



Chapitre A

4. Protection des enfants dans l'environnement numérique



4. La protection des enfants en environnement numérique

L'environnement numérique pose des défis croissants pour la protection des enfants, tant en termes de violences (p. ex. cyberharcèlement, sextorsion, grooming) que de préjudices liés à l'utilisation d'outils numériques. Comme le rapport thématique 2024 de l'OKAJU l'a mis en avant, les réseaux sociaux facilitent l'accès des prédateurs aux enfants et l'intelligence artificielle crée de nouveaux risques, avec notamment la multiplication de matériel d'abus sexuels d'enfants (CSAM) généré artificiellement ; en parallèle, l'usage et la possession généralisés de smartphones et d'appareils connectés facilitent une exposition précoce et croissante des enfants à la pornographie et au CSAM. L'âge du premier contact diminue chaque année et le phénomène prend de l'ampleur, avec des taux d'exposition inédits chez les plus jeunes. Cette exposition massive s'accompagne de graves conséquences : elle constitue un facteur déterminant dans l'augmentation des violences sexuelles entre mineurs – dont le nombre explose de concert avec la précocité des expositions – et participe à l'émergence d'une « culture de l'abus », comme l'analyse en détail le rapport annuel 2024 de l'OKAJU²⁷.

Les impacts sur la santé et le développement liés à l'environnement numérique sont considérables pour les enfants : troubles du sommeil, déficit de l'attention, risque de dépendance numérique, isolement social, retard de langage et augmentation de la sédentarité pouvant conduire à l'obésité, etc. L'utilisation précoce et/ou excessive des smartphones, tablettes et autres écrans s'impose désormais comme un véritable enjeu de santé publique au Luxembourg, appelant des réponses éducatives, préventives et réglementaires afin de mettre en place une stratégie intégrée et globale pour protéger les mineurs.

Une étude de 2025 basée sur les données de plus de 100 000 personnes à travers le monde, menée par Sapien Labs via le Global Mind Project²⁸ – la plus grande base de données sur le bien-être mental – démontre que le fait d'obtenir un smartphone avant 13 ans augmenterait drastiquement le risque de troubles de santé mentale à l'âge adulte²⁹. L'utilisation précoce est associée à des idées suicidaires, à de l'agressivité et au détachement, principalement en raison de l'exposition aux réseaux sociaux, au cyberharcèlement et à la perte de sommeil³⁰.

Les auteurs de l'étude appellent à des mesures urgentes pour restreindre l'accès et protéger les jeunes esprits. Ils insistent que les décideurs doiventurgemment instaurer des restrictions comparables à celles en vigueur pour l'alcool et le tabac, proposant ainsi quatre mesures prioritaires³¹ :

1. Éducation à la littératie numérique pour les enfants d'âge scolaire, incluant des sujets comme le cyberharcèlement et les prédateurs en ligne.
2. Restrictions d'âge contraignantes pour l'accès aux réseaux sociaux, accompagnées de sanctions réelles.
3. Interdiction de l'accès aux réseaux sociaux sur tous les appareils connectés détenus par des enfants de moins de 13 ans.
4. Restrictions progressives d'accès aux smartphones, encourageant des dispositifs « adaptés aux enfants » qui permettent seulement les fonctions de base comme les appels et les SMS, tout en excluant les réseaux sociaux et les contenus algorithmiques.

Tandis que certains demandent des preuves causales plus solides avant d'envisager des restrictions généralisées, les auteurs estiment qu'il n'y a pas de temps à perdre pour obtenir des preuves irréfutables : les politiques de santé publique s'appuient souvent sur la réduction des risques plu-

²⁷ Voir l'annexe à la fin de ce chapitre « Extraits du rapport annuel 2024 de l'OKAJU, chapitre C : « La protection des enfants contre les violences et autres préjudices en milieu numérique ».

²⁸ L'étude internationale menée par Sapien Labs, à partir des données anonymisées de plus de 100 000 jeunes, a été publiée dans une revue scientifique à comité de lecture (peer-reviewed), le Journal of Human Development and Capabilities. Cela garantit la rigueur du processus d'évaluation scientifique et la fiabilité des résultats présentés.

²⁹ <https://www.sciencedaily.com/releases/2025/09/250906013448.htm>

³⁰ <https://www.sciencedaily.com/releases/2025/09/250906013448.htm>

³¹ <https://scitedaily.com/owning-a-smartphone-before-13-linked-to-alarming-mental-health-declines-global-study-finds/>; <https://www.psychiatrist.com/news/how-young-is-too-young-for-a-smartphone/>

tôt que sur la certitude absolue ; or, selon eux, les données présentées ici sont trop alarmantes pour être ignorées³².

Face à ces constats alarmants, l'OKAJU a encore cette année affirmé son engagement à garantir une protection renforcée des mineurs en ligne, s'inscrivant dans la continuité de son rapport annuel de 2024.

Ce chapitre retrace l'évolution récente de la protection des enfants dans l'environnement numérique, aussi bien sur le plan législatif qu'institutionnel, et s'inscrit comme le suivi de la réflexion menée dans le chapitre dédié du rapport 2024. Il analyse les avancées publiques et les pratiques émergentes, détaille la mobilisation croissante des institutions, et propose une vision ambitieuse d'une protection actualisée et effective pour tous les enfants en environnement numérique.

a) Perspective du Comité des droits de l'enfant sur l'environnement numérique

L'Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique du Comité des droits de l'enfant³³ constitue une interprétation approfondie de la Convention relative aux droits de l'enfant (CRDE). Elle insiste sur la nécessité de protéger les enfants contre les risques en ligne tels que l'exploitation, le harcèlement, l'abus, la collecte excessive de données et l'exposition à des contenus inappropriés. Elle invite les États parties à la CRDE et les entreprises à adapter les environnements numériques aux besoins des enfants, à prévenir les dangers spécifiques et à garantir leur vie privée et leur sécurité en ligne, tout en assurant leur accès à l'éducation et à l'information.

L'Observation générale indique notamment : « Les États parties devraient veiller à ce que des mécanismes efficaces de protection des enfants en ligne et des garde-fous soient mis en place, tout en respectant les autres droits de l'enfant, dans tous les lieux où les enfants ont accès à l'environnement numérique, à savoir le domicile, les établissements d'enseignement, les cybercafés, les centres de jeunesse, les bibliothèques, les établissements de santé et les institutions de protection de remplacement ».

b) Engagements nationaux et européens pour la protection des enfants en environnement numérique

Engagements nationaux

Dans l'Accord de coalition 2023-2028, le Gouvernement luxembourgeois « s'engage ... à faire de l'Internet un espace sécurisé, mettant particulièrement l'accent sur la protection des enfants et des adolescents. À l'échelle européenne et internationale, le Gouvernement contribuera à l'élaboration de mesures concrètes et à soutenir la coopération entre les pays dans la lutte contre ces contenus erronés, illégaux ou dangereux qu'offrent actuellement BEE Secure Helpline et Stopline seront renforcés »³⁴.

Dans son discours sur l'**Etat de la Nation le 13 mai 2025**, le Premier Ministre du Luxembourg Luc Frieden a souligné le droit fondamental de tout enfant d'être protégé de contenus de plus en plus violents et sexualisés, en particulier sur Internet³⁵ :

32 <https://www.psychiatrist.com/news/how-young-is-too-young-for-a-smartphone/>

33 <https://docs.un.org/fr/CRC/C/GC/25>

34 <https://gouvernement.lu/dam-assets/documents/dossier/formation-gouvernement-2023/accord-coalition.pdf>

35 https://gouvernement.lu/fr/actualites/toutes_actualites/discours/2025/05-mai/13-frieden-etat-nation.html

« L'internet est le plus vaste réservoir de savoir de toute l'histoire de l'humanité. Ce qui dépassait autrefois les capacités des plus grandes bibliothèques tient aujourd'hui dans une poche, grâce à un simple smartphone. **Malgré l'enthousiasme que suscitent ces nouvelles possibilités, nous devons aussi apprendre à les utiliser de manière responsable.** Le téléphone remplace déjà bien trop souvent un rendez-vous, l'écran un livre et le casque une vraie conversation. Il nous revient à tous de veiller à ce que l'univers numérique ne prenne pas le pas sur la vie réelle, et que l'intelligence artificielle ne se substitue jamais à l'intelligence humaine.

C'est pourquoi nous devons en priorité agir auprès de nos enfants. Cette nouvelle génération grandit avec l'internet et les smartphones ; elle ne connaît pas de monde sans outils numériques ni réseaux sociaux. Les conséquences de cette évolution se font déjà sentir :

Des troubles du comportement de plus en plus marqués, des perturbations du sommeil, de l'anxiété, voire des états dépressifs. Et dès le plus jeune âge, des écarts notables dans le développement social et cognitif.

Le rapport de l'Ombudsman fir Kanner a Jugendlecher est alarmant. Les enfants passent non seulement de plus en plus de temps derrière les écrans, mais ils sont aussi exposés à des contenus de plus en plus violents et sexualisés, en particulier sur les réseaux sociaux.

C'est précisément de ces contenus que nous devons protéger les enfants. Il s'agit d'un droit fondamental de tout enfant ! Nous devons nous attaquer à la racine du problème au niveau européen, à l'image de ce que nous avons accompli avec le Digital Services Act. »³⁶

Engagements européens

Dans son discours de 2025 sur l'état de l'Union³⁷, la présidente de la Commission européenne Ursula von der Leyen a affirmé qu'elle « partage l'anxiété des parents qui font de leur mieux pour protéger leurs enfants...Le harcèlement en ligne. Les contenus pour adultes. La promotion de l'automutilation. Et les algorithmes qui profitent des vulnérabilités des enfants dans le but manifeste de créer des addictions. Trop souvent, des pères et des mères se sentent impuissants et désarmés. Ils ont le sentiment de se noyer face au raz-de-marée des grandes entreprises technologiques qui engloutit leur foyer. Je crois fermement que c'est aux parents, et non aux algorithmes, d'élever nos enfants. Leur voix doit être entendue. Je suis donc ici aujourd'hui pour vous dire que je suis à l'écoute. De même qu'à mon époque, nous avons – en tant que société – appris à nos enfants qu'ils ne pouvaient pas fumer, boire et regarder des contenus pour adultes avant un certain âge, je pense que le temps est venu d'envisager de faire de même pour les médias sociaux... Car lorsqu'il s'agit de la sécurité des enfants en ligne, l'Europe donne la priorité aux parents, et non aux profits ».

Le mois d'octobre 2025 a marqué des avancées au niveau européens³⁸. Lors d'une réunion des ministres européens des télécommunications accueillie à Horsens sous présidence danoise, la Commission européenne a annoncé de nouvelles demandes d'information visant les plateformes, alors que la question de l'interdiction des réseaux sociaux aux mineurs figurait à l'ordre du jour. Plusieurs États membres, dont le Danemark qui assure la présidence tournante de l'UE, se sont prononcés en faveur d'une telle interdiction ; le Danemark a d'ailleurs annoncé vouloir bannir l'accès à plusieurs réseaux sociaux pour les enfants et les jeunes de moins de 15 ans. Sous l'impulsion du pays nordique, 25 ministres des États membres de l'UE, ainsi que ceux de la Norvège et de l'Islande, ont signé une déclaration commune exigeant un renforcement supplémentaire de la protection des mineurs en ligne, notamment à travers la mise en place de dispositifs de vérification d'âge. La déclaration affirme notamment : « Nous devons approfondir notre compréhension des conséquences de l'environnement numérique sur la santé des enfants. Il est impératif de ne pas laisser la décision des limites d'âge aux seuls réseaux sociaux. »

³⁶ https://gouvernement.lu/fr/actualites/toutes_actualites/discours/2025/05-mai/13-frieden-etat-nation.html

³⁷ https://france.representation.ec.europa.eu/informations/discours-sur-le-tat-de-lunion-2025-de-la-presidente-von-der-leyen-2025-09-10_fr

³⁸ <https://infos rtl.lu/lifestyle/techworld/a/2345074.html>

Ils apportent également leur soutien à l'initiative de la présidente de la Commission européenne, Ursula von der Leyen, en faveur de la définition d'un âge de majorité numérique à l'échelle de l'UE et à la consultation d'un panel d'experts, chargé de formuler des recommandations d'ici la fin de l'année.

c) La voix des enfants sur l'environnement numérique

Concernant leur navigation sur internet, les adolescents et les jeunes adultes du Luxembourg affichent une prise de conscience quant à la nécessité d'une meilleure protection lors de leur navigation sur Internet. En effet, 69 % des adolescents et 88 % des jeunes adultes se disent en accord avec un système de vérification de l'âge sur les plateformes³⁹.

Trois témoignages d'enfants recueillis par l'OKAJU pour les besoins du présent rapport annuel illustrent la réalité des violences numériques et rappellent l'urgence accrue d'une action coordonnée : prévention, éducation, adaptation du cadre légal et implication des enfants dans la conception des solutions.

“

“My story is that I do not feel safe on the internet on online games such as Roblox because there are kidnappers who are telling you that they are kids but they are grown ups. Or like social medias like TIK TOK and Youtube. They are 14 plus but people do not care about the age limit and just watch things on it that are inappropriate and super violent and scary. Or like Fortnite which is thirteen plus and people still play it at 8 years old. and it is super violent, the game is online so you can communicate with strangers that trick you into becoming friends with them and later meet them and they turn out to be a grown up.”

“C'est dangereux d'envoyer des photos à des personnes. Il faut tout de suite dire si on voit des photos de personnes nues”.

“On the internet, you should be careful because there are dangerous things like Youtube and Tik tok that are not appropriate for kids.”

Témoignages issus de l'appel à témoignages de l'OKAJU, 2025

”

d) La voix des parents sur la protection des enfants en environnement numérique

L'étude « *Parents Talk Online Safety* » par l'organisation « *More in Common* » menée auprès de près de 10 000 parents aux États-Unis, au Royaume-Uni, en France, en Pologne et aux Pays-Bas⁴⁰, démontre que les préoccupations relatives à la protection des enfants dans l'environnement numérique sont universelles. Les parents ont exprimé une forte inquiétude concernant la sécurité en ligne de leurs enfants, notamment en ce qui concerne les contenus inappropriés, le harcèlement et le temps passé sur les écrans. Le panorama découlant de l'étude met en lumière l'importance de l'accompagnement des familles, une attente accrue vis-à-vis des institutions et le besoin de solutions concrètes adaptées à chaque réalité nationale.

Exemples de préoccupations par pays :

- ↗ Aux États-Unis, une majorité de parents estime que les risques en ligne pour leurs enfants sont inacceptables et cite l'absence de régulation adaptée comme principale source de frustration.
- ↗ Au Royaume-Uni, le harcèlement en ligne et la cyberintimidation sont cités comme les

39 <https://lequotidien.lu/a-la-une/ecrans-et-numerique%20%89-toujours-aussi-precoce-et-chronophage/>

40 <https://www.moreincommon.com/parents-talk-online-safety/>

menaces principales, avec une priorité forte donnée à la mise en place d'outils de contrôle parental et à une meilleure éducation numérique.

- ↗ En France, les parents rapportent un sentiment d'impuissance face à la technologie et demandent davantage d'interventions de la part des écoles et du gouvernement pour éduquer les enfants à l'usage des réseaux sociaux.

Statistiques et ressentis

- ↗ Plus de 80% des parents interrogés dans tous les pays évoquent des craintes sur l'accès de leur enfant à des contenus inadaptés, et près de 70 % expriment des frustrations face au manque d'engagement des géants de la technologie.
- ↗ En France, près de 9 parents sur 10 sont très préoccupés par la sécurité de leurs enfants sur Internet ; 3 parents sur 10 affirment que fixer des limites à la connexion Internet entraîne des conflits avec leurs enfants ; 2 parents sur 5 (38 %) déclarent ne pas recevoir assez d'aide pour assurer la sécurité de leurs enfants en ligne.
- ↗ Les parents polonais sont particulièrement inquiets des jeux en ligne et du rapport avec les étrangers sur Internet, alors que ceux des Pays-Bas mentionnent la problématique de la vie privée et la question du partage de données personnelles des enfants.

Exemples concrets de propos de parents

- ↗ Un parent anglais partage : « Les réseaux sociaux sont partout et j'ai l'impression de courir derrière la technologie pour protéger mes enfants. »
- ↗ En France, un parent affirme : « A l'heure actuelle, je ne compte sur personne – l'Etat ne fera rien, et les plateformes non plus vu qu'il y a tant d'argent en jeu – on peut compter que sur soi-même. »
- ↗ Aux États-Unis, un père souligne : « Les politiques et les entreprises ne font rien, c'est nous qui devons gérer tout seuls. »

e) Vers une meilleure protection des enfants face aux risques numériques au Luxembourg

A la suite de sa recommandation générale concernant l'industrie pornographique au Luxembourg et de son rapport annuel 2024 qui a mis un accent sur la protection des enfants contre les violences et autres préjudices en milieu numérique⁴¹, l'OKAJU a multiplié les échanges avec des acteurs compétents en la matière.

Dialogues institutionnels et contexte européen

Au printemps, des discussions importantes ont eu lieu avec le ministère de l'Economie autour de la protection des mineurs face à l'industrie de la pornographie en ligne.

Un point majeur a porté sur les évolutions attendues au plan européen. La Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie⁴², va connaître une révision. De même, la ePrivacy Directive⁴³, encadrant la protection et la confidentialité des communications électroniques, sera adaptée afin de renforcer la sécurité des mineurs en ligne. Ces refontes législatives devraient apporter des outils concrets et actualisés pour répondre aux nouveaux risques liés au numérique.

⁴¹ Voir chapitre C du rapport annuel 2024 de l'OKAJU, « La protection des enfants contre les violences et autres préjudices en milieu numérique » https://www.okaju.lu/wp-content/uploads/2025/02/RA2024-ONLINE_BAT-250206.pdf

⁴² <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32011L0093>

⁴³ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A32002L0058>

Ce thème a également été abordé lors de la visite du Chef adjoint de la Représentation de la Commission européenne au Luxembourg, Monsieur Dennis Wernerus, en mars. La révision annoncée de la Directive 2011/93/UE sur la lutte contre les abus et l'exploitation sexuelle des enfants, ainsi que de la Directive sur la vie privée électronique (E Privacy Directive), ouvre des perspectives législatives essentielles. Cependant, le Benelux demeure pour l'instant dans une posture plutôt attentiste.

Mobilisation nationale et coordination renforcée

En juin, l'OKAJU a également rencontré les représentants de l'ALIA, l'Association luxembourgeoise indépendante de l'audiovisuel. Face à l'intégration croissante des usages numériques dans la vie quotidienne des enfants, les deux institutions ont réaffirmé leur engagement commun envers une régulation renforcée des contenus accessibles aux mineurs. Elles ont souligné la nécessité d'une coordination étroite entre tous les acteurs concernés afin de clarifier les responsabilités, mobiliser les compétences et agir à l'unisson. Le *Digital Services Act* (DSA)⁴⁴ et l'Acte européen sur l'intelligence artificielle⁴⁵, avec leurs nouvelles exigences en matière de transparence et de protection des publics vulnérables, constituent des leviers importants dans cette démarche.

Initiatives européennes et adaptation luxembourgeoise

Début août, un échange avec l'Autorité de la Concurrence, en tant que *Digital Services Coordinator*, a permis d'identifier deux initiatives européennes majeures : la cartographie des plateformes pornographiques et la mise en place de systèmes robustes de vérification d'âge conformes, au cœur desquels l'identité numérique européenne jouera un rôle central d'ici fin 2026.

Ces collaborations renforcent la volonté affichée au Luxembourg de mutualiser les initiatives (BeeSecure, Police, ALIA, OKAJU, etc.) et d'organiser des espaces d'échanges comme des Assises en ligne, ou des forums annuels dédiés. La coalition gouvernementale a d'ailleurs annoncé l'ouverture d'un débat public sur la protection accrue des jeunes dans la société numérique.

Au regard de son rôle de promotion, sauvegarde et protection des droits de l'enfant, l'Autorité de la concurrence considère l'OKAJU comme un partenaire privilégié pour une mise en œuvre efficace du DSA au niveau national.

En perspective, le suivi attentif des lignes directrices européennes, constitue une étape stratégique pour la mise en œuvre d'une protection renforcée des mineurs sur le plan national. Parmi les pistes d'action, l'organisation de temps d'échanges thématiques (journées d'information, tables rondes, forum annuel sur la protection en ligne) et la coordination interinstitutionnelle apparaissent comme essentielles pour la mobilisation des acteurs et le partage des innovations. Approfondir les discussions sur la vérification d'âge et le rôle des signalements certifiés est également prioritaire.

f) Digital Services Act (DSA) et lignes directrices : un nouveau cadre pour la protection des enfants en Europe

Le DSA est entré pleinement en vigueur le 17 février 2024 pour tous les acteurs numériques dans l'Union européenne, tandis que les très grandes plateformes et moteurs de recherche étaient déjà soumis à ses obligations depuis le 25 août 2023. L'article 28 porte sur la protection des mineurs en ligne, imposant aux plateformes en ligne accessibles aux mineurs des obligations spécifiques pour protéger les mineurs qui utilisent leurs services. Concrètement, il leur demande de mettre en place des mesures appropriées et proportionnées qui garantissent un niveau élevé de protec-

⁴⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng?eliuri=eli%3Areg%3A2022%3A2065%3Aojo&locale=fr>

⁴⁵ Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) <https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=fr>

tion de la vie privée, de la sécurité et de la sûreté des mineurs. Cela signifie que les plateformes doivent évaluer les risques que la conception et les caractéristiques de leurs services posent aux enfants et prendre des mesures adaptées pour réduire ces risques. L'article 28 a la teneur suivante :

Article 28 du Digital Services Act

« Protection des mineurs en ligne

1. *Les fournisseurs de plateformes en ligne accessibles aux mineurs mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service.*
2. *Les fournisseurs de plateformes en ligne ne présentent pas sur leur interface de publicité qui repose sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679 en utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils ont connaissance avec une certitude raisonnable que le destinataire du service est un mineur.*
3. *Le respect des obligations énoncées dans le présent article n'impose pas aux fournisseurs de plateformes en ligne de traiter des données à caractère personnel supplémentaires afin de déterminer si le destinataire du service est un mineur.*
4. *La Commission, après avoir consulté le comité, peut publier des lignes directrices pour aider les fournisseurs de plateformes en ligne à appliquer le paragraphe 1 »⁴⁶*

Les manquements au DSA peuvent valoir aux plateformes des amendes pesant jusqu'à 6% de leur chiffre d'affaires annuel mondial. La Commission européenne a déjà ouvert de nombreuses enquêtes dans le cadre du DSA, ciblant les plateformes de Meta, Facebook et Instagram, mais aussi TikTok, X, et le site chinois AliExpress.⁴⁷

Contribution de l'OKAJU à la Consultation européenne sur la protection des enfants en environnement numérique

L'OKAJU a participé à la consultation de la Commission européenne « *Consultation publique ciblée sur les lignes directrices relatives à la protection des mineurs conformément à l'article 28 de la législation sur les services numériques (Digital Services Act)* ». La consultation comportait les sections suivantes : revue des risques, assurance de l'âge, paramètres de compte, conception de l'interface, systèmes de recommandation, pratiques commerciales, modération, outils pour les tuteurs, gouvernance, suivi et évaluation.

L'OKAJU a appelé à une protection en ligne centrée sur les droits de l'enfant, exigeant une régulation beaucoup plus stricte et des mesures efficaces contre l'exposition aux contenus dangereux, le profilage et la collecte excessive de données. Il insiste sur le respect des capacités évolutives et de l'autonomie des jeunes, la nécessité d'un contrôle de l'âge respectueux de la vie privée, une transparence accrue des paramètres et de la modération, et une réelle participation des enfants dans la conception des outils et la gouvernance du numérique. L'État et les plateformes doivent coordonner leurs efforts pour garantir un environnement numérique qui place l'intérêt supérieur de l'enfant au premier plan et repose sur la prévention, la responsabilité et des évaluations régulières.

Dans le cadre de la consultation, l'OKAJU a recommandé, entre autres, d'intégrer les principes

46 <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022R2065>

47 <https://infos rtl.lu/lifestyle/techworld/a/2345074.html>

de la CRDE dans le numérique, de réaliser des évaluations d'impact sur leurs droits et d'associer systématiquement les enfants à l'élaboration des politiques.

L'OKAJU a également relevé certains défis dans ses observations concernant les lignes directrices sur la protection des mineurs dans le cadre du DSA, et notamment son article 28 :

- ↗ Absence de force contraignante (*soft law*).
- ↗ Manque de normes de conception adaptées à l'âge.
- ↗ Faible prise en compte de la diversité des enfants.
- ↗ Risques systémiques liés aux logiques économiques des plateformes.

Publication de lignes directrices européennes sur la protection des mineurs : un nouveau cadre pour la régulation

Depuis juillet 2025, les lignes directrices européennes sur la protection des mineurs en ligne dans le cadre du DSA encadrent la protection des mineurs dans l'environnement numérique avec un niveau d'exigence renforcé. Ces lignes directrices ont été élaborées à la suite d'une large consultation publique avec les parties prenantes, qui s'est clôturée en juin 2025. Reposant sur une méthodologie fondée sur les risques, les lignes directrices mettent l'accent sur la sécurité, la protection de la vie privée dès la conception et le respect des droits de l'enfant, tout en soulignant que les plateformes doivent éviter toute restriction disproportionnée de ces droits. Elles constituent le nouveau cadre de référence pour les plateformes et les autorités nationales, y compris au Luxembourg, permettant d'évaluer la conformité des plateformes et orienter les autorités nationales luxembourgeoises dans la régulation et la coordination.

Objectif des lignes directrices

Les lignes directrices visent essentiellement à offrir aux plateformes numériques un ensemble de repères structurés leur permettant de respecter l'article 28 du DSA. Elles exigent que les fournisseurs de services mettent en place des mesures adaptées et proportionnées assurant un degré élevé de confidentialité, de protection et de sécurité pour les utilisateurs mineurs. À travers des règles pratiques, ces directives traduisent l'obligation légale en recommandations concrètes, facilitant ainsi la mise en œuvre par les plateformes et une conformité harmonisée à l'échelle européenne.

Applicabilité et recommandations principales

Les lignes directrices s'appliquent à toutes les plateformes en ligne accessibles aux mineurs, à l'exception des micros et petites entreprises. Les principales recommandations sont les suivantes :

- ↗ **Définir les comptes des mineurs en privé par défaut** afin que leurs informations personnelles, leurs données et leur contenu sur les médias sociaux soient cachés à ceux avec lesquels ils ne sont pas connectés pour réduire le risque de contact non sollicité par des étrangers.
- ↗ **Modifier les systèmes de recommandation des plateformes** afin de réduire le risque que les enfants soient confrontés à des contenus préjudiciables ou restent coincés dans des trous de lapin de contenus spécifiques, notamment en conseillant aux plateformes de donner la priorité aux signaux explicites des enfants par rapport aux signaux comportementaux et en donnant aux enfants les moyens de mieux contrôler leurs aliments pour animaux.
- ↗ **Donner aux enfants les moyens de bloquer et d'étouffer tout utilisateur** et s'assurer qu'ils ne peuvent pas être ajoutés à des groupes sans leur consentement explicite, ce qui

pourrait aider à prévenir la cyberintimidation.

- ↗ *Interdire aux comptes de télécharger ou de prendre des captures d'écran de contenus postés par des mineurs afin d'empêcher la diffusion non désirée de contenus sexualisés ou intimes et l'extorsion sexuelle.*
- ↗ *Désactiver par défaut les fonctionnalités qui contribuent à une utilisation excessive, telles que les « traces » de communication, le contenu éphémère, les « reçus de lecture », la lecture automatique ou les notifications push, ainsi que supprimer les fonctionnalités de conception convaincantes visant principalement à l'engagement et à mettre en place des garanties autour des chatbots d'IA intégrés dans les plateformes en ligne.*
- ↗ *Veiller à ce que le manque d'éducation commerciale des enfants ne soit pas exploité et à ce qu'ils ne soient pas exposés à des pratiques commerciales qui peuvent être manipulatrices, entraîner des dépenses non désirées ou des comportements addictifs, y compris certaines monnaies virtuelles ou boîtes à butin.*
- ↗ *Introduire des mesures visant à améliorer les outils de modération et de compte rendu, nécessitant un retour d'information rapide, et des exigences minimales pour les outils de contrôle parental »⁴⁸.*

Les lignes directrices préconisent l'usage de méthodes efficaces d'assurance de l'âge à condition qu'elles soient fiables, précises, non intrusives et non discriminatoires. Elles encouragent le recours à la vérification de l'âge pour limiter l'accès aux contenus pour adultes (pornographie, jeux de hasard) ou aux services soumis à des règles nationales d'âge minimal, notamment certaines plateformes de médias sociaux. En attendant la disponibilité de portefeuilles d'identité numérique européens, un prototype d'application pour la vérification de l'âge, offre d'ores et déjà une référence de conformité et un standard technique pour une vérification de l'âge basée sur les dispositifs.

Les lignes directrices proposent aussi une estimation de l'âge dans les cas où des services établissent un âge minimal inférieur à 18 ans en fonction des risques pour les mineurs.

Limites des lignes directrices européennes sur la protection des mineurs – réflexions de l'OKAJU

Malgré l'ambition du nouveau cadre, l'application des lignes directrices européennes demeure volontaire et relève du principe du « soft law » : elles n'ont pas de valeur juridiquement contraignante et ne font pas l'objet de contrôles systématiques. Ce caractère non obligatoire expose à des disparités dans l'implémentation entre plateformes et États membres, et limite la portée réelle des protections prévues pour les enfants.

Le contrôle de l'âge, pourtant central dans la prévention des risques d'exposition à des contenus inadaptés, reste morcelé. Faute de standardisation technique à l'échelle européenne, les systèmes en place varient selon les plateformes, ne garantissent pas toujours la fiabilité ni la confidentialité des données, et demeurent facilement contournables pour des mineurs avertis. La promesse d'un portefeuille d'identité numérique européen offre une piste, mais sa mise en œuvre n'est pas immédiate.

De plus, les lignes directrices ne s'attaquent pas assez aux logiques économiques des plateformes qui favorisent l'engagement et l'exposition à des risques systémiques (publicités, profilage, pratiques commerciales manipulatrices). Leur efficacité dépend largement de la volonté politique et de la capacité des États à harmoniser les pratiques, actualiser les exigences et assurer un suivi régulier. Sans une pression accrue et des garanties juridiques, les protections resteront fragmen-

48 <https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-guidelines-protection-minors>

taires, difficilement évaluables et insuffisantes face à l'ingéniosité des acteurs du numérique et à l'évolution rapide des risques pour les enfants.

g) Contribution de l'OKAJU au projet de recommandation du Conseil de l'Europe sur la sécurité en ligne

L'OKAJU a répondu à un appel du Comité du Conseil de l'Europe sur la sécurité en ligne et la responsabilisation des créateurs de contenus et des utilisateurs. L'appel avait pour objectif d'appuyer la rédaction du projet de recommandation sur la sécurité en ligne et l'autonomisation des créateurs de contenu et des utilisateurs⁴⁹. Dans ce contexte, l'OKAJU a formulé les remarques suivantes :

Dans son rapport annuel 2024, l'OKAJU a mis en lumière les nouveaux défis auxquels sont confrontés les enfants dans l'environnement numérique, où les risques sont multiples et en constante évolution. L'OKAJU souligne que les enfants et adolescents sont particulièrement vulnérables face à des formes de violence telles que :

- ↗ **Le cyberharcèlement** : comportements agressifs, intimidations et humiliations répétées via les réseaux sociaux, messageries, plateformes en ligne.
- ↗ **La sextorsion** : chantage sexuel en ligne où les jeunes sont contraints de fournir des images ou des informations intimes sous la menace.
- ↗ **Les sollicitations malveillantes et l'exploitation** : contacts non désirés avec des prédateurs, tentatives de manipulation ou d'exploitation sexuelle via internet.

Face à ces menaces, l'OKAJU insiste sur la nécessité d'une **approche globale et coordonnée** qui implique :

- ↗ **La prévention à l'échelle de la société**, notamment par l'éducation des enfants, des parents et des professionnels sur les risques numériques et les bonnes pratiques.
- ↗ **Le renforcement des dispositifs de détection et d'intervention rapide** pour protéger les victimes et sanctionner les auteurs.
- ↗ **Le développement de collaborations entre acteurs publics, associations, écoles, et familles** pour une réponse efficace.
- ↗ **L'intégration d'une perspective de santé publique** qui considère l'impact psychologique et social des violences numériques sur les enfants.

Enfin, l'OKAJU appelle à une mise à jour régulière des politiques publiques et des outils légaux pour suivre l'évolution rapide du numérique, en veillant toujours à placer l'intérêt supérieur de l'enfant au cœur des actions.

Perspectives et prochaines étapes au Luxembourg

Le Luxembourg, aux côtés de ses partenaires européens, envisage également de contribuer activement aux initiatives communes : réflexion sur des mécanismes de vérification d'âge robustes, rôle et certification des dispositifs de signalement, développement de profils spécialisés pour accompagner la régulation, et renforcement de la coordination interinstitutionnelle (BeeSecure, ALIA, CNPD, Police, OKAJU...).

⁴⁹ <https://rm.coe.int/public-msi-esec-2025-03rev2-draft-cm-recommendation-on-online-safety-a/1680b67ada>

h) Etat des lieux de la réalité numérique des enfants au Luxembourg

Possession de smartphones et autres outils numériques

En 2024, le Service national de la jeunesse (SNJ) a mené une enquête auprès de 916 jeunes et 541 parents d'enfants âgés de 3 à 16 ans⁵⁰. Elle a révélé que 90 % des enfants au Luxembourg sont équipés d'un smartphone à 12 ans et qu'en moyenne, les enfants acquièrent leur premier smartphone à 10,77 ans. Il convient toutefois de noter que dans le cadre du DigiRallye de BEE Secure, destiné aux enfants de 8 à 12 ans, il est ressorti que l'âge moyen d'obtention du premier smartphone était d'environ 9 ans et qu'environ 88 % d'entre eux utilisent déjà un smartphone⁵¹.

Dans le cadre du rapport Bee Secure Radar 2025, il est ressorti que chez les plus jeunes, les tablettes restent plus couramment utilisées que les smartphones. Selon les parents, 40 % des enfants de 3 à 11 ans utilisent un smartphone quotidiennement, tandis que 60 % utilisent régulièrement une tablette⁵².

21 % des parents déclarent que leur enfant a possédé son premier portable avant l'âge de 10 ans, l'âge moyen d'obtention, et ce pourcentage monte même à 49 % pour la première possession d'une tablette⁵³. Un accès au monde numérique si jeune expose les enfants à des risques spécifiques et constitue un véritable défi en matière de protection.

Temps d'écran

Le rapport Radar 2025 démontre que les 12-16 ans interrogés passent, en moyenne, 4 h 08 par jour sur leurs écrans. Les 17-30 ans font même pire, avec 5 h 14. Logiquement, peu d'entre eux disent avoir un usage raisonnable de leur smartphone en n'utilisant qu'une fois par heure leur appareil. Ils sont 11 % dans ce cas chez les 12-16 ans et 12 % chez les 17-30 ans⁵⁴.

Exposition à la pornographie et signalements de matériel d'abus sexuels d'enfants (CSAM)

Il ressort du Radar 2025 une opinion largement partagée, selon laquelle l'utilisation de la pornographie se produit au moins parfois (58 % des 12-17 ans) et qu'une augmentation importante de la fréquence estimée d'utilisation chez les 12 à 17 ans est observée par rapport au Radar 2024.

Les signalements de contenus CSAM à la Stopline de BEE SECURE sont réguliers : « Au cours de l'année scolaire allant du 1er septembre 2023 au 31 août 2024, un total de 5 693 signalements a été enregistré. Parmi ceux-ci, 45,2 % ont été soumis via une base de données internationale nommée ICCAM (réseau INHOPE : International Association of Internet Hotlines),⁵⁵ tandis que 54,8 % des signalements ont été effectués par le biais de la BEE SECURE Stopline »⁵⁶.

50 <https://infos rtl lu/actu/luxembourg/a/2308215.html>

51 https://www.bee-secure.lu/wp-content/uploads/2025/02/166_bee-secure-radar-2025.pdf

52 <https://infos rtl lu/actu/luxembourg/a/2308215.html>

53 <https://lequotidien lu/a-la-une/ecrans-et-numerique%E2%80%89-toujours-aussi-precoce-et-chronophage/>

54 <https://lequotidien lu/a-la-une/ecrans-et-numerique%E2%80%89-toujours-aussi-precoce-et-chronophage/>

55 « Dans le cadre de la classification et du traitement rigoureux des signalements reçus, les experts de la BEE SECURE Stopline ont identifié 1 600 d'entre eux comme potentiellement illégaux, représentant ainsi environ 28,1 % du total. Dans 222 cas (3,9 %), les contenus signalés étaient jugés douteux mais légalement acceptables. Dix signalements (0,2 %) étaient des doublons d'URLs déjà connues. Dans 2 590 cas (45,5 %), les signalements n'ont pas pu faire l'objet d'une analyse car les contenus concernés avaient déjà été retirés par les fournisseurs d'accès à Internet (Internet Service Provider) pour des raisons d'ilégalité. Pour 1 050 (18,4 %) autres URLs, aucun contenu n'a pu être localisé en raison de leur inaccessibilité. Enfin, 178 (3,1 %) signalements ont été classés comme étant hors du champ de compétence, parce qu'ils ne relevaient pas du domaine d'action de la BEE SECURE Stopline » (BEE Secure Radar 2025, p. 49).

56 https://www.bee-secure.lu/wp-content/uploads/2025/02/166_bee-secure-radar-2025.pdf

Rappel de certaines recommandations du rapport annuel 2024 de l'OKAJU concernant la protection des enfants dans l'environnement numérique

- ↗ **Âge légal minimum** : L'OKAJU propose un âge minimum légal de 15 ans pour la possession de tout smartphone ou appareil donnant un accès autonome à Internet et aux réseaux sociaux, sans supervision adulte. Avant cet âge, la supervision effective et le contrôle parental doivent être obligatoires.
- ↗ **Safety by design et alternatives aux smartphones** : L'OKAJU encourage le développement et la mise sur le marché de téléphones restreints « safephones », permettant uniquement la communication et les fonctions basiques (sans navigation Internet, installation d'applications sociales ou accès à des réseaux non sécurisés). Ces dispositifs, conçus pour protéger activement les mineurs en limitant les risques d'exposition aux contenus inadaptés, devraient devenir la norme pour tous les enfants de moins de 15 ans.
- ↗ **Vérification d'âge technique** : L'OKAJU demande que toutes les plateformes et services numériques imposent des systèmes de vérification d'âge robustes et le blocage systématique des contenus sensibles.
- ↗ **Coordination institutionnelle** : La lutte contre la pornographie, le CSAM, le grooming et la sextorsion nécessite une action coordonnée entre l'école, les familles, les autorités de protection et les acteurs de la cybersécurité.

Initiatives prises par le ministère de l'Education, de l'Enfance et de la Jeunesse (MENJE) en 2024/2025

Fin 2024, deux campagnes nationales visant à réduire le temps d'écran, à promouvoir des activités physiques/familiales non numériques et à renforcer la protection des enfants dans l'environnement numérique ont été lancées par le ministère de l'Education, de l'Enfance et de la Jeunesse (MENJE) : Screen-Life-Balance et Sécher.digital.

Screen-Life-Balance

La campagne met l'accent trois phases essentielles de développement des enfants et des jeunes :

- ↗ Éviter les écrans en dessous de 3 ans
- ↗ Éviter le smartphone personnel en dessous de 12 ans
- ↗ Éviter les médias sociaux en dessous de 15 ans⁵⁷

Sécher.digital

La campagne « Sécher.digital » du MENJE offre également des recommandations adaptées en matière du temps d'écran pour chaque tranche d'âge des enfants :

- | | |
|-----------------|---|
| ↗ 0 à 3 ans : | Éviter toute exposition aux écrans |
| ↗ 3 à 6 ans : | Choisir un contenu adapté |
| ↗ 6 à 9 ans : | Accompagner l'usage des outils numériques |
| ↗ 9 à 12 ans : | Éviter le Smartphone |
| ↗ 12 à 15 ans : | Trop tôt pour les réseaux sociaux ! |
| ↗ 15 ans : | Rester vigilant |

Des recommandations supplémentaires sur l'utilisation des écrans en famille ont été présentées

57 https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2024/09-septembre/30-meisch-screen-life-balance.html

par les Eltereform dans la [lettre aux parents « Screen-Life-Balance »](#) : « 7 réflexions sur moins d'écrans, davantage de mouvement, de découvertes et d'expériences »⁵⁸.

Recommandations du MENJE

L'OKAJU salue que le MENJE déconseille depuis fin 2024 l'accès aux réseaux sociaux et l'autonomie numérique avant 15 ans, en cohérence avec l'âge recommandé par l'OKAJU en la matière. Cependant, il déconseille seulement la possession de smartphones avant 12 ans—une recommandation bien moins ambitieuse que celle de l'OKAJU (15 ans).

Restrictions dans les écoles

L'OKAJU salue les restrictions imposées dans les écoles :

- ↗ Smartphones interdits dans les écoles fondamentales et maisons relais dès avril/juin 2025, séparation physique obligatoire entre élèves et leurs smartphones pendant les cours ;
- ↗ Dans les lycées, l'accès au réseau Wi-Fi pédagogique (eduroam) est réservé aux élèves âgés de 15 ans ou plus, c.à.d. l'accès dans l'enceinte de l'école ne sera possible que pour les élèves ayant atteint la maturité digitale⁵⁹.

L'OKAJU observe néanmoins qu'au moins une école publique internationale poursuit l'utilisation d'iPads connectés dès le cycle fondamental en classe, exposant les enfants très jeunes au numérique. Plus préoccupant encore, le MENJE continue de doter les élèves de cette école d'iPads individuels dès l'entrée au lycée, c'est-à-dire dès l'âge de 11 ans, avec un accès à YouTube.

Un cadre légal à renforcer pour répondre aux vulnérabilités réelles

L'écart persiste entre la législation souhaitée et la réalité du terrain, où les enfants s'exposent aux écrans et aux contenus sexuels dès le primaire. L'OKAJU appelle à une mobilisation collective : légalité, technique, supervision adulte et prévention, associées à des solutions innovantes (*safety by design*, « safephones », filtres, sensibilisation, etc.).

La politique publique au Luxembourg évolue vers un accès encadré et progressif au numérique, mais pour l'OKAJU, l'urgence demeure d'aligner le cadre législatif à la réalité de la situation des enfants, afin de protéger effectivement les enfants des dangers de l'environnement numérique. Il convient, entre autres, de :

- ↗ Fixer un âge minimum légal à 15 ans pour la possession de tout smartphone ou appareil donnant un accès autonome à Internet et aux réseaux sociaux, sans supervision adulte. Avant cet âge, la supervision effective et le contrôle parental doivent être obligatoires
- ↗ Développer des alternatives sûres aux smartphones classiques, tout en imposant une supervision et un contrôle strict de l'exposition.

⁵⁸ https://elteforum.lu/wp-content/uploads/2025/04/Elterebrief_Activity-Box_FR.pdf

⁵⁹ <https://men.public.lu/dam-assets/catalogue-publications/dossiers-de-presse/2024-2025/dossier-presse-smartphone-exclusives.pdf>

Le tableau comparatif suivant rassemble les recommandations de l'OKAJU, les données du BEE SECURE Radar 2025 et les mesures et recommandations du MENJE concernant l'âge d'accès aux outils numériques et la réalité de l'usage des écrans au Luxembourg :

Critère	OKAJU (2024) – Recommandations du rapport annuel	BEE SECURE Radar 2025 – Réalité luxembourgeoise	MENJE – Campagnes & mesures 2024/2025
Âge de première exposition aux écrans	Introduction d'un âge minimum légal de 3 ans pour l'exposition aux écrans	Pas d'écran avant 3 ans	Eviter les écrans avant 3 ans
Âge minimum pour smartphone	Introduction d'un âge minimum légal de 15 ans pour la possession de smartphones	Âge moyen d'obtention : 10,76 ans ; 90% des enfants ont un smartphone à 12 ans	Éviter l'attribution d'un smartphone personnel avant 12 ans
Accès autonome à Internet/Réseaux sociaux	Introduction d'un âge minimum légal de 15 ans pour la possession de tout smartphone ou appareil donnant un accès autonome à Internet et aux réseaux sociaux, sans supervision adulte. Avant cet âge, la supervision effective et les contrôles parentaux doivent être obligatoires. Introduction d'un système de vérification de l'âge	88% des enfants (8-12 ans) utilisent déjà un smartphone ; Selon le BEE SECURE Radar 2025, âge moyen d'ouverture du premier compte sur un réseau social se situe autour de 12 ans	Accès aux réseaux sociaux déconseillé avant 15 ans ; Wi-Fi scolaire réservé dès 15 ans au lycée, mais mesure non harmonisée ; pas d'internet seul avant 12 ans
Contrôle parental, supervision, alternatives technologiques	Contrôles parentaux techniques obligatoires ; promotion de « safephones » (safety by design) avant 15 ans	Souvent partiel ou absents, usage libre majoritaire ; alternatives peu diffusées	Information, sensibilisation, incitation à usages alternatifs et à l'équilibre screen-life-balance
Temps d'écran quotidien (12-16 ans)	Encadrement parental souhaité et limitation stricte ; prévention des abus d'usage	32% passent >4h/jour sur smartphone, 54% se disent « accros » ou en situation d'abus	Activités non numériques promues, recommandations selon l'âge (3-6-9-12-15 ans)

Des recommandations du ministère de la Santé et de la Sécurité sociale sur l'usage des écrans et la prévention chez les enfants ont également été rendues publiques le 19 novembre 2024, lors de la publication du dossier « Bon usage des écrans » sur le Portail Santé du Luxembourg⁶⁰. L'OKAJU déplore qu'elles préconisent que les enfants peuvent « surfer » seuls après l'âge de 12 ans et que « les tablettes tactiles peuvent être utilisées de façon ludique au même titre que tous les jouets traditionnels, mais pas avant l'âge de 2 ans et jamais plus que 10 à 15 minutes par jour ».

Du point de vue de l'OKAJU, et notamment de la perspective des droits de l'enfant à la protection et à la santé, l'approche consistant à instaurer un seuil légal et technique strict à 15 ans pour l'autonomie numérique, l'accès aux réseaux sociaux et la possession autonome d'un smartphone représente le standard le plus protecteur face aux risques du numérique. La supervision parentale systématique et l'incitation à l'usage de dispositifs conçus pour la sécurité des enfants renforcent cette protection, en anticipant les dangers d'une exposition précoce et en favorisant le développement d'une maturité digitale adaptée à l'âge.

60 <https://santesecu.public.lu/fr/espace-citoyen/dossiers-thematiques/p/petite-enfance/danger-des-ecrans1.html>

L'analyse du tableau comparatif met en évidence que, malgré les recommandations du MENJE d'éviter le smartphone avant 12 ans et de réserver l'accès autonome aux réseaux sociaux à 15 ans, la réalité observée demeure préoccupante : les enfants luxembourgeois sont majoritairement équipés d'un smartphone avant 12 ans et accèdent à Internet sans supervision, alors même qu'ils ne disposent pas encore de l'autonomie et du discernement requis. Ceci tend à confirmer la pertinence et la nécessité de l'approche défendue par l'OKAJU, qui se distingue par sa cohérence et sa capacité à répondre pleinement aux enjeux de protection et de prévention propres à l'enfance, invitant à une mobilisation plus collective et réglementaire de la société luxembourgeoise.

Il est pertinent de rappeler qu'une véritable protection des enfants dans l'environnement numérique nécessite une démarche interministérielle et intersectorielle. Les discussions récentes entre l'OKAJU, l'ALIA et d'autres institutions nationales confirment l'importance d'une concertation plus étroite entre les différents ministères concernés (Justice, Digitalisation, Famille, Santé, Affaires étrangères, etc.), ainsi qu'avec des acteurs tels que l'ALIA, le Digital Services Coordinator auprès de l'Autorité de la Concurrence. Cela permettrait d'éviter des approches en silos et d'assurer une stratégie cohérente sur l'ensemble des aspects de la protection numérique des enfants.



ANNEXE

Extraits du rapport annuel 2024 de l'OKAJU, chapitre C : « La protection des enfants contre les violences et autres préjudices en milieu numérique »

Facilité d'accès à la pornographie

Les enfants et les adolescents peuvent avoir accès à des contenus pornographiques en quelques clics, de manière accidentelle ou involontaire, de manière volontaire ou par l'influence de pairs, de mineurs d'âge plus âgés, voire de cybergroomers. Selon le rapport BEE SECURE Radar (2024), environ un tiers (31%) des adolescents au Luxembourg sont au moins « parfois » exposés à des contenus pornographiques. Pour les 17-30 ans, ce chiffre monte à 81%, avec plus d'un tiers (36%) y étant exposés « très fréquemment ». Toujours selon le Radar de BEE SECURE (2024) :

- ↗ 37% des 12-16 ans citent les contenus sexuels comme risque majeur
- ↗ 31% des 12-16 ans estiment que leurs pairs sont parfois exposés à la pornographie
- ↗ Un tiers des parents d'enfants de 12 à 16 ans pensent que leur enfant y a été exposé.

Âge et prévalence de l'exposition à la pornographie en ligne

La recherche montre que l'âge de la première exposition à la pornographie est en constante diminution. Concernant l'âge de première exposition à la pornographie, les résultats sont contradictoires avec des variations allant de 10 à 17 ans (Habidin et al. 2016). Cependant, la plupart des garçons recherchent activement de la pornographie dès l'âge de 10 ans (Watts 2020). La prévalence de l'exposition à la pornographie en ligne, particulièrement aux contenus violents ou abusifs (UNICEF 2019), est particulièrement élevée chez les adolescents masculins (UNODC, 2015) et les garçons plus âgés sont plus susceptibles d'être exposés à des images sexuelles en ligne que les enfants plus jeunes et les filles (Flood 2009 ; Quadara et al. 2017 ; Smahel et al. 2020). De plus, la consommation de pornographie devient plus fréquente et régulière à mesure que les jeunes grandissent (Brown et L'Engle 2009 ; Horvath et al. 2013 ; eChildhood 2021).

Nature des contenus : pornographie violente et CSAM

L'analyse de 400 vidéos pornographiques provenant des quatre sites web pornographiques les plus visités par Klaassen et Peter (2015) a révélé que les femmes étaient plus susceptibles d'être représentées comme soumises et les hommes comme dominants. Jusqu'à 88% de la pornographie populaire sur Internet comporte des actes de violence physique (Bridges et al. 2010 ; Owens et al. 2012 ; Stanley et al. 2016 ; Sun et al. 2016 ; Donevan et Mattebo 2017 ; Foubert 2017), auxquels les femmes représentées réagissent souvent de manière positive (Purcell 2012).

Les deux dernières décennies ont été caractérisées par des préoccupations croissantes concernant la prolifération de CSAM sur Internet (Quayle et Taylor 2006 ; Quayle et Newman 2015), y compris via des sites Internet de contenus pornographiques comme Pornhub, alors que le CSAM dépeint des enfants toujours plus jeunes, des abus toujours plus violents et des contextes plus domestiques (Griffiths 2005). De plus, les adolescents sont de plus en plus condamnés en justice pour la possession de CSAM (SFIS 2009 ; Finkelhor et Ormrod 2010 ; Mitchell et al. 2011 ; Aebi et al. 2014).

Impacts néfastes de l'exposition à la pornographie et au CSAM

Les impacts neurologiques^[52] et comportementaux^[53], ainsi que les risques d'addiction à la pornographie et au CSAM sont bien documentés.

Normalisation de la violence sexuelle et émergence d'une culture de l'abus

L'exposition aux contenus sexuellement explicites contribue à créer une « culture de l'abus » qui normalise la violence sexuelle (Baxter 2014) et génère des « normes sociales favorables à la violence encourageant la participation aux abus sexuels » (Flood 2009, p. 384). Cette culture se manifeste notamment par une plus grande tolérance et une moindre désapprobation des relations sexuelles non consenties, auxquelles l'exposition à la pornographie contribue directement (Bonino et al. 2006 ; Horvath et al. 2013). L'omniprésence de contenus sexuellement explicites dans la vie des mineurs contribue à la normalisation d'actes sexuels caractérisés par le sexismme, l'inégalité, la violence et la dégradation (Walker 2017).

Lien entre l'exposition à la pornographie et au CSAM et l'augmentation des violences sexuelles entre mineurs

Des niveaux croissants de violence sexuelle parmi les mineurs ont été révélés par des études de prévalence de l'expérience des enfants en matière de violence sexuelle en Europe et au Royaume-Uni (Barter et al. 2009 ; Radford et al. 2011 ; Nelson 2016). Les statistiques sont alarmantes. En France, le nombre de jeunes de moins de 18 ans parmi les auteurs d'infractions sexuelles a augmenté de 70% entre 1996 et 2003 (Rabaux 2007). Un rapport du Sénat publié en 2022 note une augmentation de 59,7% des violences sexuelles commises par des mineurs sur d'autres mineurs entre 2016 et 2021. L'Observatoire national de la délinquance et des réponses pénales (ONDREP) souligne une explosion de ces violences entre 1996 et 2018, avec une hausse de 279% pour les viols et de 315% pour les agressions sexuelles. En Allemagne, le *Bundeskriminalamt* rapporte des chiffres tout aussi préoccupants : une augmentation de 31% des contenus pornographiques destinés aux jeunes en 2023, avec une proportion significative de suspects mineurs (38% pour les contenus de matériel d'abus sexuels d'enfants, 49,5% pour les contenus de pornographie juvénile).

Stimulation d'un intérêt sexuel envers les enfants

La sexualisation à travers les médias de masse peut stimuler l'intérêt sexuel envers les enfants (Rush 1980 ; Wurtele et Miller-Perrin 1993 ; Russell 1998), tandis qu'un environnement sociétal tolérant les fantasmes sexuels impliquant des mineurs rend plus probables l'intérêt sexuel pour les enfants et les abus sexuels (Schmitt 1994 ; van Dam 2001).

Préjudices liés à l'intelligence artificielle

L'utilisation croissante de l'intelligence artificielle (IA) dans la production de contenus illicites nécessite une réponse forte pour contrer la normalisation de ces violences et sensibiliser le public à leur gravité. Les développements récents en matière d'IA soulèvent de nouvelles préoccupations majeures. Le rapport CyberTipline 2023 du National Center for Missing and Exploited Children (NCMEC 2023) révèle avoir reçu 4.700 signalements de CSAM ou autres contenus sexuellement exploitatifs liés à l'IA générative. Plus inquiétant encore, plus de 70% de ces signalements de CSAM généré par l'IA proviennent des plateformes traditionnelles, ce qui indique que la plupart des plateformes d'IA où le contenu est créé ne signalent pas au CyberTipline. Le NCMEC se montre particulièrement préoccupé par cette tendance en rapide croissance, car les malfaiteurs peuvent utiliser l'IA générative pour créer des deepfakes sexuellement explicites basés sur n'importe quelle photographie d'un enfant réel ou générer du CSAM montrant des enfants générés par ordinateur dans des actes sexuels graphiques. En outre, des familles et des enfants sont victimes de chantage par des criminels utilisant du CSAM généré par l'IA à des fins lucratives.

L'intelligence artificielle représente une nouvelle frontière de risques, avec notamment la création de CSAM généré artificiellement et l'émergence de chatbots pouvant avoir des interactions hautement inappropriées avec les mineurs. Ces développements technologiques exigent une vigilance accrue et des réponses réglementaires adaptées.