoir le respect des limites d'âge
- Montrez aux parents comment aider leurs enfants à utiliser le service
- Mettre en évidence et fournir des instructions claires sur les contrôles parentaux et les fonctions de sécurité
- Utilisez un langage simple et compréhensible localement

Partenariats

- S'engager avec les parties prenantes pour trouver les meilleurs moyens d'éduquer:

Gouvernement, éducateurs, parents, enfants, autre industrie

- Les ONG de sécurité en ligne pour enfants peuvent fournir des conseils précieux

Les Guides de sécurité en ligne pour enfants

- Digiworld: jeu et matériel pédagogique associé de Telenor
- Be Internet Awesome + Interland: programme et jeu de Google
- Cours virtuels de Telefónica et Capital Humano y Social Alternativo
- Campagne d’éducation aux médias de Twitter
- Projet deSHAME: boîte à outils et ressources pour les écoles et les forces de l'ordre de Facebook et de l'UE
- Promouvoir la technologie numérique comme moyen d'augmenter l'engagement civique

Promouvoir la technologie numérique comme moyen d'augmenter l'engagement civique

«L'enfant a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toutes sortes, indépendamment des frontières, que ce soit oralement, par écrit ou par écrit, sous forme d'art ou par tout autre média au choix de l'enfant. "

–Article 13 de la Convention des Nations Unies relative aux droits de l'enfant

Participation civique

- L'industrie peut **faciliter activement la participation civique** des jeunes
- Veiller à ce que les **efforts visant à protéger les enfants n’étouffent pas leur droit** de participer et de s’exprimer
- Réduisez la **fracture numérique** pour que toutes les voix soient entendues

Éviter le silence

- Encourager le droit de participer aux politiques
- Gerer le le procesus du dialogue pour les enfants, pas vers des environnements où les adultes n’entendront pas leur voix
- Ne bloquez pas trop le matériel
- Peut entraver l'engagement et le développement de la résilience
- Indiquez clairement lorsque le matériau est bloqué
- Autoriser la contestation du blocage

Renforcer la participation

- Développer des **plateformes d'expression** civique des jeunes
- Inculquer la **pensée créative et la résolution** de problèmes chez les utilisateurs
- **Promouvoir la culture** numérique et les compétences en TIC
- Élargir l'accès aux populations mal desservies

Directives spécifiques aux fonctionnalités

Focus spécial sur Industries

- Infrastructure numérique
- Médias et jeux
- Des médias sociaux
- Intelligence artificielle

Infrastructure numérique

À propos de l'infrastructure numérique

Exemples:

- Fournisseurs de connectivité / FAI/ISP
- Services d'hébergement/Hosting
- Fournisseurs de stockage de données
- Cafés Internet

Combattre le CSAM

- **Collaborer étroitement** avec le gouvernement et les forces de l'ordre

  - Fournir **une formation** aux TIC aux agents des forces de l'ordre

- Utilisez des **listes de blocage**, pour empêcher l'accès aux domaines CSAM
- Activer **les rapports d'utilisateurs**, en indiquant ce qui est illégal et comment signaler
- Avoir une **procédure pour se conformer aux avis de retrait**

Créer un environnement plus sûr

- Créer **des outils de blocage et de filtrage**
  - Vous pouvez également mettre en évidence les ceux qui existent déjà.
- Les fournisseurs de WiFi publics devraient envisager de **filtrer le contenu**, en particulier si les enfants accèdent au réseau, et **d'encrypter le trafic réseau**
- Les services d'hébergement devraient avoir des **fonctionnalités de signalement des abus**

Médias et jeux

À propos des médias et des jeux

- Ceux-ci offrent des matériaux sélectionnés et conçus
  - Sites Web qui créent leur propre contenu, tels que des sites d'actualités
  - Jeux
  - Services vidéo et multimédia

Créer un environnement plus sûr

- Utilisez un **système de classification du contenu** cohérent dans l'ensemble du secteur
- **Distinguer clairement la publicité du contenu** et réglementer la publicité destinée aux enfants
- Utilisez la **vérification de l'âge pour restreindre le contenu** destiné à un public plus âgé
- Tenez-vous-en au **matériel destiné aux enfants ou aux adultes**

Éducation et plus

- **Encourager la participation des parents** à la consommation des médias par l'enfant
- Combattre les comportements **addictifs**, en particulier pour les **fournisseurs de jeux**
- **N'incluez que des images ou des informations** sur des enfants spécifiques dans le matériel avec une bonne raison
- **Détecter, masquer, conserver et signaler** le contenu généré par l'utilisateur contenant CSAM
- Développer du matériel **adapté à l'âge destiné** à susciter l'intérêt civique chez les jeunes

Les Médias Sociaux

À propos des médias sociaux

Catégories:

1. Applications de messagerie (par exemple WhatsApp, Telegram)
2. Services de réseautage social et de découverte de contenu (par exemple Facebook, TikTok)
3. Services de diffusion en direct (par exemple, Twitch, YouTube Live)

Certains intermédiaires, tels que Snapchat (1 et 2) ou OnlyFans (2 et 3)

Créer un environnement plus sûr

- Avoir des **paramètres de confidentialité et de partage de contenu** par défaut plus stricts pour les jeunes utilisateurs
- S'assurer que les utilisateurs disposent **d'outils pour bloquer et signaler les communications** indésirables
- Envisager des restrictions d'accès aux groupes de **discussion dont le contenu est inapproprié** pour les jeunes utilisateurs
- Incorporer **le point de vue des enfants dans l'élaboration** d'un programme de modération de contenu
- **Supprimer le contenu partagé** contenant des informations personnelles sensibles sur les enfants

Éducation et combat contre CSAM

- Créer un système de réputation formel pour encourager un **comportement positif**
- Obtenez **la permission des enfants** apparaissant dans le contenu généré par les utilisateurs en vedette
- **Analyser de manière proactive** le contenu généré par l'utilisateur pour CSAM au fur et à mesure de son téléversement
- Informer les utilisateurs que le matériel illégal, y compris le CSAM, sera **retiré et peut entraîner une interdiction ou une action en justice**

Systèmes d‘Intelligence Artificielle - IA

À propos de l'IA

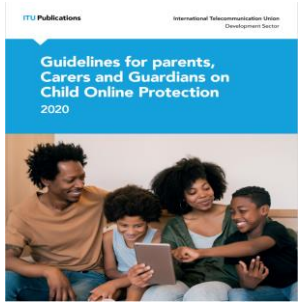
- Parfois appelé «**machine learning», «deep learning**», etc. - un domaine quelque peu flou
- Croissance de **la prévalence, des capacités et de la gamme d'applications**
- Facebook utilise un système automatisé pour détecter le matériel faisant la promotion de l'automutilation
- Instagram en utilise un pour trouver la cyberintimidation
- Mais les programmes font exactement ce que vous leur dites de faire, pas ce que vous voulez dire!
- Par exemple. susciter l'engagement en orientant les enfants vers des contenus extrêmes

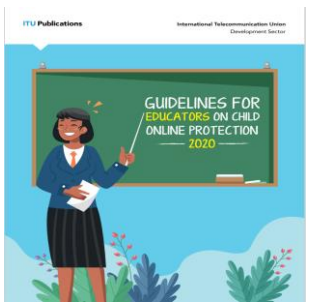
Plan opérationnel du UIT-D 2020-2023

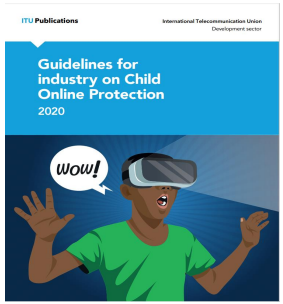
Défis?

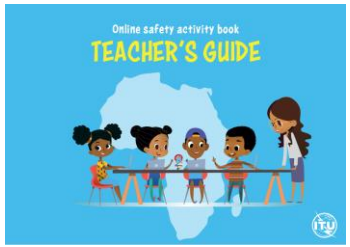
- **The pandemic of COVID-19 shows the urgent need to action:** Children and young people spend more time online, so do online predators.
- **Connectivité:** de nombreux enfants n'ont pas les moyens de se connecter avec le monde extérieur, ni de **bénéficier des opportunités offertes par Internet** (apprendre, jouer, communiquer, s'engager, etc.).
- • **Fracture numérique**: la fracture numérique va au-delà des questions de connectivité, étant fortement liée aux **compétences numériques et à la littératie numérique** des enfants et des familles.
- • **Écart de transformation numérique:** les enfants doivent avoir **accès, compétences, éducation et protection en ligne.**
- • **Écart de compétences numériques et d'alphabétisation:** les enfants doivent être **équipés et engagés** dans des programmes **de compétences numériques et d'alphabétisation numérique** qui comprennent des mesures de sécurité et de protection.
- • **La pandémie de COVID-19 nous montre le besoin urgent d'agir**: les enfants et les jeunes passent plus de temps en ligne, tout comme les prédateurs en ligne.

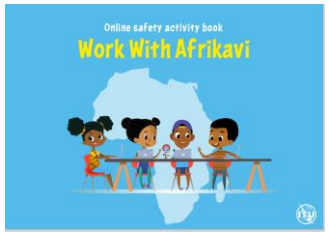
Avec lesLignes directives COP révisées et réécrites











<u>Campagne Instagram</u>

La campagne couvre huit messages clés et un microsite: https://www.itu-cop-guidelines.com/netrules

Avec engagement envers COP

- **Niveau National:** créer l'**écosystème** dans votre pays pour établir un **Cadre National**?
- **Harmoniser les Lois et Coordonner les actions** au niveau national.
- Identifier les **Parties Prenantes** (entités gouvernementales, ONG, etc.) et réaliser une **évaluation nationale de la situation actuelle**.
- Identifier les **institutions de recherche** (universités) et le **secteur privé** pour prendre des mesures sur les différentes priorités?
- Mettre en place **l'infrastructure pour mettre en œuvre** les politiques.

ITU/COP Initiative &(w) WeProtect

Pourquoi les Lignes Directrices de l'UIT 2020 COP?

• Fournir la toute première **approche holistique de la COP** avec une large focalisation sur **toutes sortes de risques et de préjudices**, mais aussi potentiels, pour les enfants liés à l'environnement en ligne.

• **Effort conjoint d'un groupe de travail d'experts, d'enfants et de jeunes**.

• Servir **de plateforme de leadership** avec une **communauté multipartite**, fournissant un solide réseau de partenaires pour la validation et la mise en œuvre conjointe

Vision

Nous créons un monde dans lequel les enfants peuvent être connectés et peuvent pleinement profiter des opportunités d'un environnement en ligne fiable et sûr

Les 3 Domaines d‘Objectifs du Plan de Mise en Œuvre

- Domaine d’objectif 1: Développement des capacités et des compétences en matière de protection en ligne des enfants

- Domaine d’objectif 2: Assistance aux politiques

- Domaine d'objectif 3: Bilan international de la mise en œuvre de la COP.

#COP4Africa
#SafeOnline