

Avis en faveur d'un environnement numérique sûr, inclusif et conforme aux droits de l'enfant

Date : 28/01/2026

Face à l'ampleur mondiale et européenne des abus et de l'exploitation sexuelle, qui touche respectivement un enfant sur huit¹ et un sur cinq², et malgré le tournant majeur marqué par la Convention de Lanzarote en 2007, le phénomène s'aggrave, comme en témoigne l'augmentation spectaculaire des signalements en ligne (jusqu'à + 6000 % au cours des dix dernières années dans l'UE³) et un nombre record de plus de 36,2 millions de signalements d'exploitation présumée en 2023, révélant une crise d'autant plus grave qu'un tiers des victimes gardent le silence, nécessitant un renforcement continu des législations pour mieux protéger les enfants⁴.

Le cadre européen

L'Union européenne a établi un cadre pour un internet plus sûr, notamment grâce au règlement sur les services numériques (*Digital Services Act, DSA*)⁵ et à la proposition de règlement relatif à la lutte contre les abus sexuels commis sur enfants (CSAR - Child Sexual Abuse Regulation)⁶

Le DSA, pleinement applicable depuis février 2024, est considéré comme un levier essentiel pour rendre les plateformes responsables de leurs contenus et services. Il met en œuvre les principes de « sécurité dès la conception » (*safety by design*) et de « protection par défaut » (*safety by default*).

¹ UNICEF. Action to End Child Sexual Abuse and Exploitation : A Review of the Evidence, 2020.

² « Campagne un sur cinq du Conseil de l'Europe contre la violence sexuelle à l'égard des enfants » sur <https://www.coe.int>

³ Commissaire européenne aux Affaires intérieures, Ylva Johansson, sur <https://www.childsafetyineurope.com>.

⁴ Rapport A/79/122 de la Rapporteuse spéciale sur la vente d'enfants, l'exploitation sexuelle d'enfants et les abus sexuels sur enfants, 9 août 2024.

⁵ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Digital Services Act), JOUE L 277 du 27.10.2022, p. 1–102. Disponible sur EUR-Lex : <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

⁶ https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0011.02/DOC_1&format=PDF

Les très grandes plateformes en ligne (VLOP/ VLOSE⁷) ont des obligations renforcées, notamment :

- Réaliser des évaluations régulières des risques (y compris les risques pour les mineurs) ;
- Bannir les interfaces trompeuses (*dark patterns*) et offrir des systèmes de recommandation transparents, avec au moins une option « non fondée sur le profilage » ;
- Interdire la publicité ciblée fondée sur les données des mineurs ;
- Proposer des paramètres de confidentialité renforcés par défaut pour les mineurs, ainsi qu'un design adapté à l'âge ;
- Fournir des mécanismes de signalement accessibles.

Le CSAR, lui, vise à établir un cadre permanent de prévention, de détection ciblée et de signalement des images d'abus sexuels sur enfants afin d'éviter un vide juridique à l'échéance du régime temporaire actuel. Le Délégué général soutient ce texte, sous réserve de garanties strictes en matière de droits fondamentaux.

Risques systémiques

Le fonctionnement des plateformes repose sur une « économie de l'attention » qui met les utilisateurs en danger à des fins mercantiles. Les effets sur la santé mentale des mineurs sont qualifiés de « dévastateurs » et de « mortifères ».

Le rapport d'une commission d'enquête française a d'ailleurs qualifié TikTok « d'un des pires réseaux sociaux à l'assaut de notre jeunesse ».⁸

Ces plateformes offrent des services en ligne apparemment gratuits (réseaux sociaux, messageries) uniquement parce que la collecte indistincte de données à caractère personnel constitue leur véritable valeur économique. Les entreprises utilisent des algorithmes pour

⁷ VLOP (*Very Large Online Platform*) et VLOSE (*Very Large Online Search Engine*) sont les catégories définies par le DSA pour désigner les plateformes et moteurs de recherche comptant plus de 45 millions d'utilisateurs actifs mensuels dans l'Union européenne.

⁸ <https://www.assemblee-nationale.fr/dyn/17/organes/autres-commissions/commissions-enquete/tiktok>

traiter ce *Big Data* dans le but d'influencer les comportements à des fins commerciales, poussant à prolonger leur temps de présence.

Les algorithmes présentent des risques spécifiques :

- Ils sont souvent des « boîtes noires » dont le fonctionnement exact et les objectifs sont opaques.
- Ils ne sont pas neutres et peuvent renforcer les préjugés sociaux (racistes ou sexistes) à cause des biais introduits par leurs concepteurs ou des déséquilibres dans les bases de données d'apprentissage.
- Le filtrage personnalisé tend à réduire la diversité des informations, enfermant les utilisateurs dans le « profil » prédéfini.

Recommandations du Délégué général

1. L'environnement numérique, un enjeu majeur crucial pour la santé publique et les droits de l'enfant

L'environnement numérique est une composante essentielle de la vie quotidienne des enfants et des jeunes en Fédération Wallonie-Bruxelles : un internaute sur trois est un enfant âgé de 0 à 18 ans⁹. Cet espace offre d'immenses possibilités pour l'exercice des droits reconnus par la Convention internationale relative aux droits de l'enfant (CIDE), notamment le droit à l'information (art. 17 CIDE), à la liberté d'expression (art. 13 CIDE), à l'éducation (art. 28 CIDE) et à la participation (art. 12 CIDE).

Toutefois, le numérique expose également les mineurs à des risques importants tels que les sollicitations excessives, les (cyber)violences (art. 19 CIDE), les atteintes à la vie privée (art. 16 CIDE), l'exposition à des contenus nuisibles (art. 17 CIDE), l'isolement social (art. 15 CIDE) et le mal-être, ce qui en fait un enjeu majeur de santé publique (art. 6 CIDE). Le numérique agit en effet comme un puissant catalyseur en favorisant la diffusion, la permanence et la viralité des violences. Selon le rapport d'évaluation mondiale de la menace 2023 de la *We Protect Global*

⁹ Conseil de l'Europe, Stratégie du Conseil de l'Europe pour les droits de l'enfant (2022-2027) - Les droits de l'enfant en action : poursuivre la mise en œuvre et innover ensemble, mars 2022, p. 29 ;

Comité de Lanzarote, Avis interprétatif sur l'applicabilité de la Convention de Lanzarote aux infractions sexuelles commises à l'encontre des enfants et facilitées par l'utilisation des TIC, 12 mai 2017, p. 5 ;

UNICEF, La situation des enfants dans le monde : Les enfants dans un monde numérique, décembre 2017.

Alliance, 54 % des jeunes adultes déclarent avoir subi des agressions sexuelles en ligne durant leur enfance.¹⁰

2. Protéger les enfants dans le numérique, et non les en exclure

Ces constats alarmants invitent à repenser la protection des enfants en ligne non pas comme une mise à distance du numérique, mais comme la garantie d'un environnement sûr, inclusif et respectueux de leurs droits. Pour le Délégué général, il convient de protéger les enfants et les jeunes **dans** le numérique, et non de les en exclure. Cette approche intégrée combine protection, autonomisation et accompagnement éducatif. En cette matière, on peut utilement se référer aux travaux et campagnes de sensibilisation développées par Yapaka au sujet de l'utilisation des écrans par les enfants¹¹ ainsi qu'au récent avis du Conseil supérieur de la santé sur les effets de l'utilisation des écrans et des réseaux sociaux sur les jeunes¹². Relevons également que le réseau européen des ombudsmans des enfants (ENOC - European Network of Ombudspersons for Children) ainsi que son forum participatif de jeunes (ENYA - European Network of Young Advisors) se sont également penchés sur la question des droits de l'enfant dans l'environnement numérique et ont tous deux formulé des recommandations en la matière.¹³

3. Intérêt supérieur de l'enfant (art. 3) et droit à la vie privée (art. 16)

L'intérêt supérieur de l'enfant recommande de placer la protection et le développement des enfants au cœur de toute réflexion sur les outils numériques, y compris dans les choix législatifs ou technologiques. L'article garantit la protection contre les atteintes à la vie privée.

- La protection doit être assurée dans le numérique, et non par l'exclusion. Le Délégué général s'oppose à une interdiction généralisée des réseaux sociaux avant 15 ans. Une telle mesure est jugée peu applicable, potentiellement discriminante, et inefficace, car elle encouragerait le contournement (par exemple via le partage ou le prêt de comptes

¹⁰ We Protect Global Alliance, [Évaluer l'ampleur et la portée de l'exploitation et des abus sexuels en ligne envers les enfants pour transformer la riposte](#), 18 août 2023.

¹¹ Notamment la campagne « Maîtrisons les écrans : La campagne 3-6-9-12 donne des repères » - <https://www.yapaka.be/écrans>

¹² <https://www.hgr-css.be/fr/avis/9877/les-effets-de-lutilisation-des-ecrans-et-des-reseaux-sociaux-sur-les-jeunes>

¹³ <https://enoc.eu/wp-content/uploads/2020/01/FV-D%C3%A9claration-ENOC-2019-sur-les-droits-de-lenfant-dans-lenvironnement-num%C3%A9rique.pdf> et <https://enoc.eu/wp-content/uploads/2019/10/ENYA-2019-report-and-recommendations-FV.pdf>

d'adultes) et la migration vers des plateformes moins régulées. Si les enfants se déclarent majeurs ou utilisent des comptes d'adultes, ils perdent les garanties de sécurité prévues par le DSA telles que les paramètres de confidentialité renforcés et les limitations du profilage et ils et s'exposent à des risques pour leur vie privée. À cet égard, le Délégué général ne soutient pas une identification générale des utilisateurs (« pseudonymat vérifié »), en raison de son effet dissuasif sur la parole des jeunes (« chilling effect ») et de son manque de proportionnalité par rapport à des enquêtes ciblées sous contrôle judiciaire.

La responsabilité première doit être portée par les plateformes, et non par les familles ou les enfants. Cette responsabilité doit s'inscrire dans l'application rigoureuse du DSA, concrétisant les principes de sécurité dès la conception (*safety by design*) et de protection par défaut (*safety by default*).

- Mettre en place des lignes directrices belges sur l'assurance d'âge, conformes au DSA, qui doivent être proportionnées, inclusives et respectueuses de la vie privée. L'objectif doit se limiter à la vérification d'une tranche d'âge (oui/non), et non l'identification des personnes. L'assurance d'âge ne doit pas devenir un outil d'identification des utilisateurs. Les solutions doivent en outre être « privacy-preserving » (minimisation des données, pas de base centrale, pas de collecte excessive ni de profilage biométrique). Enfin, pour être réellement inclusives, les solutions doivent être accessibles aux jeunes sans smartphone et fonctionner aussi sur ordinateur, y compris en usage partagé ou familial.
- Concernant la proposition de règlement CSAR, le Délégué général demande de préserver le chiffrement de bout en bout, la protection de la vie privée, et de conditionner toute détection à des ordres ciblés, nécessaires et proportionnés délivrés par une autorité judiciaire ou indépendante.

4. Droit à la vie, à la survie et au développement (art. 6) et santé physique et mentale (art. 24)

L'article 6 de la CIDE impose de veiller à l'impact de la surexposition numérique sur la santé physique, mentale et sociale des enfants. Le droit à la déconnexion est jugé essentiel pour protéger la santé physique et mentale et le développement des enfants.

- Le Délégué général recommande, en s'inspirant du droit des adultes, d'instaurer via les règlements d'ordre intérieur (ROI) des établissements, des « trêves numériques scolaires ». Celles-ci limiteraient l'exigence de remise de devoirs après une heure fixée et restreindraient les sollicitations le week-end, favorisant un équilibre de vie sain.
- L'école doit désactiver les notifications non essentielles sur les outils numériques institutionnels. Elle doit également éviter les mécanismes de jeu incitant à un usage compulsif (gamification compulsive) et privilégier des paramétrages sobres et non intrusifs.
- Une vigilance accrue et un accompagnement éducatif continu sont requis tout au long du parcours scolaire, notamment face à l'hyperconnexion importante des adolescents qui dépasse largement les recommandations en matière de santé publique.

5. Droit d'être entendu et à participer (art. 12)

Le droit à la participation suppose de donner aux enfants la possibilité de s'exprimer sur leurs usages du numérique et d'être entendus dans les politiques publiques qui les concernent.

- Il est nécessaire de construire, avec les enfants, un dialogue collectif et continu ayant des répercussions concrètes.
- Il faut associer les jeunes eux-mêmes aux réflexions et à la construction des règles d'usage, notamment à travers des conseils consultatifs, des ateliers de co-construction et des consultations régulières sur la déconnexion et la vie numérique à l'école. Le Délégué général insiste sur le fait qu'on protège mieux en construisant avec les enfants.

6. Droit à l'information, à la protection contre les contenus nuisibles (art. 17) et autonomisation

L'article 17 de la CIDE reconnaît le rôle essentiel des médias dans la diffusion d'informations bénéfiques à l'enfant, tout en exigeant des États qu'ils protègent les enfants contre les informations préjudiciables à leur bien-être. L'approche doit être éducative et visée par le *digital empowerment*.

- Le Délégué général recommande de renforcer les programmes d'éducation aux médias et le volet numérique de l'éducation à la vie relationnelle, affective et sexuelle (EVRAS).

- L'éducation aux médias et au volet numérique de l'EVRAS, qui sont considérées comme des responsabilités collectives essentielles pour l'autonomisation et la protection des jeunes dans l'environnement numérique doivent aborder des thèmes cruciaux tels que le consentement et l'intimité numériques, l'e-réputation, le sexting, les *deepfakes*, l'intelligence artificielle (IA) générative, le *grooming*, la pornographie et les algorithmes de recommandation.
- L'éducation est préférable aux interdictions pures et simples car elle donne aux jeunes les clés pour comprendre, décrypter et résister aux manipulations en ligne.

7. Droit à la protection (art. 19)

La prévention dans l'environnement numérique doit devenir une priorité collective pour mieux protéger les enfants. Les abus sexuels en ligne — dont la pédopornographie n'est qu'un exemple parmi d'autres — exigent une action préventive forte, afin d'éviter tout passage à l'acte. En Fédération Wallonie-Bruxelles, il est urgent de renforcer les dispositifs de sensibilisation, d'écoute et d'auto-assistance. Par exemple, sur la question spécifique de la pédopornographie, le modèle flamand et son initiative *Stop It Now!*, claire et accessible, constitue une source d'inspiration. Investir dans la prévention, c'est agir dans l'intérêt supérieur de l'enfant. Prévenir la violence, c'est préserver son intégrité, sa sécurité et son droit à évoluer dans l'environnement numérique de manière sereine.

8. Stratégie nationale pour la protection des mineurs dans l'environnement numérique

- Organiser une conférence interministérielle « Jeunesse et numérique » (fédéral, communautés, régions) pour coordonner les compétences transversales aux différents niveaux de pouvoir et développer un plan national d'application du DSA axé sur les mineurs.
- Renforcer l'Institut belge des services postaux et des télécommunications (IBPT), désigné Coordinateur des services numériques, en y intégrant une cellule « Mineurs en ligne » chargée de la prévention, de la veille des risques et de la réception des plaintes.
- Structurer la coopération entre l'IBPT, les régulateurs communautaires (CSA, VRM, Medienrat) et l'Autorité de protection des données (APD).



- Mettre en place un guichet unique de signalement trilingue (FR/NL/DE), orientant vers les services compétents en matière de protection des mineurs en ligne (Child Focus, forces de l'ordre).
- Certifier, soutenir et financer des « trusted flaggers » (organisations de confiance), afin que leurs signalements soient traités en priorité par les plateformes.

Le Délégué général, tout comme le Comité des droits de l'enfant des Nations Unies dans son commentaire général n°25¹⁴, exhorte la Belgique à s'emparer de ces recommandations pour prendre des mesures efficaces et ambitieuses. C'est au monde numérique de s'adapter aux enfants, et non l'inverse.

¹⁴ <https://www.ohchr.org/fr/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>