Commission nationale consultative des droits de l'homme

Avis sur la protection de l'intimité des jeunes en ligne (A – 2025 – 1)

NOR : *CDHX2502929V*

Assemblée plénière du 23 janvier 2025
(Adoption à l'unanimité, moins une abstention)

1. Les jeunes sont très présents sur les réseaux sociaux, tant pour s'informer, jouer, et communiquer que pour partager leur quotidien à travers des messages, photos et vidéos (1). Ils y échangent parfois des contenus intimes, exposant ainsi leur vie sexuelle et affective, au risque d'être confrontés à des actes malveillants. Les jeunes sont d'ailleurs de plus en plus victimes en ligne d'atteintes à leur intimité (2). Cette amplification s'explique en partie par une évolution de la cybercriminalité qui n'est plus le monopole de cybercriminels expérimentés, mais devient accessible à tout délinquant « *sans compétence ni budget important* » (3), en particulier du fait de l'essor des outils d'intelligence artificielle (IA) générative de textes, d'images ou de contenus audio hypertruqués. Au terme d'une série d'auditions menées avec des représentants de plateformes, des acteurs de la protection de l'enfance d'une part et de la répression pénale d'autre part, la Commission nationale consultative des droits de l'Homme fait le constat que la réponse des réseaux sociaux ainsi que des pouvoirs publics n'est pas à la hauteur des risques encourus par les mineurs.
2. Ces atteintes à l'intimité peuvent prendre différentes formes :
   – partager des photos ou des vidéos intimes d'une personne sans son consentement ;
   – concevoir et partager des deepfakes (4) à caractère sexuel à partir de la photographie d'un visage, ou encore dénuder numériquement une personne ;
   – exposer une personne qui ne l'a pas sollicité à une image à caractère sexuel (*cyberflashing*) (5) ;
   – pour un adulte, tromper un mineur en ligne pour qu'il se livre à des pratiques sexuelles (*grooming*) (6) ;
   – extorquer des images intimes et/ou de l'argent d'une personne sous la menace de diffuser des contenus intimes partagés au préalable par cette personne, ou des deepfakes à caractère sexuel mettant cette personne en scène (sextorsion).
3. D'après les auditions menées par la CNCDH, si tous les jeunes, quel que soit leur genre, peuvent être visés par ces comportements, la majorité de ces actes malveillants visent les filles. La CNCDH relève aussi que ces cyberviolences à caractère sexiste et sexuel (7) peuvent engendrer une vulnérabilité susceptible de faciliter l'entrée dans la prostitution et l'exploitation sexuelle.
4. Ces risques en ligne pour les jeunes femmes ont été rappelés récemment par l'Assemblée générale des Nations Unies dans une résolution intitulée « intensification de l'action menée pour prévenir et éliminer toutes les formes de violence à l'égard des femmes et des filles : l'environnement numérique » (8). Le texte invite notamment les Etats à mieux protéger les droits des femmes et des filles dans l'environnement numérique et à lutter contre l'impunité des agresseurs. Il appelle également les acteurs du numérique, en particulier les plateformes, à « *redoubler d'efforts pour supprimer les contenus en ligne relatifs à des actes de violence sexuelle et fondée sur le genre* ». La CNCDH salue le travail accompli par la diplomatie française à l'origine de cette résolution.
5. A l'exception du cyberflashing, les violences sexuelles et sexistes évoquées précédemment sont incriminées en droit français. La dernière actualisation du code pénal en la matière est issue de la loi visant à sécuriser et à réguler l'espace numérique (la loi SREN), adoptée en mai 2024 (9). Elle a enrichi l'arsenal répressif sur les violences sexuelles en ligne, en y ajoutant les sextorsions et la diffusion de deepfakes à caractère sexuel (10), mais a omis néanmoins de réserver un traitement spécifique aux victimes mineures (11). Elle a aussi inclus, au sein de la formation scolaire, à partir du collège, à l'utilisation des outils et des ressources numériques, une sensibilisation aux violences sexistes et sexuelles en ligne (12).
6. Outre le volet pénal, le cadre légal pour assurer la protection des mineurs en ligne repose en grande partie sur la réglementation européenne, principalement le règlement de l'UE sur les services numériques adopté en 2022 (DSA) (13). Parmi les objectifs affichés par ce règlement, figure en bonne place la protection des mineurs. Son article 28 enjoint en particulier aux fournisseurs de plateformes en ligne accessibles aux mineurs de mettre 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* ».
7. Les auditions ont permis de constater qu'un certain nombre de réseaux sociaux, parmi les plus populaires auprès des jeunes, prennent les enjeux de protection très au sérieux et s'emploient d'ores et déjà à mettre en place des mesures pour protéger les mineurs. L'avis reviendra plus en détail sur ces mesures qui consistent dans l'ensemble à restreindre leurs possibilités, d'une part, d'échanger des contenus et, d'autre part, d'élargir leur réseau de relations. Les dispositifs mis en place pour limiter les risques manquent cependant leur cible à défaut de pouvoir vérifier l'âge des utilisateurs. Indépendamment même du contournement par certains mineurs, parfois très jeunes, de l'interdiction de s'inscrire sur un réseau social en dessous de 13 ans (14), les

plateformes se heurtent à cette difficulté : plus elles mettent en place des mesures de protection à destination des utilisateurs âgées de 13 à 18 ans, plus ces derniers sont tentés de déclarer qu'ils sont majeurs afin de ne pas être entravés dans leurs usages.

8. Le 31 juillet 2024, la Commission européenne a lancé une consultation auprès des parties prenantes (plateformes, autorités de régulation, ONG de protection de l'enfance, etc.) pour l'élaboration des lignes directrices qu'elle adoptera afin d'éclairer les plateformes sur la mise en œuvre de l'article 28 du DSA. Par ailleurs, il convient de rappeler que la Commission européenne a lancé en 2022 sa nouvelle stratégie pour un internet plus sûr pour les enfants, (Better Internet for Kids (BIK +), qui prend la suite de celle qui a été initiée en 2008. En pratique, sa mise en œuvre repose sur deux réseaux d'actions ; le réseau Insafe mis en place pour accompagner les jeunes et les professionnels dans la prévention des risques et la promotion des usages positifs d'internet (*awareness* et *helpline*) ainsi que Inhope qui permet de coordonner les plateformes de signalement de chaque pays (*hotline*).

9. Le volet français du BIK – le « Safer internet France » – repose sur trois partenaires : Tralalere, producteur de programmes éducatifs pluri médias et de campagnes de sensibilisation, souvent avec le soutien du ministère de l'éducation nationale, et qui anime un programme de sensibilisation aux risques en ligne, « Internet sans crainte » (15) (*awareness*) ; Point de contact, qui gère une plateforme de signalement de contenus illicites (16) (*hotline*) ; et e-Enfance, dédié à l'aide des jeunes victimes et témoins de harcèlement et de violences numériques, qui gère la ligne d'écoute « 3018 » (17) (*helpline*), numéro gratuit, confidentiel et anonyme. Cet écosystème est toutefois insuffisant pour répondre aux besoins des jeunes en la matière et manque de lisibilité.

10. Dans la continuité de ses travaux sur la haine en ligne (18), la CNCDH s'est auto-saisie du problème des atteintes à l'intimité des jeunes en ligne. L'un des enjeux soulevés par ce sujet est de parvenir à garantir un équilibre entre la protection des enfants et le respect de leur vie privée. Deux écueils menacent en effet une politique de protection de l'intimité des jeunes en ligne : d'un côté, enserrer les jeunes dans un carcan technologique ou parental trop étroit pour qu'ils puissent exercer librement leur vie affective et relationnelle en ligne ; d'un autre côté, adopter des mesures destinées à la protection des jeunes potentiellement attentatoires aux libertés de tous les utilisateurs.

11. Le présent avis traite des points suivants :

– la protection de l'intimité des jeunes en ligne suppose de faire connaître aux mineurs leurs droits et leurs obligations et de leur apporter l'aide et le soutien dont ils ont besoin lorsqu'ils sont victimes ou témoins d'actes malveillants. Au-delà, il est urgent de renforcer la sensibilisation aux violences sexuelles et sexistes, en ligne et hors ligne, ce qui passe en partie par une éducation à la vie affective, sexuelle et relationnelle garantie à tous les âges (1) ;
– de leur côté, les réseaux sociaux doivent aller plus loin dans la protection des mineurs, en alignant leurs paramétrages par défaut sur des standards de protection élevés, et en s'investissant dans les programmes de partage et de détection des hashs – empreintes numériques (19) – d'images intimes (2) ;
– les autorités doivent rester très vigilantes face à l'essor des deepfakes à caractère sexuel et limiter les systèmes d'intelligence artificielle susceptibles d'en générer (3) ;
– enfin, une réponse pénale appropriée permettra de sanctionner les auteurs de violences sexistes et sexuelles et contribuera à l'effort de dissuasion (4).

1. **Prévenir les violences sexuelles**

12. Les violences sexuelles en ligne sont encore trop peu évoquées dans l'espace public ou dans l'enceinte scolaire. Les mineurs ont ainsi rarement conscience des risques auxquels ils sont exposés lorsqu'ils sont présents sur les réseaux sociaux. Ils peuvent aussi eux-mêmes adopter des comportements répréhensibles, faute d'une prise en compte suffisante de l'autre et de son intimité. C'est pourquoi les pouvoirs publics doivent sensibiliser les jeunes et, plus largement l'ensemble de la population, aux risques pour l'intimité encourus sur les réseaux sociaux.

13. La CNCDH recommande d'informer en début d'année scolaire les élèves sur les violences sexuelles en ligne, en complément de la sensibilisation au harcèlement actuellement prévue. Cette information devrait être complétée par la communication, en début d'année et par tout moyen, des interdictions prévues par la loi (sextorsion, deepfakes à caractère sexuel, etc.). Il faut aussi renforcer l'information sur l'existence des services d'accueil et d'écoute, tels que la ligne d'écoute « 30 18 », dans tous les lieux scolaires, péri et extrascolaires (20).

14. La CNCDH recommande aussi d'adresser ces informations aux parents d'élèves, à l'occasion des réunions auxquels ils sont conviés (notamment via des webinaires), ou par le biais des canaux de communication de l'école (Espaces numériques de travail (ENT), mails, newsletters), ou encore par des conférences organisées au sein de l'établissement et animées par des professionnels pour expliquer les risques des cyberviolences avec des termes simples et accessibles. Consciente des difficultés pour impliquer les parents dans ce type de séance, la CNCDH invite les pouvoirs publics à réfléchir à des modalités d'accueil plus attractives. Sur le fond, il faut passer par des exemples concrets de situations à risque, des signaux d'alerte à surveiller, des premiers réflexes, etc. Ces séances d'information adressées aux parents doivent promouvoir le dialogue ouvert avec leurs enfants sur leurs pratiques en ligne, le consentement et l'importance de demander de l'aide en cas de besoin, en valorisant leur rôle de soutien et d'écoute, plutôt que de contrôle.

15. En outre, la CNCDH réitère sa recommandation, formulée dans son avis sur la lutte contre la haine en ligne (21), de développer des formations aux bonnes pratiques numériques sur le temps professionnel ou du moins sur le lieu de travail, par exemple avec le soutien des syndicats ou des comités sociaux et économiques des entreprises qui en disposent. Ces formations axées sur les ressorts techniques et économiques des réseaux sociaux pourront inclure une sensibilisation aux violences sexuelles et sexistes en ligne, et avertir ainsi les parents des risques auxquels sont exposés les enfants.

16. La CNCDH recommande par ailleurs d'organiser au niveau national une campagne de sensibilisation aux risques de sextorsion et de violences sexuelles en ligne (sur le modèle de la campagne « Enfants et écrans » 2024 de l'ARCOM (22)), adaptée au public : des messages de différente nature selon les âges, pourront être proposés, en fonction des horaires de diffusion et des programmes. En plus des médias classiques, les réseaux sociaux devraient être associés à la diffusion de cette campagne. La CNCDH préconise également d'intégrer les élèves dans les dispositifs de prévention et de détection des cyberviolences afin d'en accroître l'efficacité.

17. Enfin, s'agissant de la prise en charge des jeunes victimes d'abus sexuels en ligne, les auditions ont pu mettre en évidence leur sentiment de solitude : bien souvent, ils ne savent pas vers quels adultes se tourner en cas de problème. Dans le cadre du programme Phare (contre le harcèlement), est prévue la formation d'une « communauté protectrice autour des élèves » : notamment cinq personnels ressources (au minimum) par établissement du second degré sont formés à la prise en charge des situations de harcèlement. La CNCDH recommande d'étendre leur rôle à l'écoute et à la prise en charge des mineurs exposés à des violences sexuelles. Ils pourraient au minimum les orienter vers les services dédiés en cas de besoin.

18. La ligne d'écoute mise à la disposition des victimes et de leurs parents, le « 30 18 » porté par l'association e-Enfance, n'est pas en mesure actuellement de répondre à la quantité d'appels qui leur sont adressés (sur les 160 000 appels reçus en 2024, les équipes du « 30 18 » n'ont pu répondre qu'à un tiers d'entre eux). La CNCDH recommande d'augmenter les capacités d'écoute du « 30 18 », en finançant des postes d'écoutants supplémentaires et en assurant une meilleure visibilité du service auprès de la population, en particulier des mineurs, des parents et des professionnels.

19. La part prise par les violences sexuelles et sexiste en ligne doivent également alerter les pouvoirs publics. Ces agissements s'inscrivent plus largement dans un système de relations marqué par des stéréotypes de genre et une objectivation du corps des femmes. C'est justement à leur remise en cause que l'éducation à la sexualité et à la vie affective doit s'appliquer. Depuis 2001, une information et une éducation à la sexualité doivent normalement être dispensées dans les écoles, les collèges et les lycées à raison d'au moins trois séances annuelles et par groupes d'âge homogène (23). Le code de l'éducation précise que ces séances « *présentent une vision égalitaire des relations entre les femmes et les hommes* » et « *contribuent à l'apprentissage du respect dû au corps humain et sensibilisent aux violences sexistes ou sexuelles* ». Or, d'après un rapport de l'Inspection générale de l'Education nationale remis en juillet 2021, « *force est de constater que bien des élèves traversent leur scolarité sans avoir bénéficié d'une seule séance d'éducation à la vie affective et sexuelle, si l'on excepte les apports des programmes des disciplines liées aux sciences de la vie, aux sciences médicosociales et à la prévention santé environnement, portant sur des aspects essentiellement physiologiques* ».

20. La CNCDH tient à rappeler qu'en garantissant une éducation à la vie affective, relationnelle et sexuelle (EVARS), les pouvoirs publics répondraient aussi aux obligations prévues par la Convention internationale des droits de l'enfant (CIDE), relatives au respect de la vie privée, au droit à la protection contre toute violence et formes d'exploitation sexuelle, à l'information et à l'éducation, et par plusieurs dispositions de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Convention d'Istanbul). Il incombe en effet à l'État de faire prévaloir les droits fondamentaux des jeunes, notamment face aux oppositions exprimées de manière croissante par certains groupes et acteurs politiques à l'égard de l'EVARS. C'est d'autant plus important que, par-delà le respect des droits fondamentaux des enfants, c'est une question de santé publique qui est en jeu : les atteintes à l'intimité en ligne et, plus largement, l'exposition à des contenus pornographiques et la tendance à l'hypersexualisation des jeunes, ont des répercussions préoccupantes sur leur santé mentale et physique d'après les auditions menées par la CNCDH.

21. La CNCDH a pris connaissance avec intérêt des recommandations formulées par le Conseil économique, social et environnemental (CESE) dans son avis sur l'EVARS publié en septembre 2024 (24). Le CESE y préconise notamment la mise en place d'une « *éducation aux compétences psychosociales et à l'égalité* » (25), au sein de laquelle s'inscrirait l'EVARS, avec un volume horaire annuel d'au moins 30 heures dès le collège. Au minimum, la CNCDH recommande de porter une politique publique consacrée à l'EVARS, pilotée au niveau national et local, destinée à garantir l'effectivité de l'obligation légale des trois séances annuelles. La CNCDH soutient également la recommandation du CESE visant à créer une incrimination pénale pour sanctionner toute entrave au droit des enfants de bénéficier de l'EVARS.

22. S'agissant du contenu de l'EVARS, la CNCDH recommande d'insister sur le respect du consentement, la diffusion d'une culture de l'égalité, la déconstruction d'un certain nombre d'idées reçues liées à la sexualité et perpétuées par des contenus pornographiques en ligne souvent violents, ainsi que la prévention des pratiques prostitutionnelles. Une attention critique particulière pourra être aussi portée à l'essor des discours masculinistes dans la mesure où ils sont attachés à la perpétuation des rapports de domination des hommes sur les femmes, et des stéréotypes de genre. Pour protéger l'intimité des jeunes en ligne, il est fondamental de croiser l'éducation à la sexualité et l'éducation au numérique et aux médias. Les pratiques en ligne évoquées

dans le cadre de cet avis doivent donc être mentionnées dans les séances d'EVARS tout en intégrant la dimension genrée des cyberviolences.

23. La CNCDH recommande de faire appel à des intervenants extérieurs ayant une expertise particulière en matière d'EVARS, dont les associations agréées par le ministère de l'éducation nationale, pour animer ces séances. Actuellement, les associations manquent de ressources humaines et financières suffisantes pour répondre à l'ensemble des sollicitations qu'elles reçoivent. Elles sont précarisées par la nécessité de répondre régulièrement à des appels à projets pour maintenir leurs activités. La CNCDH recommande donc de passer d'un financement de projet à un financement pérenne de fonctionnement de ces associations. Elle recommande également d'assurer la protection de leurs membres et de leurs intervenants, parfois menacés par des groupuscules hostiles à l'EVARS.

24. En lien avec les travaux du CESE, le Conseil national numérique (CNNum) a aussi publié récemment ses analyses et ses recommandations en matière d'EVARS (26). D'un côté, il y met en lumière les ressources d'EVARS disponibles en lignes – le numérique comme « outil » de l'EVARS – et, d'un autre côté, souligne la nécessité de prendre en compte au sein de l'EVARS les « *pratiques numériques [qui] représentent aussi de nouveaux terrains d'exploration de l'éveil relationnel, affectif et sexuel* ».

25. A l'instar du CNNum, la CNCDH déplore l'invisibilisation en ligne des contenus susceptibles de contribuer de manière positive à l'EVARS en dehors du cadre scolaire. Parmi ces contenus, certains émanent d'acteurs institutionnels (notamment « onsexprime.fr » conçu par santé publique France) tandis que d'autres sont conçus par des acteurs privés, avec de nombreux comptes et pages souvent alimentés par de jeunes femmes soucieuses de proposer des contenus favorables à l'égalité de genre (27).

26. Dans son rapport, le CNNum éclaire sur les obstacles restreignant l'accès à ce type de contenu, qui tiennent à plusieurs facteurs, telles que les conditions générales d'utilisation (CGU) des plateformes – en particulier la lutte contre les contenus pornographiques – associées à des algorithmes de modération qui suppriment des contenus pédagogiques liés à la sexualité faute d'une appréciation suffisante du contexte (28). Le modèle économique des plateformes, qui valorise des contenus polarisants, contribue également à la sous-représentation de contenus ou de créateurs de contenus en lien avec l'EVARS.

27. La CNCDH, à l'instar du CNNum, recommande de protéger les contenus d'EVARS de tout mécanisme d'invisibilisation. Elle recommande en outre de mettre en avant les comptes et contenus qui proposent des informations en lien avec l'EVARS attachées à favoriser l'égalité des genres, en raison de leur utilité publique.

28. En outre, afin d'assurer un meilleur accès à ces contenus et de renforcer l'autonomie des jeunes face aux recommandations fournies par les algorithmes des plateformes, la CNCDH recommande à nouveau la consécration d'un droit au paramétrage au bénéfice des utilisateurs afin de leur permettre de définir précisément le type de contenus auxquels ils souhaitent être exposés lors de leurs interactions via les réseaux sociaux (29).

2. **Contrôler davantage les réseaux sociaux**

29. Face aux risques d'atteintes à l'intimité des jeunes en ligne, certains réseaux sociaux mettent en place des mesures de protection. Ces dernières s'apparentent le plus souvent à des restrictions d'utilisation en fonction de l'âge. Les restrictions vont porter notamment sur :

- la visibilité limitée des messages publiés par le mineur ;
- l'impossibilité de recevoir des messages de personnes avec lesquelles le mineur n'est pas connecté ;
- l'impossibilité de publier des vidéos ;
- la désactivation des captures d'écrans des photos envoyées par message privé ;
- l'envoi à l'expéditeur de messages de sensibilisation aux risques auxquels il s'expose lors de la transmission d'images intimes ;
- une mise en garde à la réception d'une image intime, floutée dans un premier temps, précisant à son destinataire qu'il ne doit pas se sentir obligé de l'ouvrir.

Certaines plateformes utilisent aussi des logiciels de détection automatique pour supprimer des images à caractère sexuel.

30. La CNCDH a pris connaissance avec intérêt de ces paramétrages par défaut destinés à renforcer la protection et l'autonomie des mineurs, en les mettant à l'abri de sollicitations intempestives, de partage non consenti de contenus, et en leur ménageant davantage de temps et de réflexivité dans leurs échanges.

31. La limite de ces paramétrages plus protecteurs repose toutefois en grande partie sur le fait qu'à l'heure actuelle la détermination de l'âge des utilisateurs des réseaux sociaux relève d'un régime déclaratoire. Les mineurs peuvent donc être tentés d'échapper à ces mesures restrictives de liberté en se déclarant majeurs. C'est d'autant plus aisé pour eux que les parents contrôlent rarement ce que font leurs enfants sur internet.

32. Par ailleurs, les mesures destinées à protéger les mineurs peuvent s'analyser comme des atteintes à leurs droits fondamentaux. Ce faisant, elles doivent répondre à certaines conditions, en particulier présenter un caractère nécessaire, adapté et proportionné. Des mesures qui consisteraient à supprimer automatiquement des images à caractère sexuel échangés entre des mineurs peuvent ainsi apparaître disproportionnés. Ces mesures seraient d'autant plus inadaptées que les jeunes ont non seulement le droit au respect de leur vie privée, mais qu'ils peuvent également échanger des contenus pédagogiques d'EVARS qui seraient susceptibles d'être supprimés par des outils technologiques incapables de tenir compte du contexte.

33. La CNCDH suit avec attention les travaux menés par l'Arcom pour l'élaboration d'un référentiel technique relatif aux systèmes de vérification de l'âge pour l'accès à des contenus pornographiques. Elle souscrit au point de vue exprimé par la CNIL, dans son avis sur le projet de référentiel que lui a soumis l'Arcom, selon lequel il faut réserver le contrôle de l'âge sur Internet à certains contextes spécifiques, en particulier en cas de danger pour les mineurs (30). Selon l'autorité administrative indépendante, « *sa généralisation pourrait en effet conduire à la mise en place d'un monde numérique fermé, dans lequel les individus devraient constamment prouver leur âge, voire leur identité, entraînant d'importants risques pour leurs droits et libertés, notamment la liberté d'expression* ».

34. Réservée à l'égard d'une vérification de l'âge pour l'accès à tous les réseaux sociaux, mais consciente également du contournement des paramétrages par défaut proposés à l'heure actuelle pour les mineurs par certaines plateformes, la CNCDH recommande d'appliquer ces paramétrages à tous les utilisateurs. Parmi ces paramètres, l'impossibilité pour une personne qui ne fait pas partie du cercle d'"amis" d'un utilisateur de lui envoyer des messages privés, peut contribuer à protéger le mineur. Si l'on peut admettre à partir d'un certain âge que les adolescents renoncent à cette fonctionnalité, un message d'information, adapté à l'âge et dans un format approprié, devra leur être communiqué afin de les mettre en garde contre les risques d'atteinte à leur intimité en ligne, notamment la sextorsion. Cette communication, par un message texte ou par une vidéo, devra permettre d'assurer un temps de réflexion à l'adolescent sur ses usages des réseaux sociaux.

35. Par ailleurs, la CNCDH relève que la disparité des dispositifs de signalement entre les différentes plateformes est une source de confusion pour les usagers. Elle recommande donc d'uniformiser ces outils de notification.

36. De surcroît, les réseaux sociaux doivent répondre au plus vite à la demande de suppression d'un contenu intime. Les auditions ont rendu compte de la célérité des plateformes pour supprimer des images intimes de mineurs lorsque des associations telles que e-Enfance ou Point de contact leur adressent un signalement. La CNCDH relève qu'elles devraient observer la même diligence lorsqu'un signalement émane d'un usager victime dès lors que le contenu est manifestement illicite. La CNCDH salue la réactivité de la France dans la désignation du premier signaleur de confiance, l'association e-Enfance, le 6 novembre 2024, tout en pointant la nécessité d'en désigner d'autres.

37. L'une des options prometteuses pour lutter contre la diffusion non consentie de contenus intimes en ligne réside dans le développement du hachage, en particulier les hachages perceptuels. Le hash perceptuel s'apparente à une signature/empreinte numérique attribuée à une image, permettant de détecter des contenus similaires. Cette signature permet d'avoir un suivi du contenu et ainsi d'ajouter cette information dans un système d'IA qui permettra de détecter le hash perceptuel s'il se présente à nouveau (ce qui permet d'agir plus rapidement) ; puis, de transmettre le hash à des plateformes pour qu'elles fassent de la détection proactive et identifient rapidement le contenu afin d'en assurer le retrait. Cette technologie soulève néanmoins des enjeux en termes de centralisation et de partage des données, sans compter les risques de faux positifs et de faux signalements. Cela implique donc une évaluation rigoureuse et transparente permettant de mesurer la robustesse et l'efficacité des fonctions de hachage.

38. Les jeunes pourraient ainsi télécharger au préalable les images qu'ils craignent de voir publiées en ligne, afin qu'un système d'IA sécurisé détecte et bloque toute tentative de télécharger une image similaire. La plateforme peut aussi s'engager à désactiver automatiquement les comptes qui publieraient ce contenu. Cette approche se heurte toutefois à plusieurs difficultés : elle suppose que la victime consente à confier cette image à la plateforme, qu'elle soit consciente de l'existence de l'image en question et/ou en possession de l'image utilisée contre elle. Il y a aussi un aspect technique dans la mesure où si l'image est recadrée ou un peu modifiée (ajout d'un émoji par exemple), elle s'apparente à une nouvelle photo, et ne sera donc pas reconnue par le hash. De surcroît, l'ampleur du « filet » de détection des hash est conditionnée par la participation des plateformes.

39. A l'heure actuelle, il existe plusieurs initiatives qui reposent sur cette technologie. Au début de l'année 2023, le *National Center for Missing and Exploited Children* (NCMEC), organisme américain de protection de l'enfance, a lancé une plateforme baptisée « *Take it down* », pour aider les mineurs à faire retirer des réseaux sociaux les photos et vidéos d'eux dénudés ou à caractère sexuel (31). La liste des hashs (32) ainsi créés par la plateforme est partagée avec une dizaine de plateformes volontaires (33).

40. Fin 2023, l'association Point de contact, spécialisée dans l'analyse et le signalement des contenus illicites en ligne, a lancé une initiative du même genre – Disrupt – adaptée à la législation nationale et accessible à tous les usagers. Si elle a pu bénéficier d'un financement pour la création de la plateforme de partage des images destinées à être hachées, elle ne disposait pas des moyens de finaliser le développement du dispositif en partageant les hashs avec le plus grand nombre de plateformes/hébergeurs, et en le faisant connaître par des campagnes de communication/sensibilisation ciblées. La CNCDH recommande donc aux pouvoirs publics de financer le développement de la plateforme (afin de permettre notamment l'amélioration de l'interface, les évolutions technologiques et les partenariats, l'augmentation des ressources humaines) et d'en assurer une plus grande visibilité auprès de la population, en particulier les enfants. Afin d'améliorer les techniques de hachage, la CNCDH recommande, en outre, aux pouvoirs publics d'apporter un soutien à la recherche dans ce domaine, notamment par des projets financés par l'Agence nationale de la recherche.

3. **Mieux encadrer l'utilisation de l'IA**

41. S'agissant de l'utilisation de l'IA, il faut distinguer deux cas de figure : d'un côté l'IA générative, de l'autre une IA spécifique à la réalisation de deepfakes. A titre d'illustration, chacune de ces technologies peut être utilisée pour déshabiller numériquement une personne. L'IA générative fonctionne à partir de l'analyse de millions de photos de personnes nues et sera en mesure, au terme de cet apprentissage, de « reconstituer » le corps dénudé de la personne dont la photo aura été présentée à la machine. La technologie associée au deepfake permettra pour sa part d'associer la photo du visage de la personne à un corps nu anonyme, mais conduira à un résultat beaucoup plus crédible qu'un simple photomontage. Quelle que soit la technologie employée, une personne peut donc faire l'objet d'un « déshabillage » sans son consentement.

42. Pour chacune de ces technologies, le règlement de l'UE sur l'intelligence artificielle consacre une obligation de transparence (art. 50) : les fournisseurs de systèmes d'IA, y compris de systèmes d'IA générative, doivent veiller à ce que les sorties (*outputs*) soient marquées dans un format lisible par la machine et identifiables comme ayant été générées ou manipulées par une IA ; quant aux déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage, ils doivent indiquer que les contenus ont été générés ou manipulés par une IA (34). La CNCDH relève l'importance pour l'autorité de surveillance du marché, chargée de faire respecter ces obligations, de traiter des deepfakes à caractère sexuel de manière prioritaire, en particulier lorsqu'ils concernent des mineurs. De surcroît, la CNCDH estime que les fournisseurs de très grandes plateformes et de très grands moteurs de recherche en ligne doivent s'employer, au titre de l'article 35 du DSA (35), à endiguer la diffusion de ce type de *deepfake*.

43. En outre, la CNCDH recommande aux fournisseurs de systèmes d'IA générative de brider la capacité du système à produire des deepfakes à caractère sexuel mettant en scène des enfants et de mettre en place les moyens suffisants pour en garantir l'effectivité. Les modèles d'IA peuvent en effet être conçus de manière à rejeter, en raison de leur caractère inapproprié, certains types d'instructions émanant d'utilisateurs. Ils peuvent aussi être développés de manière à ne pas générer certains contenus, identifiés comme problématiques au stade de la conception. Dans ce cas, le modèle inspecte automatiquement le contenu généré avant de le délivrer à l'utilisateur. Il convient par ailleurs de mettre en œuvre tous les moyens nécessaires afin de vérifier que ces outils ne peuvent pas être ou n'ont pas été détournés, notamment en favorisant la collaboration avec des chercheurs indépendants pour en tester la robustesse, et de mettre en place des mécanismes de réponse adaptés pour corriger tout risque de contournement.

44. Enfin, la CNCDH recommande le déférencement sur les moteurs de recherche, des sites et des applications dédiés aux deepfakes à caractère sexuel, ainsi que le blocage sur les magasins d'applications (« app stores ») des applications qui dénudent numériquement les individus sans leur consentement, à moins que le fournisseur de l'application n'apporte à la plateforme toutes les garanties pour s'assurer du consentement de la personne dénudée numériquement.

4. **Améliorer la réponse pénale**

45. La plupart des agissements malveillants évoqués dans le cadre de cet avis font l'objet d'une infraction pénale. Afin de réprimer plus sévèrement les auteurs de sextorsion, la loi SREN du 21 mai 2024 a modifié l'article 312-10 du Code pénal qui érige désormais en circonstances aggravantes tout chantage lorsqu'il est exercé par un service de communication en ligne « *au moyen d'images ou de vidéos à caractère sexuel* », ou « *en vue d'obtenir des images ou des vidéos à caractère sexuel* ».

46. La CNCDH recommande de compléter le nouvel article 312-10 du code pénal relatif au chantage par la prévision d'une aggravation de la peine lorsque les faits ont été commis à l'encontre d'un mineur de moins de 15 ans et de prévoir une aggravation supplémentaire quand ils l'ont été en bande organisée. La rédaction retenue pourrait ainsi s'inspirer de celle de l'article 227-23-1, alinéa 2, du code pénal.

47. Par ailleurs, le code pénal incrimine à l'heure actuelle le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique (36). Cette disposition mériterait d'être complétée afin de viser aussi la création d'un tel contenu, indépendamment d'une diffusion éventuelle, par un système d'IA. Pour le libellé de ce nouvel alinéa, la CNCDH recommande de s'inspirer de la formulation suggérée par la Fondation pour l'enfance dans son rapport récent consacré à « l'IA générative, nouvelle arme de la pédocriminalité » : « *Le fait, de concevoir, de créer, de diffuser ou de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, tout montage, contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique tel que visé à l'alinéa 1 de l'article 226-8-1 est puni lorsqu'il s'agit de la représentation, de l'image ou de la parole d'un mineur* » (37).

48. Aux termes de l'article 226-8-1 du code pénal, les deepfakes à caractère sexuel sont incriminés lorsqu'ils concernent les paroles ou l'image d'une personne et qu'ils sont portés, sans son consentement, à la connaissance du public ou d'un tiers. La CNCDH recommande de revoir la rédaction de cet article afin d'interdire ce type de contenu lorsqu'il concerne des mineurs de moins de quinze ans, sans référence dans ce cas à leur consentement éventuel. En outre, il conviendrait d'ériger en circonstance aggravante la minorité de la victime, en s'assurant d'une cohérence avec les peines prévues par l'article 227-23. Par ailleurs, à l'instar du projet de loi britannique prochainement en discussion (38), la CNCDH recommande d'incriminer, en complément de sa diffusion, la création d'un deepfake à caractère sexuel dès lors qu'il est réalisé sans le consentement de la personne.

49. Enfin, la CNCDH recommande d'incriminer le cyber-flashing, sachant que la directive européenne adoptée en mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique (39) appelle les Etats membres à ériger ce comportement en infraction. La CNCDH relève que la directive précise, cependant, que l'interdiction ne vaut que si elle « *cause un préjudice psychologique important à [la] personne* ». Le souci d'assurer une protection maximale aux victimes supposera de ne pas retenir cette condition lors de la transposition.

50. La CNCDH recommande en outre d'accompagner l'entrée en vigueur des trois nouveaux alinéas de l'article 312-10 du Code pénal par l'élaboration et la diffusion d'une circulaire de politique pénale du garde de sceaux à l'attention des parquets aux fins de favoriser l'appropriation de ces nouvelles circonstances aggravantes, pour saisir ce phénomène en pleine croissance, et d'encourager les parquets et l'ensemble des magistrats à y apporter une réponse rapide, systématique et efficace.

51. Dans le même sens, la CNCDH recommande de faciliter l'accueil des victimes, en favorisant leur dépôt de plainte et en conduisant des enquêtes fouillées que les sextorsions soient à caractère sexuel ou à des fins financières, et quel qu'en soit le préjudice.

52. La CNCDH recommande d'assurer la formation des magistrats, des policiers, des avocats, tant dans la formation initiale que dans la formation continue, aux dispositifs pénaux visant à lutter contre les infractions à caractère sexuelle et sexiste, et notamment en matière de cybercriminalité, en mettant l'accent sur les infractions les plus récentes.

53. La CNCDH recommande de faire évoluer les catégories de contenus illicites disponibles sur la plateforme de signalement en ligne (PHAROS), afin d'y inclure les infractions évoquées dans cet avis. Cela pourrait prendre la forme d'une catégorie générique telle que « Atteinte à l'intimité des mineurs en ligne », accompagnée d'une explication et de quelques exemples pour permettre aux victimes d'en comprendre la portée. Afin de pouvoir répondre à l'ampleur du phénomène, il convient également d'augmenter les effectifs de PHAROS.

54. Pour conclure, la protection de l'intimité des jeunes en ligne et, plus globalement, la lutte contre les violences sexuelles et sexistes dépendra surtout de l'engagement des pouvoirs publics à garantir l'EVARS, et de la capacité des régulateurs européens et nationaux à s'assurer que les plateformes assument leurs responsabilités en la matière sans se défausser sur les parents. Par ailleurs, au regard des débats relatifs à la Convention des Nations unies contre la cybercriminalité récemment adoptée par l'Assemblée générale (40) et à la proposition de règlement de l'Union européenne, actuellement en discussion, relative aux abus sexuels sur enfants (41), la CNCDH souligne l'importance de lutter contre la pédocriminalité, tout en respectant le droit à la vie privée des mineurs. La proposition de règlement prévoit notamment d'imposer aux plateformes de détecter et de supprimer des contenus « pédosexuels ». Si l'objectif poursuivi est parfaitement légitime, une telle mesure suscite néanmoins des réactions controversées s'agissant de son caractère adapté et proportionné. Outre les discussions sur la fiabilité des technologies utilisées à cet effet, ce type de dispositif impliquerait une surveillance accrue des messages échangés et des contenus publiés en ligne, au risque de porter une atteinte excessive au respect de la vie privée de l'ensemble des usagers des réseaux sociaux. Par conséquent, la CNCDH appelle à la conduite d'une réflexion approfondie entre l'ensemble des parties prenantes.

Liste des recommandations

Recommandation nº 1 : Informer en début d'année scolaire les élèves sur les violences sexuelles en ligne, en complément de la sensibilisation au harcèlement actuellement prévue.

Recommandation nº 2 : Renforcer l'information sur l'existence des services d'accueil et d'écoute pour les victimes de cyberviolence, tels que la ligne d'écoute « 30 18 », dans tous les lieux scolaires, péri et extrascolaires.

Recommandation nº 3 : Informer et sensibiliser les parents aux risques encourus par leurs enfants en ligne, par des réunions et par le biais des canaux de communication de l'école (Espaces numériques de travail (ENT), mails, newsletters).

Recommandation nº 4 : Développer à destination des parents des formations aux bonnes pratiques numériques, et des actions de sensibilisation aux cyberviolences, sur le temps professionnel ou, du moins, sur le lieu de travail.

Recommandation nº 5 : Organiser au niveau national une campagne de sensibilisation adaptée à différentes tranches d'âge, dans les médias et sur les réseaux sociaux, aux risques de sextorsion et de violences sexuelles en ligne.

Recommandation nº 6 : Étendre la mission des membres du personnel scolaire dédiés à la prise en charge des situations de harcèlement à l'écoute et à la prise en charge des mineurs exposés à des violences sexuelles.

Recommandation nº 7 : Augmenter les capacités d'écoute du « 30 18 », en finançant des postes d'écoutants supplémentaires et en assurant une meilleure visibilité du service auprès de la population, en particulier des mineurs, des parents et des professionnels.

Recommandation nº 8 : Porter une politique publique consacrée à l'éducation à la vie affective, relationnelle et sexuelle, pilotée au niveau national et local, afin de garantir l'effectivité de l'obligation légale des trois séances annuelles dans le primaire et dans le secondaire.

Recommandation nº 9 : Incriminer toute entrave au droit des enfants de bénéficier des séances d'éducation à la vie affective, relationnelle et sexuelle.

Recommandation nº 10 : Faire appel à des intervenants extérieurs ayant une expertise particulière en matière d'éducation à la vie affective, relationnelle et sexuelle, dont les associations agréées par le ministère de l'Éducation nationale, pour animer ces séances.

Recommandation nº 11 : Garantir la visibilité et assurer la promotion des comptes et contenus en ligne qui proposent des informations en lien avec l'éducation à la vie affective, relationnelle et sexuelle, et attachées à favoriser l'égalité des genres.

Recommandation nº 12 : Reconnaître un droit au paramétrage au bénéfice des utilisateurs afin de leur permettre de définir précisément le type de contenus auxquels ils souhaitent être exposés lors de leurs interactions via les réseaux sociaux.

Recommandation nº 13 : Appliquer à toutes les personnes inscrites sur les réseaux sociaux les paramétrages par défaut prévus pour la protection et l'autonomie des mineurs, en prévoyant la possibilité pour l'utilisateur de revenir sur ces paramètres, après avoir été pleinement averti des risques d'atteinte à son intimité en ligne.

Uniformiser le design des dispositifs de signalement de contenus illicites présents sur les plateformes en ligne.

Recommandation nº 14 : Financer le développement de la plateforme Disrupt, développée par l'association Point de Contact, et lui assurer une plus grande visibilité auprès de la population, en particulier les enfants.

Recommandation nº 15 : Apporter un soutien à la recherche consacrée à la détection des hashs, notamment par des projets financés par l'Agence nationale de la recherche.

Recommandation nº 16 : Imposer aux fournisseurs de systèmes d'IA de brider la capacité de leur système à produire des *deepfakes* à caractère sexuel mettant en scène des enfants et prévoir les moyens suffisants pour en garantir l'effectivité (vérifier en particulier que ces outils ne peuvent pas être ou n'ont pas été détournés, notamment en favorisant la collaboration avec des chercheurs indépendants pour en tester la robustesse, et mettre en place des mécanismes de réponse adaptés pour corriger tout risque de contournement).

Recommandation nº 17 : Déférencer, sur les moteurs de recherche, les sites et les applications dédiées aux deepfakes à caractère sexuel, et bloquer sur les magasins d'applications (« app stores ») des applications qui dénudent numériquement les individus sans leur consentement, à charge pour le concepteur de l'application de fournir à la plateforme les garanties prévues pour s'assurer du consentement de la personne dénudée numériquement.

Recommandation nº 18 : Compléter le nouvel article 312-10 du code pénal en prévoyant une aggravation de la peine lorsque les faits ont été commis à l'encontre d'un mineur de moins de 15 ans et une aggravation supplémentaire quand ils l'ont été en bande organisée.

Recommandation nº 19 : Ajouter un nouvel alinéa à l'article 227-23 du code pénal ainsi rédigé : « *Le fait, de concevoir, de créer, de diffuser ou de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, tout montage, contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique tel que visé à l'alinéa 1 de l'article 226-8-1 est puni lorsqu'il s'agit de la représentation, de l'image ou de la parole d'un mineur* ».

Recommandation nº 20 : Réviser l'article 226-8-1 du code pénal afin d'interdire les deepfakes à caractère sexuel mettant en scène des mineurs de moins de quinze ans, sans référence dans ce cas à leur consentement éventuel ; ériger en circonstance aggravante la minorité de la victime, en s'assurant d'une cohérence avec les peines prévues par l'article 227-23 ; incriminer, en complément de la diffusion d'un deepfake à caractère sexuel, la création d'un deepfake à caractère sexuel dès lors qu'il est réalisé sans le consentement de la personne.

Recommandation nº 21 : Incriminer l'envoi non sollicité d'une image/vidéo représentant l'organe génital d'une personne.

Recommandation nº 22 : Accompagner l'entrée en vigueur des trois nouveaux alinéas de l'article 312-10 du code pénal (sextorsion) par l'élaboration et la diffusion d'une circulaire de politique pénale du garde de Sceaux à l'attention des parquets aux fins de favoriser l'appropriation de ces nouveaux alinéas aggravants la peine encourue, et d'encourager les parquets à y apporter une réponse rapide, systématique et efficace ; faciliter l'accueil des victimes, en favorisant leur dépôt de plainte et en conduisant des enquêtes fouillées que les sextorsions soient à caractère sexuel ou à des fins financières, et quel qu'en soit le préjudice matériel.

Recommandation nº 23 : Assurer la formation des magistrats, des policiers, des avocats, tant dans la formation initiale que dans la formation continue, aux infractions les plus récentes, à savoir celles prévues aux articles 226-8-1 et 312-10 du code pénal.

Recommandation nº 24 : Compléter les catégories de contenus illicites disponibles sur la plateforme de signalement en ligne (PHAROS), afin d'y inclure les atteintes à l'intimité en ligne ; augmenter en conséquence les effectifs de PHAROS.

---

(1) « Enfants et écrans : à la recherche du temps perdu », Avril 2024. Ce rapport a été adopté par une Commission nommée en janvier 2024 par le Président de la République, et constituée d'experts issus de la « société civile » pour évaluer les enjeux attachés à l'exposition des enfants aux écrans et formuler des recommandations.

(2) Selon les chiffres communiqués par l'« Office mineurs » (OFMIN), le nombre de signalements de sextorsion réalisés par les plateformes est passé de 1174 en 2022 à 12000 en 2023, puis à 28767 en 2024. Par ailleurs, entre 2023 et 2024, l'association e-Enfance a reçu trois fois plus de sollicitations dont une grande part est liée au partage non consenti de contenu intime, à la sextorsion, au sexting et autres atteintes à l'intimité en ligne.

(3) Ministère de l'intérieur, rapport annuel sur la cybercriminalité 2024, p. 27.

(4) Au sens du règlement de l'UE relatif à l'intelligence artificielle, un deepfake, parfois aussi appelé « hypertrucage », est une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques.

(5) L'une de ces pratiques, couramment appelée « dick pic », consiste à envoyer une photo d'un sexe masculin sans le consentement du destinataire.

(6) Le « grooming » désigne une stratégie menée par une personne majeure envers une personne mineure, dont l'objectif est de créer un lien de confiance et émotionnel permettant à terme au majeur·e de faire des propositions sexuelles et, souvent, d'abuser sexuellement du ou de la mineur·e.

(7) Les violences s'entendent ici d'agissements qui peuvent causer une atteinte non seulement à l'intégrité physique mais également psychologique de la personne. Les violences sexistes et sexuelles sont couramment désignées par l'acronyme VSS. On parle aussi parfois de « violences de genre » (« gender-based violence »). Voir not : CEDAW, Recommandations générales adoptées par le Comité pour l'élimination de la discrimination à l'égard des femmes, Recommandation générale nº 19 : Violence à l'égard des femmes, 11e session (1992).

(8) Nations unies, Assemblée générale, 11 novembre 2024 :
https://documents.un.org/doc/undoc/ltd/n24/340/34/pdf/n2434034.pdf

Pour rappel, tous les deux ans, la France et les Pays-Bas présentent à l'Assemblée générale des Nations Unies (AGNU) une résolution intitulée « Intensification des efforts pour prévenir et éliminer les violences faites aux femmes et aux filles ». Dans ce cadre, cette résolution axée sur les violences commises dans l'environnement numérique a été présentée à l'occasion de la 79e session de l'AGNU, qui a débuté en septembre 2024.

(9) Loi nº 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

(10) Création de l'article 226-8-1 sur les deepfakes à caractère sexuel et modification de l'article 312-10 sur la sextorsion en ligne.

(11) *Cf.* infra.

(12) Art. L 312-9 du code de l'éducation.

(13) 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 (règlement sur les services numériques), *JO*RF nº 277 du 27.10.2022.

(14) D'après l'étude online réalisée par l'institut Audirep en mai 2024 pour l'Association e-Enfance/3018, 67% des 6-10 ans sont inscrits sur un réseau social en France. https://e-enfance.org/wp-content/uploads/2024/09/FINAL-INFOGRAPHIE-AUDIREP.pdf

(15) https://www.internetsanscrainte.fr/

(16) https://www.pointdecontact.net/

(17) https://e-enfance.org/

(18) CNCDH, Avis relatif à la proposition de loi visant à lutter contre la haine sur internet (A-2019-1), *JO*RF nº 0161 du 13 juillet 2019, texte nº 107 ; Avis relatif à la lutte contre la haine en ligne (A-2021-9), *JO*RF nº 0170 du 24 juillet 2021, texte nº 79.

(19) *Cf.* infra.

(20) Les clubs sportifs, les centres de loisir, les MJC, les bibliothèques, les services hospitaliers, etc.

(21) CNCDH, avis relatif à la lutte contre la haine en ligne (A-2021-9), *JO*RF nº 0170 du 24 juillet 2021, texte nº 79.

(22) Les outils et les spots de la campagne sont disponibles ici : https://www.arcom.fr/actualites/campagne-enfants-et-ecrans-2024-les-bons-usages-des-ecrans-pour-nos-enfants

(23) Article L. 312-16 du code de l'éducation.

(24) CESE, « Éduquer à la vie affective, relationnelle et sexuelle », 2024

(25) Les compétences psychosociales recouvrent *« un ensemble cohérent et interrelié de capacités psychologiques (cognitives, émotionnelles et sociales), impliquant des connaissances, des processus intrapsychiques et des comportements spécifiques, qui permettent d'augmenter l'autonomisation et le pouvoir d'agir (empowerment), de maintenir un état de bien-être psychique, de favoriser un fonctionnement individuel optimal et de développer des interactions constructives »* : Santé Publique France, « Les compétences psychosociales : état des connaissances scientifiques et théoriques », 2022.

(26) CNNum, « Éveil à la vie affective, relationnelle et sexuelle : donner le pouvoir d'agir », Septembre 2024.

(27) Rapport du CNNum, p. 8.

(28) Le CNNum pointe aussi le fait que ces contenus propices à l'EVARS peuvent faire l'objet de signalements massifs par des internautes hostiles à l'EVARS.

(29) CNCDH, Avis relatif à la lutte contre la haine en ligne (A-2021-9), *JO*RF nº 0170 du 24 juillet 2021, Texte nº 79. Voir aussi le rapport de la mission « Enfants écrans », pp. 79-80.

(30) CNIL, délibération nº 2024-067 du 26 septembre 2024 portant avis sur un projet de référentiel de l'ARCOM relatif aux systèmes de vérification de l'âge mis en place pour l'accès à certains services permettant l'accès à des contenus pornographiques.

(31) Le site est accessible en de nombreuses langues, y compris le français : https://takeitdown.ncmec.org/fr/.

(32) Il convient d'insister ici à nouveau sur la nécessité de garantir la robustesse du système d'IA et du serveur dédié à la conservation des hashs, pour limiter les risques de manipulation par des acteurs malveillants.

(33) La liste des plateformes actuellement associées à *Take it down* est disponible sur le site : https://takeitdown.ncmec.org/fr/participants/ Elle inclut notamment : Facebook, Instagram, Snapchat, Tiktok, PornHub, Only fans, Youtube.

(34) 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) nº 300/2008, (UE) nº 167/2013, (UE) nº 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.

(35) Article consacré à l'atténuation des risques systémiques engendrés par les services proposés par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche.

(36) Art. 227-23 du code pénal.

(37) La CNCDH attire l'attention sur le fait que l'article 227-23 du code pénal vise des images à caractère « pornographique ». Or, dès lors que la Cour de cassation admet l'application de ce texte à la détention d'images d'enfants dénudés (voir not. : Cass. Crim., 18 octobre 2017, nº 16-85-398), le législateur pourrait profiter de cette révision pour substituer aussi le terme « sexuel » à celui de « pornographique ». Outre la jurisprudence de la Cour de cassation relative à cet article, une telle révision pourrait être justifiée par l'adoption récente de l'article 226-8-1 qui érige en infraction la diffusion de deepfakes « à caractère sexuel ».

(38) Ministère de la justice du Royaume-Uni, « *Government crackdown on explicit deepfakes* », Communiqué de presse du 7 janvier 2025 : https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes

(39) Directive (UE) 2024/1385 du Parlement européen et du Conseil du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique, JO L, 2024/1385, du 24.05.2024.

(40) Convention des Nations unies contre la cybercriminalité, adoptée le 24 décembre 2024 par la résolution A/RES/79/243.

(41) Proposition de règlement du Parlement Européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, 11 mai 2022, COM(2022) 209 final.