Étude juridique IRJS

MINEURS ET RÉSEAUX SOCIAUX

Novembre 2025

ÉTUDE DES DISPOSITIFS LÉGAUX RELATIFS À L'USAGE DES RÉSEAUX SOCIAUX PAR LES MINEURS

Analyse du cadre juridique existant, des enjeux et des évolutions en cours

Réalisée sous la direction de ***Célia ZOLYNSKI***

Professeure de droit à l'Ecole de droit de la Sorbonne, Université Paris 1 Panthéon Sorbonne, IRJS

En collaboration avec

Margaux DEBOSQUE-TRUBERT

Doctorante en droit à Université Paris 1 Panthéon Sorbonne, IRJS

Doriane RETTIG

Doctorante en droit à Université Paris 1 Panthéon Sorbonne, IRJS

Marylou LE ROY

Docteur en droit à l'Université Paris Saclay, Maîtresse de conférences à l'INU Champollion

Muriel Mc CRACKEN

Juriste en IP/IT/Data, Élève Avocate en Angleterre

Institut de Recherche Juridique de la Sorbonne André Tunc

DReDIS - Département de Recherche en Droit de l'Immatériel de la Sorbonne

UNIVERSITÉ PARIS 1 PANTHÉON SORBONNE

ÉCOLE DE DROIT DE LA SORBONNE

Ce travail a été financé par l'Anses dans le cadre d'une convention de recherche et développement (2023-CRD-07). Les conclusions développées dans ce rapport n'engagent que la responsabilité des auteurs.

TABLE DES MATIÈRES

PRINCIPALES ABRÉVIATIONS

al.	alinéa
art.	article
Arcep	Autorité de régulation des communications électroniques, des postes et de la distribution de la presse
Arcom	Autorité de régulation de la communication audiovisuelle et numérique
cf.	*confer*
CGU	Conditions générales d'utilisation
CJUE	Cour de justice de l'Union européenne
CNIL	Commission Nationale Informatique et Libertés
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DSA	Digital Services Act (Règlement sur les services numériques)
DMA	Digital Markets Act (Règlement sur les marchés numériques)
FTC	Federal Trade Commission
JAF	Juge aux affaires familiales
LCEN	Loi pour la confiance dans l'économie numérique
LIL	Loi Informatique et libertés
op. cit.	*opus citatum*
OSA	Online Safety Act
p.	page
PPO	principe du pays d'origine
PPV	plateforme de partage de vidéo
RGPD	Règlement général sur la protection des données
RIA	Règlement sur l'intelligence artificielle
TGP	Très grande plateforme en ligne
TGMR	Très grand moteur de recherche en ligne

SIA	Système d'intelligence artificielle
SMA	Services de médias audiovisuels
UE	Union européenne

SYNTHÈSE

La présente étude porte sur l'identification des dispositifs légaux relatifs à l'usage des services de réseaux sociaux par les mineurs consacrés en droit français et en droit de l'Union européenne, et analyse leur adéquation avec les pratiques comportant des risques sanitaires pour les utilisateurs âgés de 11 à 17 ans. L'analyse porte successivement sur les dispositions transversales encadrant les services de réseaux sociaux, puis sur les dispositions spécifiques visant diverses pratiques existantes et émergentes dès lors qu'elles sont sources de préjudice pour les mineurs, pour enfin envisager le cadre juridique relatif à la conception et à l'accès aux services de réseaux sociaux. Elle en apprécie la mise en œuvre, met en lumière leurs éventuelles limites et lacunes, présente diverses solutions retenues dans le cadre d'autres systèmes juridiques (Angleterre et Pays de Galles, Australie, Etats-Unis), puis formule plusieurs préconisations concernant l'évolution potentielle du cadre juridique et des politiques publiques afin d'assurer une meilleure protection des mineurs de 11 à 17 ans s'agissant de leurs usages de ces services. Pour ce faire, l'étude se fonde sur l'examen des textes en vigueur et de la jurisprudence, complétés des propositions de réformes en cours de discussion et pistes d'évolution envisagées tant dans le cadre de rapports produits par diverses institutions que de contributions académiques publiées sur le sujet ; elle s'appuie par ailleurs sur les entretiens réalisés avec différentes parties prenantes (académiques, représentants d'associations, d'opérateurs ainsi que d'autorités et d'institutions publiques).

La première partie dresse un état des lieux des dispositions transversales encadrant les usages des réseaux sociaux par les utilisateurs âgés de 11 à 17 ans. À cet égard, il convient de relever que les droits français et de l'Union européenne applicables aux réseaux sociaux, pionniers en ce domaine, sont composés d'un millefeuille de textes relevant de plusieurs branches du droit. Plusieurs dispositions récemment adoptées ont plus particulièrement pour objectif de mieux protéger les mineurs compte tenu de leur vulnérabilité, en renforçant la responsabilisation des services de réseaux sociaux et, dans une certaine mesure, les droits de leurs utilisateurs finaux.

Le Règlement sur les services numériques (DSA) du 19 octobre 2022, qui vise à assurer une plus grande sécurité des utilisateurs des services numériques, consacre différentes avancées en ce sens. Le texte impose aux opérateurs de fournir des informations adaptées aux mineurs en proposant des conditions générales d'utilisation aisément compréhensibles (article 14) et un système de gestion de plaintes et de signalements adéquat. Il interdit par ailleurs aux plateformes de présenter aux mineurs des publicités reposant sur le profilage (article 28.2) et contraint celles qui sont accessibles aux mineurs à mettre en place des "*mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sécurité et de sûreté des mineurs sur leur service*" (article 28), ce qui est précisé dans le cadre des lignes directrices publiées par la Commission européenne le 14 juillet 2025. De surcroît, les très grandes plateformes et moteurs de recherche doivent réaliser des analyses de risques et prendre des mesures pour les atténuer (articles 34 et 35) : ces acteurs doivent notamment évaluer si leurs services sont compréhensibles par un jeune public, s'ils exposent les mineurs à des contenus susceptibles de nuire à leur santé et à leur bien-être et si leur conception favorise des comportements addictifs ; pour limiter ces risques, ils sont tenus de mettre

en place des dispositifs tels que le contrôle parental, la vérification de l'âge et des outils permettant aux jeunes de signaler les abus et d'accéder à un soutien adapté.

Le DSA complète les textes précédemment adoptés, en particulier le Règlement général sur la protection des données (RGPD) du 27 avril 2016 qui encadre le traitement des données à caractère personnel notamment des mineurs. À ce titre, le RGPD impose l'adoption de conditions générales d'utilisation formulées dans des *"termes clairs et simples, que l'enfant peut aisément comprendre"* (article 12), et encourage les États membres, les autorités de contrôle ainsi que la Commission européenne à promouvoir l'adoption de codes de conduite afin d'harmoniser l'application des dispositions relatives aux mineurs (article 40). Le droit français précise ces dispositions en fixant l'âge du consentement pour le traitement des données personnelles (article 45 de la loi informatique et liberté) et en reconnaissant un droit à l'effacement des données renforcé pour les mineurs (article 51 de la loi informatique et liberté). Il convient également de mentionner la Directive sur les services de média audiovisuels (SMA) du 14 novembre 2018 qui contraint les plateformes, dont les réseaux sociaux, à mettre en place des mesures de lutte contre l'incitation à la haine et contre l'apologie du terrorisme. D'autres textes sont par ailleurs en cours de discussion, à l'image de la proposition de Règlement sur la prévention et la lutte contre les abus sexuels sur mineurs (CSAM) de mai 2022 qui vise à renforcer la lutte contre la pédocriminalité en ligne, ou sont actuellement envisagées, en particulier le Digital Fairness Act (DFA) qui pourrait compléter l'acquis afin de renforcer la protection des consommateurs notamment contre les interfaces trompeuses et la conception addictive des services numériques.

En parallèle, la Commission européenne a initié la stratégie *Better Internet For Kids* (BIK+) afin de promouvoir un "internet meilleur pour les enfants" en établissant un cadre souple fondé sur la sensibilisation et la coopération entre acteurs du secteur (gouvernements, ONG, services numériques) au travers les réseaux européens INSAFE (accompagnement des jeunes et des éducateurs dans la prévention des risques et la promotion des usages positifs d'Internet) et INHOPE (coordination des plateformes de signalement) qui rassemblent les réseaux partenaires existant au niveau national, les *Safer Internet Centres* (SIC). Le Safer Internet France est composé de trois partenaires : (1) *Internet sans crainte* - programme national d'éducation au numérique des jeunes et des familles opéré par Tralalère - propose des ressources de sensibilisation aux usages d'Internet s'adressant aux jeunes ainsi qu'aux parents, éducateurs et professionnels de l'éducation. (2) *Point de Contact* constitue le service de signalement de contenus illicites, traitant les signalements qui lui sont adressés par les internautes ainsi que les signalements transmis par ses homologues membres du réseau *INHOPE*. (3) Le *3018* est le numéro unique national opéré par l'association *e-Enfance* pour lutter contre les violences numériques, qui accompagne les jeunes et leurs parents à faire face à des contenus dangereux, indésirables ou offensants.

Le droit français s'est en outre enrichi de nouvelles dispositions qui attestent d'une forte volonté politique d'assurer une plus grande protection des mineurs en ligne. En témoignent notamment la loi du 2 mars 2022 imposant aux fabricants d'appareils connectés d'installer un dispositif de contrôle parental, la loi du 7 juillet 2023 fixant à 15 ans l'âge pour s'inscrire sur un réseau social (13 ans avec l'autorisation du représentant légal), la loi du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux ou encore la loi du 19 février 2024 visant à garantir le respect du droit à l'image des enfants. En dernier lieu, la loi

du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) entend renforcer la protection des utilisateurs des services numériques dont les réseaux sociaux, en particulier les mineurs en ligne, en consacrant par exemple des conditions d'accès tenant à l'âge pour les contenus à caractère pornographique, des incriminations relatives au partage non consenti de contenu intime et de sextorsion ainsi que la diffusion d'hyper trucages (*deepfakes*) à caractère sexuel ou encore en prévoyant des peines de bannissement des réseaux sociaux pour les cyberharceleurs en cas de récidive.

L'efficacité de ces différentes avancées reste toutefois difficile à évaluer à ce jour. Elle dépendra en grande partie de la mise en œuvre concrète de plusieurs dispositifs à l'image du respect de l'obligation de *Safety by design* à laquelle sont désormais soumises les plateformes envers les mineurs et de la régulation des risques systémiques imposée aux très grandes plateformes au titre du DSA. Elle supposera en outre un renforcement des moyens des différents services d'accompagnement des jeunes dans leurs usages en ligne, dont l'association *e-Enfance/3018*, désignée pour la France premier signaleur de confiance au titre du DSA, ainsi que des enquêteurs et magistrats.

Dans une deuxième partie, l'étude s'attache à analyser les pratiques en ligne présentant un risque sanitaire pour les mineurs de 11 à 17 ans, en détaillant les préjudices spécifiques qui en découlent et les solutions juridiques retenues afin de s'en prémunir.

Les mineurs peuvent être exposés à plusieurs formes de cyberviolence, dont le cyberharcèlement qui peut se traduire par divers comportements répétés à l'égard des victimes tels que l'envoi de messages de haine, moqueries et injures, la divulgation de données personnelles (*doxing*), etc. Ils peuvent également être exposés à différentes atteintes à leur intimité en ligne. Les abus de contenus intimes constituent plus spécifiquement une pratique susceptible de générer d'importants effets dommageables notamment pour les jeunes filles en cas de diffusion non consentie d'images intimes, souvent obtenues dans un cadre privé puis partagées publiquement ou en message privé, sans l'accord de la victime. Les jeunes utilisateurs peuvent aussi être victimes de chantage et d'exploitation sexuelle en ligne, notamment au moyen de sextorsion, c'est-à-dire une tentative d'extorsion d'argent ou de faveurs sexuelles sous la menace de divulguer des images intimes les représentant. Le *grooming* constitue plus généralement un risque majeur dès lors que cette pratique repose sur des stratégies de manipulation menées par une personne majeure en créant un lien de confiance avec une personne mineure en vue d'obtenir de sa part des faveurs sexuelles. Ces différentes pratiques prennent désormais une ampleur particulière, comme en atteste le nombre croissant de signalements de cas de sextorsion (selon les chiffres de l'OFMIN : 1400 en 2022, 12 000 en 2023, 28 767 en 2024). Cette augmentation peut en partie s'expliquer par la démocratisation des systèmes d'intelligence artificielle générative dès lors que ces derniers facilitent la génération de contenus inauthentiques (par exemple, la technologie *deepfake* peut être utilisée pour générer des vidéos ou images truquées à caractère sexuel), possiblement en nombre, et ce sans nécessiter ni budget ni compétence technique importants, y compris en utilisant des applications de dénudage aisément accessibles à tous depuis les moteurs de recherche ou magasins d'applications. Pour chacune de ces pratiques, l'étude revient sur la définition retenue, le cadre juridique existant, en identifie les possibles limites et formule dans ce cas des propositions d'évolution. Quant au cyberharcèlement, il est ainsi proposé d'améliorer la prise en charge, la gestion et l'engagement

des poursuites concernant les plaintes déposées, de retenir une définition des infractions plus protectrice des victimes que celle actuellement consacrée par le Code pénal, d'évaluer l'incidence des sanctions ou encore d'améliorer l'accessibilité et l'efficacité de la modération des contenus. Concernant les atteintes à l'intimité, s'il convient de saluer les récentes évolutions du cadre légal notamment consacrées par le DSA et en France par la loi SREN, il paraît important de compléter les dispositifs existants pour renforcer la protection des mineurs. Il s'agirait ainsi de favoriser le signalement de ces atteintes par les victimes et de renforcer la réponse pénale pour sanctionner plus efficacement leurs auteurs, notamment en prohibant non seulement la diffusion mais également la création de deepfakes à caractère sexuel représentant un mineur, ou encore en prévoyant une aggravation de la peine en cas de sextorsion sur mineurs. En outre, il paraît essentiel de mieux prévenir ce type d'atteinte. À cette fin, il est proposé de conduire des campagnes de sensibilisation massive sur le sujet ainsi que de renforcer les dispositifs de responsabilisation des opérateurs déjà prévus au titre du DSA. Afin de lutter contre la sextorsion et le grooming, il est essentiel de leur imposer d'assurer un meilleur accompagnement des mineurs dans le paramétrage de leurs comptes, y compris en retenant un paramétrage par défaut plus sûr pour empêcher les inconnus d'interagir avec eux.

Sont également envisagées les pratiques des mineurs en ligne les conduisant, de manière plus ou moins volontaire, à être exposés à des contenus choquants ou incitant à des conduites à risque. Le cadre répressif paraît alors assez complet, sous réserve de son effectivité et surtout d'une nécessaire sensibilisation des jeunes. Certains types de contenus appellent cependant une attention particulière dès lors qu'ils sont susceptibles d'affecter la perception de soi, en ce qu'ils promeuvent les troubles du comportement alimentaire, l'automutilation voire le suicide. Le droit pénal ne saisit que la provocation au suicide ou la propagande en faveur de moyens de se donner la mort ; les autres contenus ne sont pas prohibés en soi et il incombe aux réseaux sociaux de les réguler au titre du DSA. Ceci pourrait supposer une modification de leurs systèmes de recommandation et un renforcement de la faculté de paramétrage des utilisateurs, assortis d'un effort national de sensibilisation aux troubles de la santé mentale.

Enfin, l'étude s'attache aux variations de ces pratiques selon les caractéristiques de l'utilisateur mineur, dans la mesure où son appartenance à certains groupes protégés emporte des pratiques ou des risques propres. Sont particulièrement développés le genre, l'orientation sexuelle et l'identité de genre, la situation de handicap, ainsi que la diversité ethnique, culturelle, linguistique ou religieuse. À cet égard, il convient de souligner qu'une réglementation optimale des réseaux sociaux nécessiterait une meilleure prise en compte de ces caractéristiques, y compris à travers des efforts de sensibilisation ciblés. Cela suppose notamment de s'assurer de l'accessibilité, pour les mineurs en situation de handicap et les mineurs allophones, des dispositifs de soutien et de signalement et, s'agissant en particulier des jeunes LGBTQ+, de veiller à ce que la recherche légitime d'une plus grande sécurité en ligne ne conduise pas à l'impossibilité de tout anonymat ou à l'invisibilisation indue de contenus pourtant essentiels à la formation et à la représentation de cette communauté.

La troisième partie de l'étude porte sur la conception et les conditions d'accès aux services, pour envisager les évolutions du cadre juridique en ce domaine.

Concernant la conception des services, la réglementation existante interdisant aux réseaux sociaux d'exposer leurs utilisateurs à des interfaces trompeuses et manipulatrices doit être prolongée par une appréhension juridique des conceptions addictives. Certains services sont en effet conçus pour amplifier la captation de l'attention des utilisateurs, jusqu'à susciter une forme de dépendance comportementale. Par-delà l'atténuation des risques imposée aux très grandes plateformes en ligne et l'obligation de *Safety by design* imposée aux plateformes accessibles aux mineurs par le DSA, il paraît dès lors nécessaire d'envisager l'interdiction de certaines fonctionnalités préjudiciables telles que le défilement infini, la lecture automatique par défaut ou les notifications incessantes ; il est en outre urgent de conduire des études approfondies sur l'impact des algorithmes de recommandation ultra personnalisés qui exposent les mineurs à des spirales de contenus ainsi que sur d'autres conceptions favorisant l'adoption de comportements répétitifs en ce que ces pratiques sont potentiellement toxiques pour leur santé, et d'évaluer la nécessité de réviser le cadre juridique existant pour mieux protéger les utilisateurs vulnérables tels que les mineurs. Au-delà, il convient de promouvoir une conception éthique des réseaux sociaux, assortie de la consécration d'un droit au paramétrage au bénéfice de l'utilisateur et de la poursuite des réflexions relatives au pluralisme algorithmique.

Dans la mesure où la vérification de l'âge est généralement présentée comme un enjeu majeur en ce qui concerne la protection des mineurs en ligne, le cadre légal a progressivement été complété afin d'imposer de nouvelles obligations aux plateformes. La mise en œuvre d'un tel dispositif soulève néanmoins d'importantes difficultés qui en limitent l'effectivité, notamment en raison de la marge de manœuvre accordée aux plateformes, des risques d'atteintes aux droits fondamentaux des utilisateurs, ou encore de disparité des procédés en l'absence d'harmonisation au niveau européen, auxquels s'ajoute le possible contournement de ces mesures par les mineurs.

L'étude envisage également les enjeux relatifs au contrôle parental en ce qu'il vise à restreindre l'accès des jeunes à des contenus inappropriés. Elle revient sur ses modalités (création de profils "parents", restriction des contenus, gestion du temps d'écran, etc.) ainsi que sur les limites existantes alors que, depuis 2025, la loi impose l'intégration obligatoire de ces outils dès la fabrication d'un appareil connecté. Elle rappelle à cet égard les débats suscités par sa mise en œuvre, notamment concernant la protection des données à caractère personnel, pour souligner la nécessité d'évaluer l'effectivité des solutions disponibles, d'en garantir la diversité ainsi que d'assurer l'accompagnement des parents pour les informer et les former quant à leur utilisation. Plus généralement, elle relève l'importance de promouvoir un dialogue parents-enfants concernant les usages numériques.

Compte tenu des risques identifiés et afin de renforcer la protection des mineurs de 11 à 17 ans, la dernière partie de l'étude présente un ensemble de préconisations générales s'articulant autour de plusieurs axes.

Si le cadre juridique semble relativement complet, il convient de constater un manque d'effectivité de plusieurs mesures consacrées en raison de l'insuffisance de moyens humains et techniques mis en œuvre pour protéger les mineurs victimes de pratiques préjudiciables sur les réseaux sociaux. L'étude recommande par conséquent de renforcer les moyens de la justice, des autorités publiques compétentes et des associations, et de prêter une attention particulière à la formation des acteurs, notamment en publiant des guides pratiques pour les magistrats et les forces de l'ordre. Il est

également recommandé d'impliquer les mineurs dans la mise en œuvre de ces dispositifs, sur le modèle du eSafety Youth Council existant en Australie, afin de garantir un encadrement et un accompagnement adapté à leurs pratiques et faire des enfants les acteurs de la protection de leurs droits.

Par ailleurs, il est recommandé (1) d'instituer un dispositif de suivi transversal de la mise en œuvre du DSA impliquant les représentants des différentes autorités de régulation concernées, services ministériels et experts du sujet, dont les académiques et les magistrats, (2) de favoriser la diffusion de bonnes pratiques notamment proposées par la société civile, ou encore (3) d'assurer le prononcé de sanctions efficaces en cas de pratiques préjudiciables.

Afin de s'assurer de la prise en compte des pratiques émergentes, il est également recommandé de mettre en place un système de veille agile permettant d'en évaluer et/ou d'anticiper les impacts, en conduisant des études prospectives pour anticiper au mieux ces évolutions. À cette fin, il conviendrait d'y associer les enfants pour une meilleure gouvernance anticipative, et de s'assurer de l'existence d'un réseau au niveau de l'Union européenne pour déterminer et faire évoluer de façon réactive les priorités de la Commission européenne dans le cadre de la mise en œuvre du DSA, en s'appuyant en particulier sur les Safer Internet Centres. Plus généralement, il paraît essentiel d'assurer un suivi de l'incidence de la transformation numérique sur le bien-être des enfants.

En outre, il convient de renforcer l'information, la formation et l'accompagnement des victimes notamment en réalisant des campagnes de sensibilisation au sein et hors du milieu scolaire pensées de façon adaptée.

De surcroît, il semble important de renforcer les actions au niveau collectif en soutenant les actions menées par la société civile, ce qui suppose (1) d'augmenter les moyens alloués aux associations reconnues comme bénéficiant d'une expertise forte dans la lutte contre les violences sur mineurs en ligne et (2) de mettre en place une réserve citoyenne permettant de mobiliser l'ensemble des parties prenantes, sur le modèle proposé dans le cadre du Conseil National de la refondation numérique

Au-delà, il paraît urgent de reconnaître la lutte contre les comportements en lien avec les abus sexuels d'enfants en tant que priorité nationale, en renforçant notamment les moyens d'action contre la diffusion de deepfakes à caractère sexuel et en menant des actions de sensibilisation de grande envergure concernant ces pratiques à destination des enfants et des adultes.

I. INTRODUCTION

I. OBJECTIFS DE L'ÉTUDE

La présente étude vise à :

- décrire le cadre juridique applicable aux usages des réseaux sociaux par les utilisateurs mineurs âgés de 11 à 17 ans, en envisageant les dispositions transversales ainsi que celles visant en particulier les pratiques existantes et émergentes préjudiciables pour les mineurs ;
- en identifier les limites et lacunes éventuelles ;
- réaliser une étude de droit comparé à l'aune des systèmes juridiques de l'Angleterre et du Pays de Galles, de l'Australie et des Etats-Unis afin d'identifier de bonnes pratiques ; les dispositifs retenus par le droit fédéral américain seront envisagés dès lors qu'ils inspirent la plupart des politiques des grands réseaux sociaux, ainsi que les réformes et mécanismes adoptés au Royaume-Uni et en Australie, lesquels portent depuis quelques années diverses initiatives novatrices afin de protéger ce jeune public.
- fort de ces analyses, proposer des recommandations afin de faire évoluer le cadre juridique ainsi que les politiques publiques en ce domaine en s'inscrivant dans le cadre d'une approche holistique visant non seulement à mieux protéger l'utilisateur mineur en lui garantissant de pouvoir interagir avec/via des environnements sûrs mais également à lui permettre de bénéficier de ces environnements conformément son intérêt et de préserver ses libertés fondamentales, notamment sa liberté d'expression.

II. DÉFINITIONS

- **Mineurs** :

Le premier alinéa de l'article 388 du Code civil définit le mineur comme « *l'individu de l'un ou l'autre sexe qui n'a point encore l'âge de dix-huit ans accomplis* ».

La présente étude porte sur les mineurs de plus de 11 ans et jusqu'à 18 ans, soit principalement les adolescents[1]. Il convient toutefois de relever que les pratiques numériques des jeunes sont massives et de plus en plus précoces[2]. Ceci contribue à exposer ces très jeunes utilisateurs d'autant plus vulnérables à des pratiques préjudiciables, y compris de nature sexuelle.

[1] Une enquête de Génération Numérique sur les pratiques numériques des jeunes réalisée en ligne du 01 septembre 2023 au 24 janvier 2024 auprès de 8719 jeunes de 11 à 18 ans, a révélé que 59% des 11-14 ans et 95% des 15-18 ans étaient inscrits à un ou plusieurs réseaux sociaux : Génération numérique, Enquête sur les pratiques numériques des 11 à 18 ans, janvier 2024.

[2] Une étude de l'Arcom estime à 99% des 11 - 17 ans utilisent au moins une plateforme en ligne : Arcom, Protection des mineurs en ligne : étude quantitative, septembre 2025.

- **Réseaux sociaux :**

Le Règlement sur les marchés numériques définit les réseaux sociaux comme toute "*plateforme permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations*"[3].

Dans son étude annuelle de 2022, le Conseil d'Etat relevait par ailleurs "*la grande diversité des réseaux sociaux comme leur caractère protéiforme (plus ou moins publics, à usage professionnel ou de loisir, faisant des discussions ou échanges de contenus une fonctionnalité principale ou accessoire, etc.)"* et ainsi que « *les différences avec d'autres notions, comme celle de médias sociaux ou de messageries, sont faibles voire inexistantes"*. Le Conseil d'Etat soulignant ainsi l'opportunité d'en retenir une définition large, dans un souci de pragmatisme, "*compte tenu de la diversité des réseaux sociaux et du phénomène d'hybridation des plateformes (d'un côté, les réseaux sociaux s'ouvrent à l'activité purement commerciale des marketplaces et, d'un autre côté, les plateformes de vente de services en ligne permettent la discussion entre internautes sur leurs sites)"*[4]. La présente étude s'inscrit dans le prolongement de cette étude en retenant une définition élargie des réseaux sociaux.

III. MÉTHODOLOGIE

La présente étude porte sur l'identification des dispositifs légaux relatifs à l'usage des services de réseaux sociaux par les mineurs et l'analyse de leur adéquation avec les pratiques identifiées comme comportant des risques sanitaires pour les utilisateurs des réseaux sociaux âgés de 11 à 17 ans.

À cette fin, l'étude a été conduite comme suit :

- **première phase** : analyse des principaux textes juridiques en droit français et en droit de l'Union européenne visant à réguler l'usage des réseaux sociaux numériques pour les mineurs en France et à l'échelle européenne, ainsi que les évolutions à venir, notamment dans le cadre de la mise en œuvre du DSA ;
- **deuxième phase** : analyse du traitement juridique de questions spécifiques relatives à l'impact de la conception et de l'usage des réseaux sociaux pour les utilisateurs mineurs âgés de 11 à 17 ans. Ces points saillants ont été identifiés à travers les pratiques des usagers ou des plateformes numériques, pouvant être liées, de façon directe ou indirecte, à l'émergence d'effets sur la santé ;
- **troisième phase :** étude des propositions et des controverses ;
- **quatrième phase :** étude des solutions de droit comparé (Etats-Unis, Australie, Royaume-

[3] Règlement 2022/1925 sur les marchés numériques du 14 septembre 2022, article 2, 7).

[4] Conseil d'Etat, *Les réseaux sociaux : enjeux et opportunités pour la puissance publique*, Etude annuelle pour 2022, p. 11.

Uni) afin d'envisager leur possible transposition en droit français et de l'Union européenne.
- **cinquième phase :** formulation de préconisations quant à l'évolution du cadre légal en droit de l'Union européenne et du droit français.

Afin de nourrir ces différentes analyses, l'étude se fonde sur l'examen des textes en vigueur et de la jurisprudence, complétés des propositions de réformes en cours de discussion et pistes d'évolution envisagées tant dans le cadre de rapports produits par diverses institutions que de contributions académiques publiées sur le sujet ainsi que sur plusieurs entretiens réalisés avec les parties prenantes (académiques, représentants d'associations, d'opérateurs ainsi que d'autorités et d'institutions publiques - v. la liste en annexe).

IV. PLAN DE L'ÉTUDE

La présente étude est divisée en quatre parties. La première partie (*Dispositions transversales*) propose une présentation des principaux textes juridiques applicables concernant la protection des mineurs sur les réseaux sociaux. Ensuite, la deuxième partie (*Pratiques en ligne*) recense et définit les principales pratiques préjudiciables pour les utilisateurs des réseaux sociaux âgés de 11 à 17 ans ainsi que le cadre juridique applicable. La troisième partie (*Encadrement de la conception des services*) propose une étude de l'encadrement de la conception des services, les conditions d'accès tenant à l'âge et les mesures de contrôle parental. Enfin, la quatrième partie (*Préconisations générales*) recense les préconisations générales identifiées à l'issue de cette étude afin de mieux protéger et mettre en capacité d'agir les mineurs sur les réseaux sociaux.

II. DISPOSITIONS TRANSVERSALES

Une présentation des dispositions transversales applicables à l'utilisation des réseaux sociaux par les mineurs de 11 à 17 ans suppose tout d'abord de dresser un panorama de l'état du droit français et le droit de l'Union européenne (**Chapitre 1**) puis de présenter la stratégie européenne de la protection des mineurs en ligne (**Chapitre 2**).

CHAPITRE 1 : PANORAMA DES TEXTES DE DROIT EUROPÉEN ET FRANÇAIS APPLICABLES AUX RÉSEAUX SOCIAUX

Il faut d'emblée souligner que les droits français et européen applicables aux réseaux sociaux lorsque les utilisateurs sont mineurs sont relativement pionniers et sont composés d'un millefeuille de textes applicables en ce domaine[5]. Cet arsenal législatif comporte des textes relevant de plusieurs branches du droit applicables hors ligne comme en ligne. Il contient également des dispositions spécifiques au numérique. Les mineurs sont en effet considérés comme des utilisateurs considérés comme vulnérables, ce qui nécessite une protection accrue par le droit. À cet égard, le principe cardinal du droit de l'Union européenne concernant les droits de l'enfant est l'article 24 de la Charte des droits fondamentaux de l'Union européenne qui énonce que :

"*Les enfants ont droit à la protection et aux soins nécessaires à leur bien-être. Ils peuvent exprimer leur opinion librement. Celle-ci est prise en considération pour les sujets qui les concernent, en fonction de leur âge et de leur maturité.*

2. Dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale.

3. Tout enfant a le droit d'entretenir régulièrement des relations personnelles et des contacts directs avec ses deux parents, sauf si cela est contraire à son intérêt."

1.1. PANORAMA DES TEXTES AU NIVEAU EUROPÉEN

Une nouvelle stratégie européenne intitulée « Pour un internet mieux adapté aux enfants » a été présentée en mai 2022. Cette stratégie constitue le volet numérique de la stratégie globale de l'UE

[5] Pour une étude du droit applicable aux réseaux sociaux, v. Conseil d'Etat, *Les réseaux sociaux : enjeux et opportunités pour la puissance publique*, Etude annuelle pour 2022, p. 52 et s.

sur les droits de l'enfant adoptée par la Commission européenne[6]. Il est notamment prévu un principe directeur selon lequel "*les enfants et les jeunes devraient être protégés en ligne et formés à cet environnement*"[7]. La déclaration européenne sur les droits et principes numériques pour la décennie numérique, certes de nature non contraignante, indique que "*les enfants et les jeunes devraient être formés à l'environnement numérique afin d'y faire des choix sûrs, en connaissance de cause, et d'y exprimer leur créativité. Des contenus et services adaptés à chaque âge devraient améliorer l'expérience, le bien-être et la participation des enfants et des jeunes dans l'environnement numérique. Il convient d'accorder une attention particulière au droit des enfants et des jeunes d'être protégés contre toute forme de criminalité, commise ou facilitée par les technologies numériques"*[8].

Dans sa résolution du 24 avril 2024, la Commission européenne rappelle notamment que « *les enfants doivent bénéficier d'une protection contre des menaces telles que le (cyber)harcèlement dans l'environnement tant physique que numérique, ainsi que le souligne notamment le Conseil, dans ses conclusions sur l'autonomisation numérique pour protéger et faire respecter les droits fondamentaux à l'ère numérique*[9] *et sur le soutien au bien-être dans l'éducation numérique*[10]*. La nouvelle stratégie pour un internet mieux adapté aux enfants*[11] *vise à faire en sorte que les enfants soient protégés et respectés et disposent de moyens d'agir en ligne au cours de la nouvelle décennie numérique, tandis que la protection des mineurs constitue une préoccupation majeure au sein du cadre législatif et politique, comme le règlement sur les services numériques, la directive sur les services de médias audiovisuels, le règlement général sur la protection des données et l'initiative de l'UE sur le web 4.0 et les mondes virtuels* ».

Plusieurs textes du droit de l'Union européenne comportent des dispositions applicables aux réseaux sociaux lorsqu'ils sont utilisés par les mineurs[12] :

[6] Communication de la Commission, Stratégie de l'UE sur les droits de l'enfant, COM(2021)142 final, mars 2021. Sur l'ensemble des stratégies, v. Commission européenne, Nouvelle stratégie pour un internet mieux adapté aux enfants (BIK +). Recueil des textes officiels de l'UE concernant les enfants dans le monde, mai 2024.

[7] Ibid.

[8] Déclaration européenne sur les droits et principes numériques pour la décennie numérique, 2023/C 23/01, pt. 20 à 22, 23 janvier 2023.

[9] Conclusions du Conseil sur l'autonomisation numérique pour protéger et faire respecter les droits fondamentaux à l'ère numérique, 14309/23, 20 octobre 2023.

[10] Conclusions du Conseil sur le soutien au bien-être dans l'éducation numérique, 14982/22, 28 novembre 2022.

[11] Communication de la Commission intitulée « Une décennie numérique pour les enfants et les jeunes : la nouvelle stratégie européenne pour un internet mieux adapté aux enfants », COM(2022) 212 final.

[12] Pour une présentation de l'ensemble des textes en droit de l'Union, v. notamment Commission européenne, Nouvelle stratégie pour un internet mieux adapté aux enfants (BIK +), préc.

L'un des textes fondateurs est la **Directive du 8 juin 2000 pour le commerce électronique**[13] transposée par la loi pour la confiance dans l'économie numérique datée de juin 2004[14] qui instaure une distinction notamment entre, d'une part, les éditeurs de contenus soumis à **une obligation de résultat** et chargés de faire en sorte que les mineurs n'accèdent pas à des contenus préjudiciables et, d'autre part, **les hébergeurs dont font partie les réseaux sociaux qui n'ont aucune obligation de surveillance des contenus** et qui n'engagent pas leur responsabilité s'ils ne sont pas à l'origine des contenus illicites et s'ils les retirent promptement dès lors qu'ils ont connaissance de leur caractère illicite. Ce texte a été abrogé par le Règlement sur les services numériques (DSA - v. infra).

L'entrée en application du **Règlement général sur la protection des données** (RGPD)[15] en 2018 a introduit des dispositions spécifiques aux mineurs. Elles prévoient en particulier l'exigence d'une information adaptée, le renforcement de leur droit à l'oubli et une capacité à consentir, sous certaines conditions, au traitement de leurs données (seuls au-delà de 15 ans ou avec leurs parents avant cet âge). Elles appellent également à une vigilance particulière à l'égard du profilage des mineurs.

Ces textes ont toutefois suscité certaines interrogations et un besoin de clarification, notamment pour préciser leurs implications pratiques et leur articulation avec le droit national, en particulier le droit des contrats et de la famille. En particulier, l'article 12 du RGPD indique que toute information et communication concernant le traitement de données personnelles des enfants devraient être rédigées en des *« termes clairs et simples, que l'enfant peut aisément comprendre »*. Les États-membres, les autorités de contrôle, le Comité européen de la protection des données (CEPD) et la Commission européenne sont également invités à encourager l'adoption de codes de conduite pour harmoniser les applications des dispositions relatives aux mineurs (article 40 du RGPD).

Il convient de relever, s'agissant du droit français, que l'article 45 de la Loi relative à l'informatique, aux fichiers et aux libertés de 1978 (loi dite LIL)[16] fixe à 15 ans l'âge de la prise en compte du consentement seul du mineur pour la France pour le traitement de ses données à caractère personnel. Le ou les titulaires de l'autorité parentale doivent donner leur accord conjointement avec celui de leur enfant si celui-ci a moins de 15 ans. L'article 51-II de la LIL prévoit par ailleurs un droit à l'effacement spécifique qui prévoit "*qu'en particulier sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais*

[13] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), Journal officiel n° L 178 du 17/07/2000 p. 0001 - 0016.

[14] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1).

[15] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), OJ L 119, 4.5.2016, p. 1–88.

[16] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte".

La **Directive sur les services de médias audiovisuels** (Directive dite SMA) de 2018[17] prévoit une application de certaines dispositions aux plateformes de partage de vidéos et aux réseaux sociaux, ainsi qu'à la diffusion en direct (*livestreaming*). Ces acteurs devront alors mettre en place des mesures spécifiques, notamment en matière de protection des mineurs, de lutte contre l'incitation à la haine et de lutte contre l'apologie du terrorisme. Premièrement, les contenus « *les plus préjudiciables* » (pornographie et violence gratuite) seront soumis aux mesures les plus strictes. Deuxièmement, les éditeurs devront fournir une information sur la nature du contenu qui justifie une signalétique relative à l'âge. Enfin, les données personnelles des mineurs collectées par les entreprises via les systèmes de protection mis en place ne peuvent être utilisées à des fins commerciales.

Le Règlement sur les services numériques (DSA)[18] de 2022 fait de la protection des mineurs "*un objectif stratégique important de l'Union*". Différentes dispositions du texte poursuivent cet objectif[19].

Le Règlement sur l'intelligence artificielle (RIA) de 2024[20] met l'accent sur la protection des groupes vulnérables interagissant avec les systèmes d'intelligence artificielle (SIA), en particulier les mineurs. Plusieurs points relatifs à la protection des mineurs peuvent être mentionnés.

Tout d'abord, le texte vise la reconnaissance et la primauté des droits de l'enfant. Le texte final reconnaît explicitement les enfants comme un groupe vulnérable méritant une protection et des soins appropriés nécessaires à leur bien-être (considérants 28 et 48). L'article 24 de la Charte des droits fondamentaux de l'Union européenne et la convention des Nations unies relative aux droits de l'enfant (et précisés dans l'observation générale n° 25 de la CNUDE en ce qui concerne l'environnement numérique sont cités comme des références établissent un cadre pour la protection de l'enfance face aux SIA. Il s'agit d'une amélioration par rapport à la version initiale

[17] Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, PE/33/2018/REV/1.

[18] 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).

[19] V. infra, chapitre 2.

[20] 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). Voir également : N. Patti, Children's Vulnerability in the EU AI Act, SOBIGDATA Research Infrastructure, 2024 ; S. Lindroos-Hovinheimo, Children and the Artificial Intelligence Act: Is the EU Legislator Doing Enough?, European Law Blog, 2024.

du texte davantage axée sur la sécurité des produits qu'orientée vers la protection des droits fondamentaux.

En outre, le RIA consacre l'interdiction de la mise sur le marché, la mise en service ou l'utilisation de certains SIA considérés comme des risques inacceptables. Son article 5 paragraphe 1 vise à interdire certaines pratiques en matière d'IA en particulier celles qui ont recours à "*des techniques subliminales, au-dessous du seuil de conscience d'une personne, ou à des techniques délibérément manipulatrices ou trompeuses*" (point a) ou encore qui exploitent "*les éventuelles vulnérabilités dues à l'âge*" dès lors que ces pratiques ont "*pour objectif ou effet d'altérer substantiellement le comportement de cette personne*". Seront aussi interdites les SIA visant à inférer les émotions de personnes physiques dans les établissements d'enseignement "*sauf lorsque l'utilisation du système d'IA est destinée à être mise en place ou mise sur le marché pour des raisons médicales ou de sécurité*" (article 5, paragraphe 1, f).

Par ailleurs, le RIA reconnaît la qualification de "haut risque" aux SIA dans l'éducation et la formation professionnelle. Les SIA destinés à être utilisés dans les établissements d'enseignement et de formation professionnelle sont classés comme à haut risque selon l'annexe III et doivent être soumis à des dispositions et une surveillance accrues. Par exemple, un système de gestion des risques doit être mise en place en ce qui concerne les SIA à haut risque et il doit être pris "*en considération la probabilité que, compte tenu de sa destination, le système d'IA à haut risque puisse avoir une incidence négative sur des personnes âgées de moins de 18 ans*" (article 9, 9).

Le RIA consacre également des exigences de transparence pour les SIA génératives. A ce titre, le texte exige que les SIA destinés à interagir avec des personnes ou à générer des contenus doivent être soumis à des obligations de transparence spécifiques et que les personnes soient avisées qu'elles interagissent avec un SIA ou que les contenus générés à l'aide de SIA y compris les deepfakes soient clairement soient soumises à une obligation de marquage. Dans les deux cas, il doit être tenu compte des caractéristiques des personnes physiques appartenant à des groupes vulnérables y compris en raison de leur âge (article 50 et considérants 132, 133, 134).

Il convient aussi de souligner que le RIA consacre des mécanismes de surveillance, de conformité continus et de mise à jour. Ainsi, le règlement établit des mécanismes d'évaluation et d'application continue pour garantir le respect des réglementations et atténuer les impacts négatifs sur les personnes vulnérables. L'article 7 prévoit que l'annexe III listant les SIA à haut risque peut être modifiée par la Commission européenne avec des actes délégués en y ajoutant ou modifiant des cas d'utilisation de SIA à haut risque. L'article 7(h) intègre la vulnérabilité comme facteur de mise à jour de la liste des SIA à haut risque, notamment en raison de l'âge. L'article 27 du RIA impose une analyse d'impact des systèmes d'IA à haut risque sur les droits fondamentaux. L'article 60 prévoit que des essais de systèmes d'IA à haut risque doivent être mis en place en conditions réelles en dehors des bacs à sable réglementaires de l'IA notamment si "*les participants aux essais en conditions réelles qui sont des personnes appartenant à des groupes vulnérables en raison de leur âge ou de leur handicap sont dûment protégées*" (article 60, g). L'article 79 concerne la procédure applicable au niveau national aux systèmes d'IA présentant un risque notamment avec "*une attention particulière est accordée aux systèmes d'IA présentant un risque pour les groupes vulnérables*" (article 79, paragraphe 2).

La proposition de Règlement visant à prévenir et à combattre les abus sexuels sur les mineurs a été publiée le 11 mai 2022 par la Commission européenne[21]. Ce texte vise à détecter et signaler les abus sexuels commis contre des enfants en ligne, prévenir les abus sexuels contre des enfants et soutenir les victimes. Cette future législation obligera les fournisseurs de services à signaler les abus sexuels commis contre des enfants en ligne via leurs plateformes et à alerter les autorités afin que les prédateurs sexuels puissent être traduits en justice. Les fournisseurs seront également tenus de signaler les cas de manipulation psychologique, une pratique par laquelle les prédateurs sexuels tissent une relation et un lien émotionnel avec des enfants et gagnent leur confiance afin de pouvoir les manipuler, les exploiter et les agresser. En complément de ce texte, la Commission européenne a adopté, le 6 février 2024, **une proposition de directive**[22] visant à actualiser la **Directive 2011/93 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie**. Les principales dispositions contiennent, entre autres, un élargissement, dans tous les États membres, des définitions des infractions pénales liées aux abus sexuels commis contre des enfants, le renforcement des poursuites, de la prévention et du soutien et une obligation de signalement sera également imposée au moins aux professionnels travaillant en contact étroit avec des enfants.

Une autre réforme, le Digital Fairness Act (DFA), est en cours de négociation. En octobre 2024, la Commission européenne a publié les conclusions du bilan de qualité sur l'équité numérique[23]. Celui-ci évalue si les textes européens en matière de protection des consommateurs permettent de garantir un niveau élevé de protection des consommateurs dans l'environnement numérique. Le bilan de qualité portait sur trois directives fondamentales : la directive sur les pratiques commerciales déloyales[24], la directive sur les droits des consommateurs[25] et la directive sur les clauses abusives dans les contrats[26]. En septembre 2024, la Présidente Ursula von der Leyen a adressé une lettre de mission à Michael McGrath, le Commissaire européen à la Démocratie, à

[21] Proposition de Règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, COM/2022/209 final.

[22] Proposition de Directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que contre les matériels relatifs à des abus sexuels sur enfants, et remplaçant la décision-cadre 2004/68/JAI du Conseil (refonte), COM/2024/60 final.

[23] Commission européenne, Commission Staff Working Document Fitness Check on EU consumer law on digital fairness, oct. 2024.

[24] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil.

[25] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil.

[26] Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs.

la Justice et à l'État de droit[27] évoquant notamment la nécessité de créer un futur *Digital Fairness Act*. Ce texte viserait à "*lutter contre les techniques et pratiques commerciales contraires à l'éthique, telles que les dark patterns, le marketing des influenceurs sur les réseaux sociaux, le design addictif des produits numériques et le profilage en ligne, en particulier lorsque les vulnérabilités des consommateurs sont exploitées à des fins commerciales*." Il serait pensé pour combler les lacunes plutôt que dupliquer les réglementations et il est vraisemblable que la protection des mineurs figure parmi les priorités du DFA.

1.2. PANORAMA DES TEXTES AU NIVEAU NATIONAL

Outre les adaptations du droit français résultant de l'évolution du droit de l'Union européenne, il peut être observé au cours des dernières années une densification du droit français applicable aux réseaux sociaux à l'initiative du législateur et de l'exécutif. Ainsi, plusieurs textes ont été récemment adoptés afin de renforcer la protection des mineurs dans le contexte de leurs usages des services numériques.

La Loi du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne[28] a permis d'étendre les règles du Code du travail applicable aux enfants mannequins, du spectacle et de la publicité aux employeurs dont l'activité consiste "*à réaliser des enregistrements audiovisuels* (…) *en vue d'une diffusion à titre lucratif sur un service de plateforme de partage de vidéos*".

La Loi du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet[29] facilite l'accès des parents aux outils de contrôle parental. Elle oblige les fabricants d'appareils connectés (smartphones, tablettes...) à installer un dispositif de contrôle parental et à proposer son activation gratuite lors de la première mise en service de l'appareil. Les nouvelles obligations, précisées par un décret d'application[30], pour les fabricants de matériels connectés sont applicables depuis le 11 juillet 2024[31].

[27] Lettre de mission du 17 septembre 2024 de la Présidente Ursula von der Leyen à Michael McGrath, Commissaire européen à la Démocratie, à la Justice et à l'État de droit.

[28] Loi n°2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne.

[29] Loi n°2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet.

[30] Décret n° 2023-588 du 11 juillet 2023 pris pour l'application de l'article 1er de la loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet.

[31] Services publics, Contrôle parental : de nouvelles obligations pour les fabricants de matériels connectés, 11 juillet 2024.

La Loi du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux[32] définit et encadre l'activité des influenceurs sur les réseaux sociaux, dont le public est souvent jeune. L'objectif est de mieux lutter contre certaines dérives et arnaques constatées (incitation à faire des régimes alimentaires dangereux, de la chirurgie esthétique, des paris excessifs, promotion de contrefaçons...)[33]. Des mesures spécifiques viennent protéger les enfants influenceurs. Les règles sur le travail des enfants Youtubeurs sur les plateformes de partage de vidéos, fixées par la loi du 19 octobre 2020, sont étendues à toutes les plateformes en ligne (réseaux sociaux tels qu'Instagram, Snapchat ou TikTok). Les enfants influenceurs commerciaux seront protégés par le code du travail. Leurs parents devront signer leurs contrats avec les annonceurs et consigner une part de leurs revenus (le pécule)[34].

La Loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne[35] instaure une interdiction d'inscription sur les réseaux sociaux pour les mineurs de moins de 15 ans sauf accord parental. Les plateformes devront mettre en place une solution technique pour garantir le respect de ces dispositions. Le texte contient par ailleurs des dispositions visant à mieux prévenir et poursuivre les délits en ligne, comme le cyberharcèlement[36]. A défaut de publication de ces décrets d'application en raison de dispositions incompatibles avec le droit de l'Union européenne, la loi n'est pas entrée en application à ce jour.

La Loi du 19 février 2024 visant à garantir le respect du droit à l'image des enfants[37] modifie le Code civil autour de trois objectifs. Premièrement, il s'agit d'introduire dans la définition de l'autorité parentale la notion de vie privée en consacrant de manière expresse l'obligation des parents de veiller au respect de la vie privée de leur enfant, y compris son droit à l'image, au titre de leurs prérogatives liées à l'exercice de l'autorité parentale. Une délégation partielle forcée de l'autorité parentale est créée en cas de diffusion de l'image de l'enfant portant gravement atteinte à sa dignité ou à son intégrité morale. Deuxièmement, le juge aux affaires familiales (JAF) pourra interdire à un parent de publier ou diffuser toute image de son enfant sans l'accord de l'autre parent. De plus, l'article 21 de la LIL est modifié afin de permettre à la Commission nationale de l'informatique et des libertés de saisir le juge des référés pour demander toute mesure de

[32] Loi n°2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux.

[33] V. toutefois les modifications par ordonnance à venir de la loi pour assurer sa mise en conformité avec le droit de l'Union européenne.

[34] À la suite d'une notification du texte à la Commission européenne et des observations de cette dernière communiquées aux autorités françaises, la loi a dû être modifiée pour la mettre en conformité avec la Directive e-commerce, le DSA, la Directive SMA et le Règlement sur les marchés numériques. C'est l'objet de l'Ordonnance 2024-978 du 6 novembre 2024 modifiant la Loi n°2023-451 prise en application de la Loi portant diverses dispositions d'adaptation au droit de l'Union européenne n°2024-364 du 22 avril 2024.

[35] Loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne.

[36] À la suite d'une notification du texte à la Commission européenne et des observations de cette dernière communiquées aux autorités françaises, il est prévu que la loi soit modifiée. Une discussion est désormais engagée (v. infra, chapitre 12, Contrôle de l'âge).

[37] Loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants.

sauvegarde des droits de l'enfant en cas d'inexécution ou d'absence de réponse à une demande d'effacement de données personnelles. Troisièmement, il est désormais prescrit que "*les parents protègent en commun le droit à l'image de leur enfant mineur" et que "les parents associent l'enfant à l'exercice de son droit à l'image, selon son âge et son degré de maturité*". Cette loi a notamment pour objectif de lutter contre le phénomène du *sharenting* - contraction du mot sharing (partager) et parenting (parentalité) - qui désigne le partage de photos par des parents de leurs enfants sur les réseaux sociaux[38].

La proposition de loi relative à la prévention de l'exposition excessive des enfants aux écrans[39] prévoit plusieurs mesures pour prévenir les risques de surexposition des plus jeunes enfants aux écrans et pour mieux sensibiliser les parents et former les professionnels de la petite enfance. La proposition de loi prévoit plusieurs mesures pour prévenir les risques de surexposition des plus jeunes enfants aux écrans et pour mieux sensibiliser les parents et former les professionnels de la petite enfance.

Transmise au Sénat le 8 mars 2023, elle cible les enfants de 0 à 6 ans et prévoit à ce titre plusieurs mesures pour prévenir les risques de surexposition des plus jeunes enfants aux écrans et pour mieux sensibiliser les parents et former les professionnels de la petite enfance : l'État devra développer, avec l'appui de l'Agence nationale de santé publique, des outils de mesure des risques liés à l'exposition aux écrans numériques dans les lieux d'accueil des jeunes enfants, en particulier dans les écoles maternelles :

- Une plateforme numérique comportant des informations sur les risques liés aux écrans numériques pour les enfants devra être mise en place pour les parents. Cette plateforme doit s'inscrire dans la démarche du site jeprotegemonenfant.gouv.fr, qui propose depuis février 2022 un volet dédié à l'usage des écrans, dans le cadre du plan d'actions gouvernemental « Pour un usage raisonné des écrans par les jeunes et les enfants » ;

- Des formations spécifiques sur les risques liés aux écrans numériques pour le jeune public devront être proposées aux professionnels de santé, du secteur médico-social, de la petite enfance et aux professeurs des écoles ;

- Les règlements intérieurs des écoles maternelles et élémentaires et des crèches devront réguler l'utilisation des appareils numériques par les personnels en présence des enfants et mettre en place une politique de prévention destinée aux élèves ;

- Sur le modèle de ce qui existe pour les paquets de cigarettes**,** un message de prévention devra être apposé sur les emballages des ordinateurs, des tablettes et des téléphones portables pour informer les consommateurs sur "les risques encourus par l'usage excessif de ces produits sur le développement psychomoteur, physique et cognitif des jeunes

[38] V. J. Rochfeld, "Données à caractère personnel - Données des mineurs", *Répertoire Dalloz IP IT et Communication*, 2024, pt. 34.

[39] Proposition de loi relative à la prévention de l'exposition excessive des enfants aux écrans, 8 mars 2023.

> enfants"**.** Le même message de prévention devra figurer sur les publicités pour les télévisions, les ordinateurs, les portables, les tablettes et les autres produits assimilés.

Par ailleurs le texte prévoit d'inscrire dans le carnet de grossesse ainsi que dans le carnet de santé de l'enfant des messages de prévention sur l'exposition excessive des enfants aux écrans. Lors des visites médicales scolaires obligatoires, les enfants de 3 à 4 ans seront sensibilisés aux risques des écrans. Sur amendement, les députés ont aussi prévu de faire des 20 rendez-vous médicaux dont bénéficient les enfants un temps de sensibilisation aux risques sanitaires, en particulier liés à une surexposition excessive aux écrans. Les projets éducatifs territoriaux (PEDT) devront désormais être un vecteur de l'information et de la prévention des risques liés à une exposition excessive des élèves aux écrans. Enfin, sur amendement, les députés ont proposé, conformément aux recommandations de la commission des 1000 premiers jours, de mettre en place une évaluation scientifique des logiciels se disant "éducatifs". Le gouvernement devra remettre un rapport au Parlement sur le sujet et étudier la création d'un label certifiant. Il convient de relever qu'une nouvelle version du carnet de santé de l'enfant est entrée en vigueur le 1er janvier 2025 à la suite des recommandations du Haut Conseil de la Santé Publique (HCSP) et comprend notamment des conseils sur l'utilisation des écrans[40].

La Loi du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (SREN)[41] prévoit différentes dispositions afin de renforcer la protection des utilisateurs des services numériques, dont les réseaux sociaux, et en particulier en ce qui concerne les mineurs en ligne, à savoir consacre des conditions d'accès tenant à l'âge pour les contenus à caractère pornographique, des incriminations relatives au partage non consenti de contenu intime et de sextorsion, encadre la diffusion d'hypertrucage à caractère sexuel ou encore prévoit des peines de bannissement des réseaux sociaux pour les cyber-harceleurs, ainsi qu'un stage de sensibilisation (n° 2024-866 DC)[42].

La sensibilisation est enfin une composante essentielle pour protéger les jeunes sur internet. Ainsi, la Loi du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République a généralisé l'utilisation des outils et des ressources numériques et impose aux enseignants de réaliser des actions de sensibilisation aux droits et devoirs liés à l'utilisation d'internet et des réseaux.

---

[40] Ministère de la santé, Le carnet de santé de l'enfant, 27.12.2024.

[41] Loi n°2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique.

[42] L'adoption de ce texte a été retardée en raison de la notification de ses dispositions auprès de la Commission européenne compte tenu de la possible non-conformité de certaines d'entre elles avec le droit de l'Union européenne, dont le DSA. Saisi de la constitutionnalité de certaines dispositions de la loi, le Conseil constitutionnel a rendu sa décision le 17 mai 2024 (Décision n° 2024-866 DC du 17 mai 2024). Il convient de relever que l'article 5 bis du PJL SPREN prévoyait le prononcé d'une amende forfaitaire en cas de délit d'outrage en ligne pour les personnes ayant des comportements discriminatoires, injurieux ou harcelants, disposition qui a été jugée non conforme à la Constitution par le Conseil constitutionnel au regard de l'atteinte que cette sanction pourrait porter atteinte de façon disproportionnée la liberté d'expression ; le dispositif de vérification de l'âge pour l'accès aux contenus pornographiques n'a pas été jugé contraire à la Constitution. Promulguée le 21 mai, la loi a été publiée au JORF le 22 mai 2024.

Au-delà des textes législatifs, se développe également un droit souple (soft law) applicable aux réseaux sociaux. Au niveau français, l'AFNOR a publié en novembre 2023 un guide de bonnes pratiques pour prévenir les risques et protéger les mineurs sur les réseaux sociaux[43]. Au niveau européen, l'Alliance pour mieux protéger les mineurs en ligne est une initiative d'autorégulation visant à améliorer l'environnement en ligne pour les enfants et les jeunes. Un groupe spécial a été mandaté par la Commission européenne pour élaborer un code de conduite complet de l'Union européenne sur la conception adaptée à l'âge (code BIK). Le code s'appuiera sur le cadre réglementaire prévu par la législation européenne et vise à renforcer la participation de l'industrie à la protection des enfants lors de l'utilisation de produits numériques, dans le but d'assurer leur vie privée, leur sûreté et leur sécurité en ligne.

[43]AFNOR, *Protéger les mineurs en ligne : oui, c'est possible*, 24 novembre 2023.

CHAPITRE 2 : PRÉSENTATION DE LA STRATÉGIE EUROPÉENNE DE LA PROTECTION DES MINEURS EN LIGNE

L'Union européenne a mis en œuvre une stratégie européenne de protection des mineurs en ligne. Ainsi, le Règlement sur les services numériques (DSA) comporte diverses dispositions pour assurer une telle protection qui accompagne le programme Better Internet for Kids (BIK), volet numérique de la stratégie globale de l'Union européenne en matière de droits de l'enfant.

2.1. RÈGLEMENT SUR LES SERVICES NUMÉRIQUES

2.1.1. Présentation du Règlement sur les services numériques

Le Règlement sur les services numériques adopté le 19 octobre 2022 (ou DSA pour Digital Services Act) introduit un régime d'obligations de moyens pour les fournisseurs de services intermédiaires, parmi lesquels les plateformes en ligne, où le niveau d'exigence varie en fonction de la taille des entreprises, et qui est particulièrement renforcé pour les très grands acteurs, dont les services induisent des risques systémiques (au vu du nombre de citoyens européens qui y ont recours).

Le DSA est entré en vigueur le 25 août 2023 pour les très grandes plateformes en ligne et très grands moteurs de recherche. Pour tous les autres services intermédiaires, notamment les plateformes en ligne, il trouve à s'appliquer depuis 17 février 2024.

Les très grandes plateformes en ligne (TGP) et les très grands moteurs de recherche (TGMR) en ligne sont officiellement désignés par la Commission européenne[44]. Cette dernière détient des pouvoirs exclusifs pour surveiller et faire respecter les dispositions spécifiques du règlement sur les services numériques (DSA) qui s'appliquent à TGP et TGMR (chapitre III section 5), conformément à l'article 56 (2) et (3) du DSA. Les autorités nationales de l'État membre où est situé l'établissement principal d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne ont également compétence pour les autres dispositions du règlement, notamment les chapitres II et III, sections 1 à 4.

Le DSA prévoit que chaque État membre de l'Union européenne doit nommer une ou plusieurs autorités compétentes chargées de faire respecter le règlement, dont une autorité indépendante qui assumera le rôle de coordinateur pour les services numériques (CSN). Cette entité est responsable d'assurer la cohérence de la mise en œuvre du règlement au niveau national.

[44] Commission européenne, Supervision des très grandes plateformes en ligne et des moteurs de recherche désignés au titre de la législation sur les services numériques, liste mise à jour le 17 décembre 2024, https://digital-strategy.ec.europa.eu/fr/policies/list-designated-vlops-and-vloses : les réseaux sociaux concernés sont Facebook, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, X/Twitter, YouTube.

En outre, le comité européen des services numériques a mis en place huit groupes de travail afin de soutenir la mission du comité. Le groupe 6 dédié à la protection des mineurs[45] examine les questions liées à la protection des mineurs, en particulier l'article 28 du DSA et le lien avec les contenus pour adultes et l'éducation aux médias. Elle soutient également les lignes directrices de la Commission au titre de l'article 28 qui ont été publiées le 14 juillet 2025 à l'issue d'un processus de consultation des parties prenantes. Une équipe spéciale chargée de la vérification de l'âge a été intégrée à ce groupe de travail.

L'Arcom joue un rôle essentiel dans la mise en œuvre du DSA. En tant que coordinateur pour les services numériques (CSN), elle doit assumer diverses responsabilités, notamment : (1) superviser la mise en œuvre des dispositions du Règlement sur les Services Numériques (DSA) par les fournisseurs de services intermédiaires français, en traitant les plaintes et en prononçant des sanctions en cas de non-respect du DSA ; (2) assurer que les plateformes en ligne françaises contribuent à la base de données européenne contenant les motifs de décision de modération transmis aux utilisateurs ; (3) nommer les signaleurs de confiance, dont les signalements de contenus illicites seront traités en priorité par les plateformes ; (4) certifier les organismes de règlement extrajudiciaire des litiges en France, qui examinent les cas individuels lorsque les utilisateurs contestent une décision de modération ; (5) centraliser les injonctions émises par les autorités judiciaires et administratives françaises en vertu du DSA et les transmettre à tous les coordinateurs pour les services numériques (CSN) européens. Par ailleurs, en tant que coordinateur national, (6) l'Arcom fait partie du Comité européen pour les services numériques, collaborant étroitement avec les autres coordinateurs des différents États membres et la Commission européenne. En cas de non-respect du DSA, l'Arcom a le pouvoir de sanctionner les acteurs français en dernier recours.

La **DGCCRF et la CNIL** sont désignées aux côtés de l'Arcom, et celle-ci veille à une coopération étroite entre ces autorités. La CNIL est également compétente pour vérifier le respect par les plateformes des interdictions publicitaires à l'égard des mineurs.

2.1.2. Dispositions du Règlement sur les services numériques spécifiques aux mineurs

Le DSA prévoit plusieurs règles pour protéger les mineurs. Les principales obligations portent sur l'information adaptées aux enfants, des obligations de *Safety by design*, l'interdiction du profilage dans la publicité pour les enfants et les jeunes

[45] Commission européenne, Groupe de travail 6 du Comité européen des services numériques, https://digital-strategy.ec.europa.eu/fr/library/working-group-6-european-board-digital-services-protection-minors.

2.1.2.1. Informations adaptées aux enfants

Le DSA prévoit que les conditions générales d'utilisation (CGU) qui doivent être rédigées et actualisées de manière à être faciles à comprendre par tous y compris les mineurs (article 14). Les s**ystèmes de plainte et de signalement doivent** également **être adaptés aux enfants** (considérant 89).

2.1.2.2. Conception garantissant la protection de la vie privée, de la sécurité et sûreté des mineurs (Safety by design)

Une disposition du DSA est particulièrement consacrée à la protection des mineurs qui constitue l'un des principaux objectifs du règlement. Ainsi, l'article 28 du DSA prévoit que :

"*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."

Le texte trouve à s'appliquer aux plateformes accessibles aux mineurs, c'est-à-dire toute plateforme " dont les conditions générales autorisent les mineurs à utiliser le service, lorsque son service s'adresse à des mineurs ou est principalement utilisé par des mineurs, ou lorsque le fournisseur sait par ailleurs que certains des destinataires de son service sont des mineurs" (considérant 71 du DSA). À cet égard, les lignes directrices publiées le 14 juillet 2025 précisent "*qu'un fournisseur d'une plateforme en ligne ne peut pas se fonder uniquement sur une mention dans ses conditions générales interdisant l'accès aux mineurs, pour faire valoir que la plateforme ne leur est pas accessible. Si le fournisseur de la plateforme en ligne ne met pas en œuvre de mesures efficaces pour empêcher les mineurs d'accéder à son service, il ne peut pas prétendre que sa plateforme en ligne ne relève pas du champ d'application de l'article 28*"[46].

Les lignes directrices prévues à l'article 28.4 ont été publiées le 14 juillet 2025 après un processus de consultation des parties prenantes. Il convient de préciser que celles-ci n'ont pas de valeur

[46] Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065, C/2025/5519, JOUE 10 oct. 2025, p. 3.

contraignante mais révèlent l'interprétation de la Commission de l'article 28 du DSA. Par conséquent, si les plateformes ne sont pas tenues de les respecter, elles devront alors prouver que les mesures qu'elles mettent en place sont aussi efficaces que ce que prévoient les lignes directrices en termes de protection des mineurs.

Les bonnes pratiques énoncées dans les lignes directrices visent à fournir des conseils sur les mesures et les caractéristiques permettant d'atteindre ce niveau élevé de confidentialité, de sûreté et de sécurité. Outre les mesures spécifiques énoncées dans les lignes directrices - lesquelles seront envisagées à l'aune de l'étude des différents risques supra -, il convient de préciser les mesures de gouvernance prévues par le texte afin d'en assurer l'effectivité. A cet égard, le texte préconise que les plateformes mettent en place des fonctions, des rôles et des responsabilités spécifiques dédiés à la protection et à la participation des mineurs afin de s'assurer que les actions et les mesures sont coordonnées, mises en œuvre et évaluées sur la base d'une expertise adéquate en matière de droits de l'enfant.

Par ailleurs, la Commission souligne la nécessité d'évaluer l'efficacité de ces mesures pour atteindre les objectifs poursuivis notamment, comme le propose les lignes directrices, en consultant les mineurs, en réalisant des tests avec eux, et en prenant en compte leurs retours d'information. Également, et dès que nécessaire, elle précise qu'il conviendra d'adapter ces mesures à l'évolution des techniques et des pratiques, en associant à ce processus les représentants de la société civile et les chercheurs académiques.

2.1.2.3. Interdiction du profilage dans la publicité pour les enfants et les jeunes

Selon l'article 28.2 du DSA, les plateformes ne peuvent présenter des publicités reposant sur le profilage utilisant des données à caractère personnel dès lors qu'elles savent avec une « certitude raisonnable » que le destinataire du service est un mineur.

2.1.2.4. Analyses de risques

Le DSA institue un nouveau cadre d'analyse de risques qui constitue un des dispositifs les plus novateurs et les plus prometteurs de ce texte. Ainsi, les articles 34 et 35 du DSA imposent aux très grandes plateformes et très grands moteurs de recherche de réaliser des analyses de risques et de prendre des mesures d'atténuation des risques. Concernant les mineurs, les très grandes plateformes et moteurs de recherche doivent en particulier analyser si :

- les mineurs peuvent facilement comprendre le fonctionnement du service (considérant 81) ;
- les mineurs risquent d'accéder à des contenus pouvant nuire à leur santé ainsi qu'à leur épanouissement physique, mental et moral (considérant 81) ;
- les caractéristiques de conception sont susceptibles d'entraîner des dépendances (considérants 81 et 83).

Ces opérateurs doivent ainsi mettre en place des mesures visant à atténuer ces risques ce qui implique de mettre en place des outils de contrôle parental, de vérification de l'âge ou encore des outils permettant d'aider les jeunes à signaler les abus ou à obtenir un soutien.

Analyses de risques imposées aux très grandes plateformes et moteurs de recherche. Selon l'article 34 du DSA, il est imposé aux très grandes plateformes et aux moteurs de recherche, définis par des critères quantitatifs et formels, d'adopter une approche proactive dans la gestion des risques. Ils sont à ce titre dans l'obligation de recenser, d'analyser et d'évaluer de manière diligente tout risque systémique lié à la conception, au fonctionnement de leurs services et aux systèmes connexes, y compris les systèmes algorithmiques, ainsi qu'à l'utilisation de leurs services.

Les risques systémiques à prendre en compte sont variés et touchent à la diffusion de contenus illicites amplifiée par la taille des plateformes qui ont des conséquences sur les droits fondamentaux tels que la dignité humaine, la vie privée, la protection des données personnelles, la liberté d'expression, la non-discrimination et les droits de l'enfant. Les plateformes devront également prendre en compte tout effet sur le discours civique, les processus électoraux et la sécurité publique, ainsi que les risques associés aux violences sexistes, à la protection de la santé publique et des mineurs et les "*conséquences négatives graves sur le bien-être physique et mental des personnes*".

Pour ce faire, ils devront prendre en compte les éléments suivants : a) la conception de leurs systèmes de recommandation et de tout autre système algorithmique pertinent ; b) leurs systèmes de modération des contenus ; c) les conditions générales applicables et leur mise en application ; d) les systèmes de sélection et de présentation de la publicité ; e) les pratiques du fournisseur en matière de données.

Il conviendra également d'envisager dans le cadre de ces évaluations si et comment ces risques "*sont influencés par la manipulation intentionnelle du service desdits fournisseurs, y compris par l'utilisation non authentique ou l'exploitation automatisée du service, ainsi que par l'amplification et la diffusion potentiellement rapide et à grande échelle de contenus illicites et d'informations incompatibles avec leurs conditions générale*".

S'agissant de l'évaluation des risques pour les droits des enfants, le considérant 81 précise que "*les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient examiner par exemple à quel point la conception et le fonctionnement du service sont faciles à comprendre pour les mineurs, ainsi que la manière dont ces derniers peuvent être exposés, par le biais de leur service, à des contenus pouvant nuire à leur santé ainsi qu'à leur épanouissement physique, mental et moral. Ces risques peuvent résulter, par exemple, de la conception des interfaces en ligne qui exploitent intentionnellement ou non les faiblesses et l'inexpérience des mineurs ou qui peuvent entraîner un comportement de dépendance*".

Mesures d'atténuation des risques. L'article 35 du DSA prévoit ensuite que "*les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne mettent en place des mesures d'atténuation raisonnables, proportionnées et efficaces, adaptées aux risques systémiques spécifiques recensés conformément à l'article 34, en tenant compte en particulier de l'incidence de ces mesures sur les droits fondamentaux*". Le texte précise que "*ces mesures d'atténuation peuvent inclure le cas échéant :*

1) *l'adaptation de la conception, des caractéristiques ou du fonctionnement de leurs services, y compris leurs interfaces en ligne ;*

2) *l'adaptation de leurs conditions générales et de la mise en application de celles-ci ;*

3) *l'adaptation des processus de modération des contenus, y compris la rapidité et la qualité du traitement des notifications relatives à des types spécifiques de contenus illicites et, le cas échéant, le retrait rapide des contenus qui ont fait l'objet d'une notification ou le blocage de l'accès à ces contenus, en particulier en ce qui concerne les discours haineux illégaux ou la cyberviolence, ainsi que l'adaptation des processus décisionnels pertinents et des ressources dédiées à la modération des contenus ;*

4) *le test et l'adaptation de leurs systèmes algorithmiques,y compris leurs systèmes de recommandation ;*

5) *l'adaptation de leurs systèmes de publicité et l'adoption de mesures ciblées destinées à limiter la présentation de publicités, ou à en adapter la présentation, en association avec le service fourni ;*

6) *le renforcement des processus internes, des ressources, des tests, de la documentation ou de la surveillance d'une quelconque de leurs activités, notamment en ce qui concerne la détection des risques systémiques ;*

7) *la mise en place d'une coopération avec les signaleurs de confiance, ou l'ajustement de cette coopération, conformément à l'article 22, ainsi que la mise en œuvre des décisions prises par les organes de règlement extrajudiciaire des litiges en vertu de l'article 21 ;*

8) *la mise en place d'une coopération avec d'autres fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne, ou l'ajustement de cette coopération, sur la base des codes de conduite et des protocoles de crise visés aux articles 45 et 48, respectivement*

9) *l'adoption de mesures de sensibilisation et l'adaptation de leur interface en ligne, afin de donner plus d'informations aux destinataires du service ;*

10) *l'adoption de mesures ciblées visant à protéger les droits de l'enfant, y compris la vérification de l'âge et des outils de contrôle parental, ou des outils permettant d'aider les mineurs à signaler les abus ou à obtenir un soutien, s'il y a lieu ;*

11) *le recours à un marquage bien visible pour garantir qu'un élément d'information, qu'il s'agisse d'une image, d'un contenu audio ou vidéo généré ou manipulé, qui ressemble nettement à des personnes, à des objets, à des lieux ou à d'autres entités ou événements réels, et apparaît à tort aux yeux d'une personne comme authentique ou digne de foi, est reconnaissable lorsqu'il est présenté sur leurs interfaces en ligne, et, en complément, la mise à disposition d'une fonctionnalité facile d'utilisation permettant aux destinataires du service de signaler ce type d'information*".

Le considérant 89 du DSA apporte des précisions concernant ce texte s'agissant des utilisateurs mineurs, en spécifiant que "*les fournisseurs de très grandes plateformes en ligne et de très grands*

moteurs de recherche en ligne devraient tenir compte de l'intérêt supérieur des mineurs lorsqu'ils prennent des mesures telles que l'adaptation de la conception de leur service et de leur interface en ligne, plus particulièrement lorsque leurs services s'adressent aux mineurs ou sont utilisés de manière prédominante par ceux-ci. Ils devraient veiller à ce que leurs services soient organisés de manière à permettre aux mineurs d'accéder facilement aux mécanismes prévus par le présent règlement, le cas échéant, y compris aux mécanismes de notification et d'action et aux mécanismes de réclamation. En outre, ils devraient prendre des mesures pour protéger les mineurs contre les contenus susceptibles de nuire à leur épanouissement physique, mental ou moral et fournir des outils permettant un accès conditionnel à ces informations. Lorsqu'ils choisissent les mesures d'atténuation appropriées, les fournisseurs peuvent prendre en compte, le cas échéant, les bonnes pratiques du secteur, y compris celles établies au moyen d'une coopération en matière d'autorégulation, telles que les codes de conduite, et devraient tenir compte des lignes directrices de la Commission".

Ces analyses et mesures sont soumises à audit selon l'article 37 du DSA afin d'attester de la réalité de la mise en œuvre de ces obligations. En outre, les rapports d'analyse de risques doivent être publiés annuellement par les très grandes plateformes. Par ailleurs, conformément à l'article 35 (2) du DSA, le Comité européen pour les services numériques est tenu de publier une fois par an un rapport visant à identifier les risques systémiques les plus importants et récurrents dans l'Union européenne et les États membres ainsi que les meilleures pratiques de limitation de ces risques, dont la première version a été publiée le 18 novembre 2025[47], après consultation des parties prenantes comme les groupes concernés, les organisations non gouvernementales et les chercheurs académiques. Il convient en outre de relever que différentes enquêtes ont été ouvertes par la Commission européenne à l'encontre de différentes plateformes qui portent notamment sur le non-respect de leurs obligations au titre des articles 34 et 35 du DSA[48].

Limites. Différentes observations peuvent être réalisées à la lecture de ces documents, en particulier des rapports d'analyse de risques publiés par les très grandes plateformes et moteurs de recherche depuis l'entrée en application du DSA[49]. Ces rapports illustrent les lacunes du dispositif à l'œuvre, même s'il convient de préciser que cette nouvelle approche est pensée comme un processus itératif dont la mise en œuvre doit être réalisée de façon progressive afin de renforcer ce nouveau type de régulation par la transparence. Il a ainsi été relevé par différents acteurs une insuffisance d'ordre méthodologique s'agissant des premiers rapports publiés par les opérateurs désignés comme très grandes plateformes et moteurs de recherches. Il a pu être observé que, en

[47] European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 Novembre 2025. Le Comité européen pour les services numériques est composé des coordinateurs des États membres pour les services numériques et est présidé par la Commission européenne.

[48] V. notamment Commission européenne, La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques, 19 février 2024 et La Commission ouvre une procédure formelle à l'encontre de Meta au titre du règlement sur les services numériques en ce qui concerne la protection des mineurs sur Facebook et Instagram, 16 mai 2024.

[49] DSA Civil Society Coordination Group, Initial Analysis on the First Round of Risk Assessments Reports under the EU Digital Services Act - An initiative of the DSA Civil Society Coordination Group, 2025.

l'absence de publication de lignes directrices de la Commission sur la méthodologie à suivre, les opérateurs ont retenu des approches différentes afin d'identifier les risques systémiques à évaluer et la manière de les limiter, ainsi que dans la manière de publier ces informations.

Une première difficulté a été relevée qui concerne l'analyse ponctuelle réalisée par les opérateurs s'agissant de certains risques alors qu'ils sont en principe tenus, en application de l'article 34 du DSA, de prendre en compte de façon plus large "*tout effet négatif réel ou prévisible sur l'exercice des droits fondamentaux*". Plusieurs méthodes d'analyse d'impact sur les droits fondamentaux pourraient à cet égard servir de modèle à suivre[50]. Une autre difficulté majeure concerne l'insuffisante évaluation de l'efficacité des mesures de limitation des risques mises en œuvre par les opérateurs concernés, dont les rapports restent très abstraits. En effet, plusieurs rapports publiés par les très grandes plateformes ne font qu'évoquer des mesures mises en place sans démontrer qu'elles viennent effectivement limiter les risques identifiés, et ne produisent pas de données justifiant de leur pertinence. Il paraît dès lors essentiel que soient produits des éléments probants vérifiables, de nature qualitative et quantitative.

Plusieurs préconisent dès lors de consacrer une méthodologie d'évaluation des risques adaptée et l'élaboration de mesures d'atténuation d'une manière qui soit significative et équitable, ainsi que d'exiger des plateformes la publication de rapports d'analyse de risques dans un format compréhensible et exploitable pour les tiers indépendants, y compris sous une forme lisible par la machine, afin de permettre à ces acteurs tiers d'évaluer la conformité des pratiques des plateformes concernées à leurs obligations imposées au titre du DSA[51].

En outre, il paraît essentiel que ces informations produites par les plateformes soient enrichies d'analyses indépendantes s'agissant des risques systémiques et des mesures de limitation des risques à adopter. Cela suppose pour les opérateurs de s'appuyer sur des collaborations avec des acteurs académiques et la société civile afin de réaliser ces évaluations de manière optimale.

A titre d'exemple, il est possible de se référer à l'analyse proposée par le KGI et la Panoptykon Foundation dans leur réponse à la consultation du Comité européen pour les services numériques, [52] pour illustrer la manière dont les outils de mesure et de transparence peuvent soutenir une gestion plus proactive des risques systémiques dans la conception des services numériques. Ils relèvent en particulier l'importance d'intégrer une évaluation continue des risques au sein même des processus de conception et d'expérimentation des produits. Ils proposent pour ce faire un processus en trois temps. Dans un premier temps, il est recommandé d'utiliser des groupes témoins universels (*Measuring interface design and mitigation through universal holdouts*) afin d'évaluer systématiquement l'impact des décisions relatives à la conception sur les risques. Dans un deuxième temps, il est préconisé de renforcer la transparence opérationnelle (*Improving*

[50] V. notamment European Center for Not-for-Profit Law and Access now, Towards meaningful Fundamental Rights Impact Assessements under the DSA, 2023.
[51] DSA Civil Society Coordination Group, Initial Analysis on the First Round of Risk Assessments Reports under the EU Digital Services Act - An initiative of the DSA Civil Society Coordination Group, 2025.
[52] Knight Georgetown Institute & Panoptykon Foundation, European Board for Digital Services and Europeen Commission Report on Systemic Risks and Mitigations under the Digital Services Act, 7 April 2025, p.15.

operational and product experiment transparency), notamment au moyen de la publication des objectifs des équipes produit et des résultats agrégés de leurs expérimentations, qui permettrait aux régulateurs et aux parties prenantes de bénéficier d'une meilleure visibilité sur l'alignement entre optimisation de la croissance et l'atténuation des risques. Dans un troisième temps, il est suggéré d'intégrer un suivi des effets au niveau de la population (*Tracking population-level effects)*, fondé sur des indicateurs intermédiaires permettant de mesurer l'évolution des risques à plus long terme et qui complèterait les évaluations annuelles prévues au titre du DSA. Ces indicateurs pourraient notamment s'appuyer sur les comportements des utilisateurs qui font état d'expériences négatives, ou en évaluant l'engagement au regard de contenus illicites ou préjudiciables.

Dès lors, certains recommandent que la Commission européenne propose des lignes directrices définissant les meilleures pratiques en ce domaine après consultation des parties prenantes. Compte tenu des enjeux, ces lignes directrices pourraient, a minima, porter sur l'évaluation des risques en matière de santé mentale et physique des utilisateurs.

Préconisation 1 - Promouvoir la publication par la Commission européenne, après consultation des parties prenantes, d'une méthode d'analyse de risque et d'une évaluation des mesures d'atténuation des risques à mettre en œuvre qui soient suffisamment transversales, pertinentes, probantes et compréhensibles pour être vérifiées et évaluées, en particulier en ce qui concerne l'évaluation des risques en termes de santé mentale et physique des utilisateurs.

Préconisation 2 - Promouvoir la collaboration d'acteurs tiers indépendants issues du monde académique et de la société civile pour favoriser la prise en compte de l'ensemble des risques systémiques et l'identification des mesures de limitation des risques pertinentes et efficaces.

Accès aux données. La régulation par la transparence est en outre assurée par le biais des dispositifs d'accès aux données consacrés par le DSA[53]. En effet, afin de renforcer la transparence et la responsabilisation des très grandes plateformes et moteurs de recherche, et pour compléter les informations auxquelles le régulateur peut avoir accès quant au respect de leurs obligations au titre des articles 34 et 35 du DSA, le texte consacre la possibilité, pour les chercheurs agréés, d'avoir un accès aux données des très grandes plateformes en ligne et moteurs de recherche concernant l'évaluation des risques systémiques.

Le DSA prévoit deux dispositions à cet égard. Tout d'abord une **procédure d'agrément** en vertu de l'article 40.4 qui permet à certains chercheurs d'accéder aux données des plateformes (y compris des données internes) afin d'étudier soit les risques systémiques qu'elles peuvent poser dans l'Union européenne, soit l'efficacité des mesures d'atténuation desdits risques systémiques

[53] Knight Georgetown Institute & Panoptykon Foundation, European Board for Digital Services and European Commission Report on Systemic Risks and Mitigations under the Digital Services Act, 7 April 2025, p. 19.

qu'elles mettent en place. Les chercheurs devront remplir un ensemble de conditions pour obtenir l'agrément : appartenance à un organisme de recherche, indépendance aux intérêts commerciaux, mesures de sécurité et protection des données, proportionnalité de l'accès, etc. (l'ensemble des conditions est détaillé à l'article 40.8 du DSA). L'agrément est délivré par le Coordinateur pour les Services Numériques (CSN) d'établissement, après éventuelle évaluation initiale par le CSN dans lequel l'organisme de recherche est situé. Un acte délégué de la Commission Européenne viendra préciser plus en détail ladite procédure d'agrément[54]. La procédure d'agrément sera opérationnelle après la publication de cet acte délégué.

Ensuite, un **accès aux données publiquement accessibles** de la plateforme pour des chercheurs remplissant un sous-ensemble moins restreint de critères selon l'article 40.12 du DSA, cette fois-ci uniquement pour la compréhension, recension et détection des risques systémiques. L'accompagnement de l'accès aux données pour les chercheurs est une priorité du régulateur, en particulier de l'Arcom. Ainsi, l'Arcom a publié en juin 2024 les résultats d'une consultation publique sur le sujet[55] et organisé un atelier de travail sur le sujet avec le PEReN[56].

L'Arcom se prépare à la mise en œuvre du DSA, notamment avec les homologues régulateurs européens désignés coordinateurs des services numériques (CSN) pour l'application du règlement. Il existe un sous-groupe au sein du réseau informel des CSN qui traite spécifiquement de l'identification et de l'évaluation des risques systémiques ainsi que de la supervision des mesures d'atténuation qui seront prises par les très grandes plateformes et très grands moteurs de recherche en ligne.

Il convient toutefois de souligner que la mise en œuvre des articles 34 et 35 relève avant tout de la compétence de la Commission européenne (comme l'ensemble des obligations applicables spécifiquement aux très grandes plateformes et moteurs de recherche), bien que les CSN l'accompagnent dans cette tâche, notamment dans la remontée d'informations et de phénomènes constatés au niveau national. Par ailleurs, l'accès aux données permis aux chercheurs en vertu de l'article 40 sera un fondement essentiel pour l'identification, la réduction et l'évaluation des risques systémiques.

2.1.2.5. Signalement des contenus illicites et obligations des plateformes

Notification et action. Le fournisseur de service doit promptement bloquer ou rendre l'accès impossible à tout contenu notifié comme illicite, par exemple des images représentant des abus sexuels commis sur des enfants, d'images intimes partagées sans le consentement de la personne représentée ou encore du contenu relevant du harcèlement en ligne (exemples de contenus illicites cités par le considérant 12 du DSA). En outre, l'article 9 du DSA impose aux fournisseurs de service de répondre à l'injonction d'agir émise par une autorité judiciaire ou administrative

[54] European Commission, Digital Services Act: Summary report on the call for evidence on the Delegated Regulation on data access, 24 novembre 2023.
[55] Acrom, Accès des chercheurs aux données des plateformes : synthèse des réponses à la consultation de l'Arcom et propositions, 20 juin 2023.
[56] PEReN, Atelier de travail sur l'accès aux données pour la recherche, 2023.

nationale compétente concernant un contenu illicite ou de communication d'informations, en précisant dans les meilleurs délais les suites données à l'injonction (ils doivent préciser si et quand une suite a été donnée).

A cet égard, il convient de rappeler que, conformément à l'article 6 du DSA, le fournisseur de service de réseau social n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition que ce fournisseur a) n'ait pas effectivement connaissance de l'activité illégale ou du contenu illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas conscience de faits ou de circonstances selon lesquels l'activité illégale ou le contenu illicite est apparent ou b) dès le moment où il en prend connaissance ou conscience, qu'il a agi promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible.

A cette fin, l'article 16 du DSA impose aux hébergeurs de mettre en place des mécanismes permettant à toute personne ou entité de signaler des contenus illicites. Ces mécanismes doivent être faciles d'accès et d'utilisation, et permettre la soumission électronique de notifications détaillées par la fourniture d'un formulaire dédié à la notification des contenus illicites. Il convient également de préciser que, pour préserver l'exercice de leur droit fondamental à la liberté d'expression, l'article 17 du DSA impose à tous les fournisseurs de services d'hébergement de fournir aux utilisateurs des informations claires et spécifiques lorsqu'ils suppriment ou restreignent l'accès à leur contenu, les raisons de cette mesure et les possibilités de recours disponibles pour la contester.

En outre, selon l'article 16.3 du DSA, lorsque cette notification est suffisamment précise et permet à un "fournisseur diligent de services d'hébergement d'identifier l'illégalité de l'activité ou de l'information concernée sans examen juridique détaillé ", elle est réputée donner lieu à la connaissance ou à la prise de conscience effective aux fins de l'article 6 en ce qui concerne l'élément d'information spécifique concerné.

Signaleurs de confiance. En vertu de l'article 22 du DSA, les signaleurs de confiance sont des entités qui servent d'intermédiaires pour les signalements entre les plateformes numériques et les utilisateurs. Leur rôle principal est de signaler des contenus illicites directement aux plateformes, qui sont tenues de traiter ces signalements en priorité et dans les meilleurs délais.

L'attribution du statut de signaleur de confiance relève du coordinateur des services numériques, l'Arcom en France, qui désigne des entités établies dans son ressort, telles que des collectivités, des entreprises ou des associations engagées dans la lutte contre la haine en ligne et la modération des contenus. Ces signaleurs de confiance bénéficient d'une relation prioritaire pour effectuer leurs signalements et peuvent dialoguer directement avec les plateformes afin d'améliorer la réactivité de la modération. Cette priorité accordée aux signaleurs de confiance permet une décentralisation du contrôle des contenus illicites en ligne, en renforçant la coopération entre les plateformes et les acteurs spécialisés. Pour obtenir ce statut, une organisation doit être indépendante des fournisseurs de plateformes, afin de garantir une modération impartiale et transparente.

En outre et en vertu de l'article 22.3 du DSA, les signaleurs de confiance sont également tenus de publier, au moins une fois par an, des rapports détaillés et accessibles concernant les notifications reçues conformément à l'article 16 au cours de la période considérée. Ces rapports doivent fournir

le nombre total de notifications, classées selon trois critères : a) l'identité du fournisseur de services d'hébergement, b) le type de contenu présumé illicite signalé, ainsi que c) l'action entreprise par le fournisseur en réponse à chaque notification. Par ailleurs, ces rapports doivent comporter une description des procédures mises en place afin d'assurer l'indépendance du signaleur de confiance dans l'exercice de leurs fonctions. Une fois élaborés, ces documents sont transmis au coordinateur pour les services numériques ayant attribué le statut de signaleur de confiance (l'Arcom pour la France) et sont également rendus accessibles au public.

L'Arcom joue un rôle clé dans la mise en place de ce dispositif au niveau national. Depuis le mois de juillet 2023, un groupe de travail au sein de l'Arcom élabore une approche cohérente pour les « Trusted Flaggers » à l'échelle de l'Union européenne, en conformité avec l'article 22 du DSA. L'objectif est de fixer des critères pour l'octroi du statut et d'assurer un suivi efficace des activités des signaleurs de confiance. L'Arcom a également la capacité de révoquer ce statut si l'indépendance ou l'impartialité d'un signaleur venait à être remise en cause.

L'association e-Enfance a été la première association à être désignée signaleur de confiance par l'Arcom en novembre 2024 dans le cadre du DSA[57]. Depuis, plusieurs organisations reconnues pour leur expertise dans la détection, l'identification et la notification de contenus illicites ont été désignées par l'Arcom comme signaleurs de confiance[58].

2.1.2.6. La plateforme d'alerte (Commission européenne)

Dans le cadre de la mise en œuvre du DSA, la Commission européenne a mis en ligne le 30 avril 2024 une plateforme d'alerte permettant de faire remonter toute situation à la Direction générale des réseaux de la communication, du contenu et de la technologie de la Commission européenne[59]. Ce formulaire permet un envoi sécurisé et anonyme d'envoyer des « *informations permettant d'identifier et de mettre au jour les pratiques préjudiciables* » des très grandes plateformes et moteurs de recherche du DSA. Cette plateforme permet la communication d'informations sous divers formats (rapport, mémo, mails, données, décisions…) et dans les langues officielles de l'UE.

[57] Arcom, Communiqué de presse, 6 novembre 2024.
[58] Arcom, Règlement sur les services numériques (DSA) : liste des signaleurs de confiance désignés par l'Arcom, 18 août 2025.
[59] Commission européenne, La Commission lance un outil d'alerte en cas de violation des sanctions, 4 mars 2022.

2.2. STRATÉGIE EUROPÉENNE DE PROTECTION DE L'ENFANCE EN LIGNE

Le programme BIK + (*Better Internet for Kid*)[60] est un programme européen lancé par la Commission en 2008 ; 31 pays déploient ce programme. L'objectif est de créer un environnement digital plus sûr pour les mineurs, en adoptant de nouvelles stratégies européennes.

En pratique, le programme se met en œuvre grâce à deux réseaux ; le réseau **Insafe** mis en place pour accompagner les jeunes et 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).

Chaque pays lié au programme BIK+ dispose d'un Safer Internet Center. En pratique le programme se met en œuvre grâce à deux réseaux ; le réseau Insafe mis en place pour accompagner les jeunes et 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).

En France, cela se présente comme suit :

(1) Le centre de sensibilisation aux usages d'Internet Internet Sans Crainte qui s'adresse aux jeunes aux parents, éducateurs et professeurs afin d'éduquer à un meilleur usage d'internet. Le centre offre aussi des outils de sensibilisation et des services mis en place en coopération avec d'autres acteurs tels que les écoles, le secteur privé et d'autres acteurs nationaux.

(2) Le 3018, le numéro national pour lutter contre les violences numériques, qui aide les jeunes et leurs parents à faire face à des contenus dangereux, indésirables ou offensants (par exemple le harcèlement en ligne, le discours haineux, le sexting).

(3) La hotline Point de Contact, le service de signalement de contenus illicites. Ce dispositif de signalement permet à tout internaute de signaler un contenu potentiellement illicite rencontré lors de sa navigation. Point de Contact analyse et traite les signalements adressés par les internautes et traite les signalements transmis par ses homologues membres du réseau INHOPE, le réseau mondial des hotlines.

Les associations comme l'association e-Enfance ou Point de Contact accompagnent parents, enfants et professionnels en développant des actions de sensibilisation et d'information[61].

Le Code de conduite de l'Union européenne sur la conception adaptée à l'âge "*vise à renforcer la participation de l'industrie à la protection des enfants lors de l'utilisation de produits*

[60] Commission européenne, Stratégie européenne pour un internet mieux adapté aux enfants - BIK+, 2022.

[61] Pour une présentation plus générale de l'ensemble des acteurs chargés de veiller au respect des droits fondamentaux des mineurs et à leur sécurité sur les réseaux sociaux, v. annexe 2.

numériques, dans le but ultime d'assurer leur vie privée, leur sûreté et leur sécurité en ligne". L'objectif de ce code est de légiférer dans la conception d'applications, de plateformes, de jeux en ligne, jouets connectés afin d'accorder une importance à la confidentialité et à la sécurité des enfants. De plus, ce code fait partie des stratégies BIK et propose d'inclure la parole des jeunes en laissant les mineurs prendre part aux réunions sur invitation.

III. PRATIQUES EN LIGNE

Les mineurs peuvent être victimes de plusieurs types de cyberviolence, notion qui recouvre un ensemble d'actes commis par le biais des services numériques[62]. En pratique, cela vise différentes formes de harcèlement, d'atteintes à la vie privée, d'abus et d'exploitation à caractère sexuel, ainsi que des comportements discriminatoires fondés sur le genre, l'origine, la religion ou l'appartenance à une communauté. Parmi ces formes de cyberviolence, le cyberharcèlement constitue l'une des plus répandues et se manifeste par divers comportements répétés à l'égard des victimes tels que l'envoi de messages de haine, moqueries et injures ou encore la divulgation de données personnelles - ou *doxing* - (**Chapitre 3**). Ces pratiques entraînent fréquemment des atteintes à l'intimité des personnes concernées, notamment en cas de diffusion non consentie d'images à caractère sexuel (**Chapitre 4)** et de chantage à caractère sexuel (**Chapitre 5**). Ces atteintes ne sont plus uniquement le fruit de cybercriminels expérimentés en partie du fait de la démocratisation des outils d'intelligence artificielle générative de textes, d'images ou de contenus audio permettant de générer des contenus hypertruqués (deepfakes) à caractère sexuel à partir de la photographie d'un visage, et après utilisation d'une application de dénudage numérique (**Chapitre 6**).

Les pratiques des mineurs en ligne les conduisent en outre, de manière plus ou moins volontaire, à être exposés à des contenus inappropriés en particulier sur les réseaux sociaux, notamment à "*des vidéos de violence graphique, des contenus pour adultes, des vidéos d'automutilation, des défis dangereux sur les médias sociaux, des vidéos banalisant la guerre, des conseils sur les troubles de l'alimentation et des encouragements à parier et à s'adonner à des jeux d'argent*"[63]. Au titre de ces contenus, une attention particulière doit être portée aux contenus violents et à caractère pornographique (**Chapitre 7**), aux contenus incitant à des conduites à risque (**Chapitre 8**) ainsi qu'aux contenus susceptibles d'affecter la perception de soi en ce qu'ils promeuvent les troubles du comportement alimentaire, l'automutilation voire le suicide (**Chapitre 9**).

Toutes les pratiques précédemment considérées peuvent produire un effet différent selon le profil du mineur. Dès lors, il convient d'envisager les pratiques relatives aux mineurs appartenant à des groupes protégés dans la mesure où, si l'utilisation des réseaux sociaux produit des effets communs pour tous, les mineurs présentant certaines caractéristiques sont susceptibles d'être affectés de manière disproportionnée (**Chapitre 10**).

[62] Conseil de l'Europe, Les types de cyberviolence.
[63] Commission européenne, BIK plus Strategy 2025, First évaluation of the European Strategy Better Internet for Kids (BIK +), February 2025, p. 26.

CHAPITRE 3 : CYBERHARCÈLEMENT

3.1. PRATIQUES

Dans un rapport sur la cartographie de la cyberviolence, adoptée en 2018, le Comité de la Convention sur la cybercriminalité définit la cyberviolence comme "*l'utilisation de systèmes informatiques pour causer, faciliter ou menacer une violence à l'encontre d'un individu*" pouvant entraîner un préjudice physique, sexuel, psychologique ou économique. Cette définition encadre ainsi un ensemble de violences spécifiques rendues possibles ou amplifiées par le numérique telles que le cyberharcèlement, l'atteinte à l'intimité, l'incitation à des conduites à risque, l'exposition à des contenus choquants. Quant au Conseil de l'Europe, il définit le cyberharcèlement comme un "*comportement persistant et répété visant une personne spécifique, conçu pour provoquer une détresse émotionnelle grave et souvent la crainte d'un préjudice physique*".

Parmi les principales formes de cyberharcèlement recensées, on retrouve notamment :

- les insultes, moqueries, menaces adressées directement à la victime via des messages privés ou des commentaires publics ;
- le *doxxing* : publication d'informations personnelles (adresse, numéro de téléphone, données privées) afin d'exposer la victime à des dangers extérieurs ;
- la diffusion non consentie d'images intimes : publication de photos ou vidéos compromettantes sans le consentement de la victime ;
- l'usurpation d'identité : création de faux profils pour nuire à la réputation de la victime ou la piéger dans des situations embarrassantes ;
- le *happy slapping* : agression filmée et diffusée en ligne à des fins de moquerie ou d'humiliation.

Si 99% des 11-17 ans utilisent au moins une plateforme en ligne[64], différentes études ont mis en lumière l'importance de leurs pratiques. Ainsi, pour la France, une étude de 2024 menée par la Caisse d'Épargne et l'association e-Enfance[65] relève que 18% des enfants ont déjà été confrontés à du cyberharcèlement. En outre, selon le ministère de l'Éducation nationale[66], en 2023, près de deux collégiens sur dix se déclaraient victimes d'insultes, d'humiliations ou de menaces diffusées sur les réseaux sociaux, par message. Par ailleurs, une étude de l'Organisation mondiale de la santé publiée en mars 2024[67] indique qu'un adolescent sur six en Europe a été victime de cyberharcèlement, avec des taux similaires entre garçons (15 %) et filles (16 %).

---

[64] Acrom, Mineurs en ligne : quels risques ? quelles protections ?, Synthèse de l'étude, Septembre 2025.
[65] Étude Caisse d'Épargne-association e-Enfance, Infographie AUDIREP, 2025.
[66] Ministère de l'Éducation nationale, Premiers résultats statistiques de l'Enquête harcèlement 2023.
[67] OMS, Une nouvelle étude de l'OMS/Europe révèle qu'un enfant d'âge scolaire sur 6 est victime de cyberharcèlement, 2024.

L'étude menée par la Caisse d'épargne et l'association e-Enfance[68] a relevé que les plateformes privilégiées pour le cyberharcèlement varient selon l'âge des utilisateurs. Les services de jeux en ligne peuvent être des lieux de harcèlement plus fréquent chez les jeunes garçons, tandis que les filles sont davantage victimes d'insultes et de rumeurs sur les réseaux sociaux, notamment par le biais de la diffusion non consentie de contenus intimes. Ce phénomène est souvent associé au cybersexisme, qui désigne l'utilisation des technologies numériques pour cibler et harceler les jeunes filles, en exploitant des stéréotypes de genre et des comportements sexistes[69].

Par ailleurs, il a pu être souligné que le cyberharcèlement est souvent lié à des contacts en personne dans des lieux partagés tels que l'école et peut s'intensifier en raison de la viralité des contenus sur les réseaux sociaux[70]. Certaines tendances numériques facilitent ces dynamiques, notamment les défis viraux incitant à humilier autrui et la culture de l'anonymat qui encourage les comportements malveillants sans crainte de sanctions ; la distance créée à travers l'écran favorisant également les passages à l'acte et encourage des comportements plus agressifs[71]. Il est en outre observé différents impacts du cyberharcèlement résultant de la permanence des contenus publiés et de leur diffusion rapide en ligne et virale.

3.2. CADRE JURIDIQUE

3.2.1. France et Union européenne

En droit français comme en droit de l'Union européenne, plusieurs dispositions sont consacrées à la lutte contre le cyberharcèlement. Elles prévoient à la fois des sanctions contre ces comportements, la mise en place de mécanismes de prévention et de sensibilisation - notamment en milieu scolaire - ainsi que des mesures de blocage ou de retrait des contenus concernés lorsqu'ils sont diffusés sur les réseaux sociaux.

Mesures répressives. Délit sanctionné sur le fondement de l'article 222-33-2-2 du Code pénal, le cyberharcèlement constitue une circonstance aggravante du harcèlement moral défini comme "*le fait de harceler une personne par des propos ou comportements répétés ayant pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou*

[68] Étude Caisse d'Épargne-association e-Enfance, Infographie AUDIREP, 2024.

[69] On peut notamment citer le "bodyshaming" qui désigne toute pratique visant à disqualifier, stigmatiser, marginaliser une personne ou un groupe de personnes en raison du physique ou de l'apparence. Par ailleurs, sur la progression des discours masculinistes et les phénomènes de polarisation, Haut Conseil à l'égalité, Etat des lieux du sexisme en France, Rapport 2025, p. 16, le masculinisme étant défini comme une "*idéologie prétendant que les hommes souffrent d'une crise identitaire parce que les femmes en général, et les féministes en particulier, dominent la société et ses institutions*".

[70] National Centre for Social Research, City, University of London, Key attributes and experiences of cyberbullying among children in the UK, 2024, p. 10.

[71] National Center for Social Research, étude préc.

mentale". Il est caractérisé dès lors que les faits mentionnés ont été commis par "*l'utilisation d'un service de communication au public en ligne ou support numérique ou électronique*" "*lorsque les faits ont été commis par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique*".

Concernant la mise en œuvre de l'article 222-33-2-2 du Code pénal, il convient de noter que les notions de "propos" et "comportement" sont largement définies en jurisprudence[72] et peuvent viser des paroles destinées à blesser comme des injures ou diffamations[73], des propos discriminatoires[74], de la révélation d'éléments relevant de la vie privée[75], d'images violentes[76], des faits d'usurpation d'identité ou encore des menaces[77]. La condition de "répétition" est constituée quant à elle lorsque le harcèlement a été commis par une seule personne et que les propos ou comportements ont été répétés[78], ce qui exclut les messages ou signes adressés de manière concomitante ou "*dans un seul et même trait de temps"*[79]. Pour les raids numériques - également connus sous le nom de harcèlement en meute -, en vertu des articles 222-33-2-2 a) et b), "*un comportement unique peut être incriminé dès lors qu'il s'inscrit soit dans un harcèlement concerté entre plusieurs auteurs ou à l'initiative de l'un d'eux, soit qu'il intervient dans le cadre d'un harcèlement imposé à la victime par une pluralité d'auteurs qui, sans se concerter, ont conscience d'une entreprise de harcèlement menée à l'encontre de la victime*"[80]. Enfin, "l'altération des conditions de vie" est subordonnée à une altération de la santé physique ou mentale, requise dans la caractérisation du délit de cyberharcèlement. Selon la jurisprudence, la preuve de l'altération de la santé consiste en un examen médical pouvant prouver d'une incapacité de travail qui doit être constatée, même si cette dernière est fixée à 0 jour[81] ; à ce titre, la Cour d'appel de Nancy a relaxé quatre jeunes collégiens au motif qu'il n'était pas démontré que les actes auraient porté une "*atteinte effective à la santé physique ou psychique de la victime"*[82].

L'auteur de cyberharcèlement encourt jusqu'à 2 d'emprisonnement et 30 000 euros d'amende, et jusqu'à 3 ans d'emprisonnement et 45 000 euros d'amende si la victime est mineure et que les faits

[72] N. Verly, "Prédateurs numériques et meutes en ligne : l'appréhension du cyberharcèlement par le droit et la jurisprudence", *Légipresse* 2023, p. 664.
[73] T. corr. Strasbourg, 5 déc. 2019.
[74] T. corr. Paris, 17e ch., 13 sept. 2023 ; T. corr. Paris, 10e ch., 1re sect., 12 déc. 2022.
[75] Paris, pôle 2 - 8e ch., 28 sept. 2022.
[76] T. corr. Paris, 10e ch., 1re sect., 12 déc. 2022.
[77] Paris, pôle 2 - 8e ch., 31 janv. 2023 ; T. corr. Paris, 10e ch., 1re sect., 12 déc. 2022 ; T. corr. Paris, 24e ch., 20 avr. 2022.
[78] T. corr. Paris, 10e ch., 1re sect., 12 déc. 2022.
[79] Crim. 9 mai 2018, préc. ; T. corr. Paris, 10e ch., 1re sect., 12 déc. 2022.
[80] N. Verly, article préc. La condamnation peut être encourue même pour l'envoi d'un seul message dès lors qu'en raison de "la médiatisation" et de "*la visibilité*" de la victime, "*les utilisateurs ne pouvaient ignorer qu'ils s'inscrivaient dans une forme de répétition*" : affaire Mila, Tribunal corr. Paris, 7 juil. 2021.
[81] N. Verly, article préc. et la jurisprudence citée : Paris, pôle 2 - 8e ch., 31 janv. 2023 ; Aix-en-Provence, 20 juin 2022 ; Versailles, 28 sept. 2021 ; T. corr. Paris, 17e ch., 13 sept. 2023 ; T. corr. Paris, 10e ch., 1re sect., 12 déc. 2022 ; T. corr. Strasbourg, 5 déc. 2019.
[82] Cour d'appel Nancy, 6 nov. 2023.

ont été commis par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique[83]. Les raids numériques sont passibles de peines équivalentes[84]. En outre, ce délit peut être sanctionné d'une peine complémentaire de suspension du compte d'accès au service en ligne utilisé pour commettre l'infraction. Cette peine, introduite par la Loi SREN de mai 2024, permet au juge d'ordonner le bannissement temporaire d'un individu du réseau social. Conformément à l'article 131-35-1 du Code pénal, "*La suspension est prononcée pour une durée maximale de six mois ; cette durée est portée à un an lorsque la personne est en état de récidive légale. Pendant l'exécution de la peine, il est interdit à la personne condamnée d'utiliser les comptes d'accès aux services de plateforme en ligne ayant fait l'objet de la suspension ainsi que de créer de nouveaux comptes d'accès à ces mêmes services*". La Loi SREN a également consacré une nouvelle peine complémentaire ou alternative à l'emprisonnement de stage visant à sensibiliser au respect des personnes dans l'espace numérique et à la prévention des infractions commises en ligne, dont le cyberharcèlement[85].

S'agissant du droit de l'Union européenne, la Directive 2024/1385 du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique définit le cyberharcèlement comme "*le fait d'adopter, de manière répétée ou continue, un comportement menaçant envers une personne, au moins lorsque ce comportement inclut des menaces de commettre des infractions pénales, au moyen de TIC et lorsque ce comportement est susceptible de conduire la personne à craindre sérieusement pour sa propre sécurité ou celle de personnes à charge*" et prévoit, en son article 7, que "*les États membres veillent à ce que les comportements intentionnels suivants soient passibles de sanctions en tant qu'infractions pénales:*

1. *le fait d'adopter, de manière répétée ou continue, un comportement menaçant envers une personne, au moins lorsque ce comportement inclut des menaces de commettre des infractions pénales, au moyen de TIC et lorsque ce comportement est susceptible de conduire la personne à craindre sérieusement pour sa propre sécurité ou celle de personnes à charge ;*
2. *le fait d'adopter, de manière publiquement accessible, avec d'autres personnes et au moyen de TIC, un comportement menaçant ou insultant envers une personne, lorsque ce comportement est susceptible de causer un préjudice psychologique important à cette personne ;*
3. *l'envoi non sollicité, au moyen de TIC, d'une image, d'une vidéo ou d'un autre matériel similaire représentant des organes génitaux à une personne, lorsqu'un tel comportement est susceptible de causer un préjudice psychologique important à cette personne ;*
4. *le fait de rendre accessible au public, au moyen de TIC, du matériel contenant les données à caractère personnel d'une personne, sans le consentement de cette dernière, dans le but d'inciter d'autres personnes à causer un préjudice psychologique important ou un préjudice physique à cette personne*".

[83] Code pénal, article 222-33-2.

[84] Code pénal, article 222-33-2 a) et b).

[85] Code pénal, article 131-5-1, 9°. Sur sa mise en œuvre, v. la Circulaire du Garde des Sceaux du 19 décembre 2024.

Il convient de relever que le nombre de plaintes déposées et de poursuites pour cyberharcèlement reste limité. Ceci peut notamment s'expliquer par le manque de preuves (par exemple en l'absence de captures d'écrans obtenues par les victimes) ainsi que par les difficultés relevées en pratique dans la prise en charge, la gestion et l'engagement des poursuites par les autorités compétentes, et notamment les enquêteurs. Une autre difficulté tient à la définition même du cyberharcèlement. D'une part, la condition propre du "caractère répété", telle qu'appréciée en jurisprudence, peut susciter le questionnement, notamment lorsqu'un seul message est envoyé sur plusieurs plateformes. D'autre part, l'élément constitutif de "dégradation des conditions de vie" paraît difficilement caractérisé en l'état ce qui limite les poursuites. Enfin, il peut être relevé un manque de coopération de la part des plateformes avec les services d'enquête.

Mesures de prévention. Différentes mesures de prévention ont également été récemment consacrées afin de renforcer les dispositifs de lutte contre le cyberharcèlement. Tout d'abord, l'article 3 de la Loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne prévoit que les plateformes doivent rendre "*visibles à leurs utilisateurs des messages de prévention contre le harcèlement défini à l'article 222-33-2-2 du même code et indiquent aux personnes auteurs de signalement les structures d'accompagnement face au harcèlement en ligne*". En outre, la Loi SREN est venue compléter les dispositifs de formation aux usages numériques pour viser spécifiquement le cyberharcèlement. Ainsi, son article 8 modifie l'article L. 611-8 du Code de l'éducation pour préciser que la formation à l'utilisation des outils et des ressources numériques et à la compréhension des enjeux qui leur sont associés dispensée dès l'entrée dans l'enseignement supérieur comporte *"une sensibilisation à la citoyenneté numérique, aux droits et aux devoirs liés à l'utilisation d'internet et des réseaux sociaux, à la prévention des violences sexistes et sexuelles commises par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique et à l'usage des dispositifs de signalement de contenus illicites mis à disposition par les plateformes"*. L'article 9 de la Loi SREN prévoit également la remise d'un rapport du Gouvernement au Parlement sur les actions de prévention et de sensibilisation au harcèlement, y compris au cyberharcèlement, mises en place dans les établissements scolaires. Ce rapport devra notamment évaluer la possibilité de rendre obligatoire une session annuelle de sensibilisation aux enjeux de harcèlement, dont le cyberharcèlement et la façon dont la lutte contre le harcèlement est incluse dans la formation initiale et la formation continue de l'ensemble des personnels des établissements scolaires[86]. Si l'intérêt pour ces formations et ces informations annuelles sur le numérique et ses

[86] Le rapport n'est pas encore publié. Cela étant, le Sénat avait déjà remis un rapport d'information sur la question (Sénat, Rapport d'information fait au nom de la mission d'information sur le harcèlement scolaire et le cyberharcèlement (1) sur le harcèlement scolaire et cyberharcèlement : mobilisation générale pour mieux prévenir, détecter et traiter, par Mme Colette Mélot, 22 sept. 2021). Par ailleurs, le ministère de l'Éducation nationale a mené une enquête sur le harcèlement en novembre 2023 auprès d'un échantillon de 21 700 élèves du CE2 à la Terminale. Celle-ci révèle notamment que « *5 % des écoliers déclarent avoir reçu « souvent » ou « très souvent » des messages insultants ou menaçants le concernant de la part d'un ou plusieurs élèves sur un téléphone portable, sur les réseaux sociaux ou sur une plateforme de jeux en ligne (14 % en incluant les élèves ayant répondu « parfois »)* » : Direction de l'évaluation, de la prospective et de la performance (DEPP), Premiers résultats

enjeux allant du primaire au supérieur est à saluer, les moyens humains et financiers mis en œuvre pour s'assurer de leur qualité et de leur effectivité devraient être repensés.

Obligations incombant aux fournisseurs de service. Concernant la diffusion de ces contenus sur un réseau social, le fournisseur du service est tenu, en application de l'article 6 du DSA, de supprimer promptement ces contenus clairement illicites dès lors qu'ils leur sont notifiés dans les conditions prévues par le texte, en particulier lorsque le signalement lui a été adressé par un signaleur de confiance[87]. En outre, l'article 6 IV-A de la LCEN favorise la coopération entre ce service numérique et les autorités compétentes en lui imposant de signaler les contenus illicites constituant les infractions les plus graves dont le cyberharcèlement, et à fournir des informations pour identifier le ou les auteurs. Par ailleurs, en application de l'article 28 du DSA, le fournisseur de service de réseau social devra respecter une obligation de "Safety by design" en vertu de laquelle il devra 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[88]. Pour les opérateurs désignés comme très grandes plateformes, ils sont également tenus de réaliser une analyse de risques (article 34) et de mettre en œuvre des mesures d'atténuation afin de protéger les droits de l'enfant ainsi que leur santé physique et mentale (article 35)[89].

3.2.2. États-Unis

Droit fédéral. Aux États-Unis, le droit fédéral opère une distinction entre le cyberharcèlement (*cyberstalking*) et la cyberintimidation (*cyberbullying*). Le cyberharcèlement est défini comme un comportement ayant pour but de tuer, blesser, harceler, intimider ou surveiller une personne en utilisant des services de communication électronique, y compris le courrier électronique et les plateformes en ligne. Ce comportement est sanctionné lorsqu'il cause, tente de causer ou est raisonnablement susceptible de provoquer une détresse émotionnelle chez la victime. Parmi les pratiques courantes figurent l'envoi répété de messages menaçants, le traçage en ligne (doxxing), ou encore la surveillance intrusive via des outils numériques. La cyberintimidation, quant à elle, se distingue par l'accent mis sur la "crainte physique" qu'elle induit chez la victime. Il s'agit de placer intentionnellement une personne dans une peur raisonnable pour sa sécurité ou celle de ses proches, en diffusant des informations personnelles (comme des images ou des messages privés) sans son consentement. Un exemple courant est la publication de photos ou d'informations personnelles accompagnées d'une incitation à harceler la personne ciblée (doxxing accompagné de swatting). La différence entre ces pratiques réside dans l'intention et l'effet produit : le cyberharcèlement vise une détresse émotionnelle prolongée et un contrôle sur la victime, tandis que la cyberintimidation cherche à initier une peur immédiate et concrète pour sa sécurité physique.

---

statistiques de l'enquête harcèlement 2023 : Document de travail – série études n° 2024-E02, févr. 2024.

[87] Sur ce point, v. Chapitre 2, pt. 2.1.2.5.

[88] Sur ce point, v. Chapitre 11 Conception, "Safety by design".

[89] Sur ce point, v. Chapitre 2, pt. 2.1.2.4. développements consacrés aux analyses de risques.

Le U.S. CODE § 2261A - STALKING vise spécifiquement le cyberharcèlement[90] (*cyberstalking*). Le texte prévoit différentes peines d'emprisonnement pour toute personne qui utilise les technologies de communication électronique pour "*adopter un comportement qui place une personne, un membre de la famille immédiate, un conjoint ou un partenaire intime dans une crainte raisonnable de mort ou de blessure corporelle grave, ou qui cause, tente de causer ou serait raisonnablement susceptible de causer une détresse émotionnelle substantielle à une personne*". Il est prévu une circonstance aggravante si la victime est âgée de moins de 18 ans[91].

S'agissant des fournisseurs de service numérique, la Section 230 du Communications Decency Act[92] leur accorde une double immunité. D'une part, ils ne peuvent voir leur responsabilité engagée du fait des contenus publiés par les utilisateurs (*Safe Harbor*). D'autre part, une « immunité du bon samaritain » leur permet de restreindre ou supprimer de bonne foi des contenus que le fournisseur du service ou l'utilisateur considère notamment comme "*harassing*", les règles de modération étant librement définies par chaque plateforme. Il convient toutefois de souligner que, pour renforcer la protection des enfants, le Kids Online Safety Act (KOSA)[93] en cours de discussion propose d'introduire un devoir de vigilance (*duty of care*) en matière de protection des mineurs (Section 3) qui enjoindrait aux plateformes de prendre des mesures raisonnables en ce qui concerne la conception et l'exploitation de leurs services afin de limiter les risques notamment de "*cyber bullying"* et de "*harassment of minor"*[94].

Droit étatique. Les dispositions relatives au cyberharcèlement sont intégrées aux législations sur le harcèlement ou le harcèlement "criminel" et varient selon les juridictions. Généralement, le cyberharcèlement est qualifié de délit[95] ou de crime[96], selon la gravité des faits, la répétition des actes et l'impact sur la victime. La distinction repose sur la nature des menaces proférées, l'intention de nuire et les éventuels antécédents de l'auteur. Certaines lois ciblent spécifiquement le cyberharcèlement dans un cadre scolaire, imposant des obligations aux établissements en matière de prévention, de signalement et de sanctions disciplinaires[97]. Les infractions liées au cyberharcèlement peuvent englober divers comportements : menaces, diffusion non consentie d'informations personnelles, incitation à la haine ou au passage à l'acte, et harcèlement répété via des moyens électroniques. Dans certains cas[98], la législation exige que la victime ressente une "crainte raisonnable" pour sa sécurité ou une détresse émotionnelle avérée pour que l'infraction soit caractérisée. Enfin, plusieurs États prévoient une gradation des sanctions[99], avec des peines plus lourdes en cas de récidive, de violation d'une ordonnance de protection ou lorsque le harcèlement vise des victimes particulièrement vulnérables.

---

[90] 18 USC 2261A : Stalking.
[91] 8 USC 2261B : Enhanced penalty for stalkers of children.
[92] 47 USC 230: Protection for private blocking and screening of offensive material.
[93] Kids Online Safety Act (KOSA), S.1409 - 118th Congress (2023-2024).
[94] Sur ce point, v. Chapitre 11 "Conception des services", pt. 11.2.3.
[95] California Penal Code Part 1 - Title 15 - Chap 2 - § 653.2.
[96] Arizona Revised Statutes § 13-2923.
[97] Floride - Jeffrey Johnston Stand Up for All Students Act.
[98] California - California Penal Code Part 1 - Title 15 - Chap 2 - § 646.9.
[99] Arizona Revised Statutes § 13-707 : les peines prévues sont de 6 mois d'emprisonnement et de 2 500 dollars d'amende.

3.2.3. Angleterre et Pays de Galles

Mesures répressives. S'agissant du droit de l'Angleterre et du Pays de galles, plusieurs dispositions sanctionnent la cyberintimidation pouvant prendre différentes formes (envoi d'un message textuel menaçant, partage d'images, trolling - l'envoi de messages menaçants ou dérangeants sur les réseaux sociaux, les forums de discussion ou les jeux en ligne -, cyberflashing, etc.). Ainsi, le Protection from Harassment Act 1997[100] distingue le "*stalking*" et le "*harassment*". Le "*harassment*" est considéré comme une infraction passible de peines d'emprisonnement ne dépassant pas 6 mois ou/et d'une amende ne dépassant pas le niveau 5 de l'échelle standard[101]. Il en va de même du "*stalking*", sanctionné de peines d'emprisonnement ne dépassant pas 51 semaines ou/et d'une amende ne dépassant pas le niveau 5 de l'échelle standard[102].

Obligations incombant aux fournisseurs de service. En vertu de l'Online Safety Act 2023[103] et du Risk Assessment Guidance and Risk Profiles publié par l'OFCOM[104], l'intimidation est considérée comme un "contenu prioritaire" ("*priority illegal content*"). Les plateformes doivent ainsi mettre en place des systèmes efficaces de signalement, modérer activement les contenus et supprimer rapidement les publications nuisibles ; elles sont également tenues de fournir des outils permettant aux utilisateurs de bloquer ou de désactiver les commentaires abusifs[105]. En outre, les services en ligne sont tenus d'évaluer et d'atténuer les risques liés aux contenus illégaux et préjudiciables, tels que le harcèlement en ligne.

3.2.4. Australie

Concernant le droit australien, le cyberharcèlement est défini par l'Online Safety Act 2021 (OSA) comme une communication en ligne à destination ou à propos d'un enfant australien qui est gravement menaçante, gravement intimidante, gravement harcelante ou gravement humiliante. Il peut s'agir de messages, commentaires, courriels, mèmes, images et vidéos[106].

Au niveau fédéral, la Division 474.17 du Criminal Code Act de 1995[107] punit toute forme de harcèlement, menace, intimidation ou nuisance au moyen d'un service de télécommunication. Cette infraction est passible d'une peine maximale de 5 ans d'emprisonnement[108]. Au-delà, en cas

[100] Protection from Harassment Act (1997).
[101] Protection from Harassment Act, Section 2.
[102] Protection from Harassment Act, Section 2A.
[103] Online Safety Act 2023, Chapter 50, Part. 3, Chapter 2, s. 10.
[104] OFCOM, Protecting people from illegal harms online - Risk Assessment Guidance and Risk Profiles, 16 décembre 2024, 2.27, p.9.
[105] OFCOM, Illegal content Codes of practice for user-to-user services, 24 February 2025. V. en particulier : J "Users controls", ICU J1 User blocking and muting ; ICU J2 Disabling comments.
[106] Online Safety Act, 2021, Part 1, s. 6.
[107] Criminal Code Act, v. 2.
[108] Dans les cas de cyberharcèlement plus grave, d'autres dispositions du Criminal Code Act dans sa dernière version du 8 février 2025 prévoient des sanctions plus lourdes. Par exemple, le fait d'adresser

de cyberharcèlement, l'OSA consacre une procédure spécifique de dépôt de plainte auprès de l'eSafety Commissioner[109] au bénéfice d'un enfant australien (tout enfant de moins de 18 ans qui vit habituellement en Australie ou qui voyage temporairement à l'étranger) ou d'une personne responsable [110].

Dès lors qu'un enfant est victime de cyberharcèlement, l'eSafety Commissioner peut émettre un avis de retrait auprès du fournisseur d'un service de médias sociaux, d'un service électronique pertinent ou d'un service internet désigné en vertu de la Section 65 de l'OSA ainsi que d'un fournisseur d'hébergement désigné en vertu de sa Section 66 afin de retirer le contenu si une plainte a été déposée auprès du fournisseur de services et que le contenu n'a pas été supprimé dans les 48 heures suivant le dépôt de la plainte. La demande de retrait peut viser tout site de média social ainsi que d'autres services en ligne tels que les services de jeux en ligne, sites web, ou plateformes de messagerie directe. Le fournisseur de service en ligne dispose de 24 heures pour répondre ; ce délai peut être plus long dans certaines circonstances. Un avis (*end user notice*) peut également être adressé à l'utilisateur final qui a publié, partagé ou envoyé un contenu relevant du cyberharcèlement, en vertu duquel l'utilisateur final devra retirer le contenu, et, conformément à la Section 70 de l'OSA, cesser de publier, partager ou envoyer tout contenu relevant du cyberharcèlement, et présenter des excuses à l'enfant ciblé. L'eSafety Commissioner dispose de plusieurs moyens pour faire respecter ces avis, allant de l'émission d'un avertissement formel au prononcé de sanctions civiles.

une menace de mort via un service de télécommunication est passible d'une peine maximale de 10 ans d'emprisonnement (article 474.15).

[109] Online Safety Act, 2021, Part 3, s. 30-31.

[110] e-Safety Commissioner, Cyberbullying Scheme Regulatory Guidance, 2023 : pour 2023-2024, 2 693 plaintes ont été déposées, soit une augmentation de 40 % par rapport à la période précédente.

HARCÈLEMENT SEXUEL ET CYBER-FLASHING

PRATIQUE

Il s'agit d'une pratique exhibitionniste numérique consistant à exposer une personne qui ne l'a pas sollicité à une image à caractère sexuel. L'une de ces pratiques, couramment appelée "*dick pic*", consiste à envoyer une photo de sexe masculin sans le consentement du destinataire ; cette pratique concerne majoritairement les hommes envoyant une image de leurs organes génitaux en érection à des adolescentes[111]. L'image peut être envoyée sur un compte de réseau social ou de messagerie privée ou en utilisant la technologie bluetooth ou wi-fi de transfert d'image (AirDrop d'Apple).

CADRE LÉGAL

Droit français

L'article 222-32 du Code pénal prohibe l'exhibition sexuelle imposée à la vue d'autrui dans un lieu accessible aux regards du public qui est puni d'1 an d'emprisonnement et de 15 000 euros d'amende. La mention de "*lieu accessible au public* " pose difficulté dès lors que les "dick pic" sont envoyées par l'intermédiaire de service numérique.
Par conséquent, il conviendrait d'ajouter au Code pénal une nouvelle incrimination visant spécifiquement ce type de pratique, comme le recommande la CNCDH, dans le prolongement de l'infraction désormais consacrée par l'OSA au Royaume-Uni[112].

Par ailleurs, l'article 222-33 du Code pénal pourrait s'appliquer afin d'incriminer des faits relevant du harcèlement sexuel, par exemple dans l'hypothèse où la dick pic est imposée à une personne de façon répétée et porte atteinte à sa dignité en raison du caractère dégradant ou humiliant.

Droit de l'Angleterre et du Pays de Galle

La Partie 10 de l'Online Safety Act a modifié le Sexual Offences Act[113] pour reconnaître le "cyber-flashing" comme une nouvelle infraction pénale en Angleterre et au Pays de Galles[114]. Cette pratique est ainsi clairement identifiée comme contraire à l'ordre public. Le partage ou la menace de partage d'une photographie ou d'un film d'organes génitaux sans le consentement du destinataire est passible d'une peine d'emprisonnement maximale de deux ans et/ou d'une amende ainsi que d'une inscription au registre des délinquants sexuels pour une durée maximale de dix ans. Le 19 mars 2024, la première condamnation pour cyber-flashing a été prononcée en Angleterre et au Pays de Galles à l'égard d'un homme de 39 ans pour avoir envoyé des photos non sollicitées de son pénis à une jeune fille de 15 ans et à une femme ; il a été condamné à 66 semaines d'emprisonnement[115].

[111] Pour une description de ces pratiques, v. notamment National Academies Sciences Engineering Medicine, Social Media and Adolescent Health (2024), National Academies Press, p. 180 - également

3.3. PRÉCONISATIONS

Préconisation 3 - Améliorer la prise en charge, la gestion et l'engagement des poursuites concernant les plaintes déposées pour cyberharcèlement

a. Étendre le dispositif de la pré-plainte en ligne à l'infraction de cyberharcèlement en permettant notamment aux victimes de pouvoir télécharger en ligne les éléments de preuve susceptibles de contribuer à la manifestation de la vérité et à la recherche des auteurs.

b. Renforcer la formation des enquêteurs à l'accueil des victimes et mettre l'accent sur les enjeux de dépréciation de soi et de sentiment d'insécurité pour les victimes de cyberharcèlement. Éviter que, lors de la prise de la plainte ou lors des auditions, des remarques autour de l'utilisation faite des moyens de communication en ligne blessent davantage des victimes déjà éprouvées.

c. S'assurer que les policiers et gendarmes respectent leur obligation de prendre toute plainte et notamment pour cyberharcèlement ou tentative de cyberharcèlement, l'opportunité des poursuites étant du ressort exclusif du procureur.

d. Renforcer la collaboration entre les autorités compétentes et les plateformes afin de faciliter l'identification des auteurs anonymes de cyberharcèlement, notamment en simplifiant le processus de remontée jusqu'à l'adresse IP (notamment par l'automatisation des demandes d'adresse IP auprès des réseaux).

e. Renforcer la coopération policière et judiciaire aux fins de pouvoir mener des enquêtes efficaces lorsque les auteurs de cyberharcèlement sont situés à l'étranger.

Préconisation 4 - Réviser la définition de cyberharcèlement retenue dans le Code pénal

a. Concernant l'auteur du délit, reconnaître que le caractère répétitif est atteint à partir de deux actions de harcèlement, même si les plateformes utilisées ne sont pas les mêmes ; considérer qu'un acte très grave même isolé peut suffire à caractériser le cyberharcèlement ; détailler ce que recouvre le cyberharcèlement d'ambiance. Par ailleurs, une circulaire de politique pénale pourrait

---

CyberNetic, "Dick pic, Etiologie des pratiques de cyberharcèlement" précisant que "*la fonctionnalité AirDrop d'Apple permet d'envoyer par bluetooth et wi-fi toutes sortes de documents (dont les photos) entre utilisateurs de la marque qui se situent à moins de 9 mètres de distance, sans passer par une adresse courriel ou par un numéro de téléphone. Si les réglages de réception AirDrop ne sont pas bien paramétrés, la victime peut être facilement détectable par un agresseur à proximité et recevoir des photos de pénis sans qu'elle n'y ait consenti. Même en refusant l'image, elle aura pourtant un aperçu clair et net du cliché*".

[112] CNCDH, Avis 2025-1 sur la protection de l'intimité des jeunes en ligne, 2025, recommandation n°21.

[113] Sexual Offences Act, 2003.

[114] Sexual Offences Act, Section 66 A.

[115] Crown Prosecution service, "Prison sentence in first cyberflashing case" (CPS, 19 mars 2024).

utilement rappeler aux parquets que les règles de poursuite applicables au harcèlement dans l'espace physique ont vocation à s'appliquer au cyberharcèlement :

b. Concernant la victime, une circulaire de politique pénale pourrait inviter les parquets à entendre de façon extensive l'élément constitutif de "dégradation des conditions de vie", notamment aux fins de ne pas conditionner la caractérisation de l'infraction à l'existence d'un arrêt de travail.

Préconisation 5 - Considérer les conséquences psychologiques et admettre que le cyberharcèlement peut être constitué dès lors que des propos illicites sont tenus

Chaque propos s'inscrivant dans le cadre du cyberharcèlement peut être ressenti comme une agression, qui du fait de son intensité et/ou de sa répétition peut engendrer un traumatisme complexe, avec un retentissement psychologique important de nature à dégrader durablement et profondément les conditions de vie des victimes. Il serait utile de conduire des recherches afin d'évaluer les dommages constatés afin de pouvoir éclairer les juridictions qui se prononcent sur la réparation du préjudice subi (dommages et intérêts).

Préconisation 6 - Évaluer l'évolution de l'incidence des sanctions

Le montant des sanctions prononcées s'avère pour l'heure insuffisant pour prévenir tout risque de récidive et dissuader d'autres auteurs d'agir de la même manière. Il est important de mesurer l'évolution des quantums de peines prononcées au regard des peines encourues.

Le moment où intervient la sanction est essentiel pour produire un effet sur le sentiment d'impunité et pour prévenir la récidive. À cet égard, plus les sanctions sont prises rapidement après la commission de l'infraction, plus leur utilité est grande.

Il faudrait en outre veiller à ce que les parquets communiquent sur les sanctions prononcées aux fins de faire reculer le sentiment d'impunité.

Préconisation 7 - Améliorer l'accessibilité et l'efficacité de la modération

a. Faciliter les demandes de signalement par l'institution d'un bouton de signalement et un formulaire unique (accessible en français). Plus généralement, mettre à disposition des mineurs des mécanismes de signalement adaptés et facilement accessibles leur permettant de signaler du contenu, des activités, des individus et comptes ou des groupes qui enfreignent les CGU ou qu'ils jugent indésirables (*Commission européenne, Lignes directrices sur l'article 28, 10 octobre 2025*).

b. Imposer aux plateformes de traiter ces signalements à brefs délais

c. S'assurer que tous les outils, caractéristiques, fonctionnalités, paramètres, options et mécanismes de signalement, de rétroaction et de plainte sont adaptés aux enfants, adaptés à leur âge, faciles à trouver, à accéder, à comprendre et à utiliser pour tous les mineurs, y compris ceux ayant un

handicap et/ou des besoins supplémentaires en matière d'accessibilité, sont attrayants et ne nécessitent pas de changer d'appareil pour effectuer toute action impliquée (*Commission européenne, Lignes directrices sur l'article 28, 10 octobre 2025*).

d. Augmenter les moyens dans la détection automatique (par l'IA) de contenus haineux ou illicites en ligne

CHAPITRE 4 : DIFFUSION NON CONSENTIE D'IMAGES INTIMES

La diffusion non consentie d'images intimes, sous toutes ses formes, y compris la sextorsion, soulève des enjeux majeurs en matière de protection de la vie privée et de l'intimité, en particulier pour les mineurs. L'essor des réseaux sociaux, des applications de messagerie et de dénudage a favorisé le développement de ces pratiques, exposant les jeunes utilisateurs à de nouveaux risques. Ce phénomène appelle une réponse juridique adaptée, tant au niveau national qu'international. À ce titre, les législations en la matière se sont progressivement renforcées, avec pour objectif de mieux protéger les victimes et de sanctionner plus efficacement les auteurs.

4.1. PRATIQUES

À titre général, la diffusion non consentie d'images intimes est définie à l'article 226-2-1 du Code pénal comme "*le fait de diffuser, de porter à la connaissance du public ou d'un tiers, en l'absence d'accord de la personne concernée, tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne"*.

Cette pratique inclut aussi bien les photos et les vidéos que les conversations à caractère sexuel tenues à titre privé, réalisées avec ou sans l'accord de la personne concernée. Le contenu peut notamment être créé et communiqué avec le consentement de la personne dans le cadre de pratique de "*sexting*" - pratique désignant l'échange de contenus à caractère sexuel (également appelés "*nudes*") par messages ou par chat sur les réseaux sociaux[116]. Le partage de ce type de contenu peut également résulter de pratiques dites de sextorsion qui désigne une forme de chantage par lequel la victime, sous la menace de diffusion, est contrainte d'envoyer davantage de contenus à caractère sexuel ou de payer une somme d'argent[117].

Le partage non consenti de contenus intimes se matérialise par la diffusion de ces contenus sur les messageries privées, en utilisant les technologies de transfert de fichiers sans fil[118] (ex : Airdrop) ou encore par leur diffusion sur les comptes de réseaux sociaux. À cet égard, il convient de

[116] e-Enfance, Revenge porn et Fisha, des violences en ligne à l'égard des jeunes femmes en hausse en 2020 sur la plateforme d'assistance 3018 gérée par l'Association e-Enfance, 2021.

[117] Il convient toutefois de relever que la diffusion non consentie d'images intimes est sanctionnée en tant que telle, indépendamment de tout chantage puisque l'infraction est caractérisée dès lors que ces contenus sont partagés sans l'accord de la personne concernée. Comme le souligne Point de Contact, la principale différence réside ainsi dans l'intention et la temporalité des actes, bien qu'une sextorsion puisse, dans certains cas, aboutir à une diffusion non consentie du contenu (Point de Contact, Rapport annuel 2023, rapports d'activités, avril 2024, p. 50).

[118] The Crown prosecution service, Illegal sexual behaviour online including sharing and threatening to share intimate images and cyberflashing targeted in new CPS guidance, January 2024.

mentionner le cas particulier de "*compte fisha*". Il s'agit d'une pratique courante qui se matérialise à travers la création de groupes privés ou des comptes publics, créés par département, ville ou établissement scolaire, sur lesquels les auteurs diffusent des photos de jeunes femmes dénudées ("*nudes*") sans leur consentement, dans le but de les humilier[119]. Par ailleurs, il est fréquent que les comptes fisha donnent lieu à des pratiques de doxxing lorsque les publications comportent des informations relatives à la vie privée de la personne visée[120]. Ces différents vecteurs favorisent la propagation rapide de ces contenus, notamment en ce qui concerne les mineurs dans les établissements scolaires[121]. ll convient en outre de relever que les images intimes non consenties sont très présentes sur les plateformes pornographiques en raison du manque de restrictions mises en place par ces sites, comme a pu notamment le relever le rapport du Revenge Porn Helpline britannique soulignant que les plateformes pornographiques sont devenues le principal moyen de diffusion non consentie d'images intimes[122].

La diffusion non consentie de contenus intimes connaît une très forte croissante. Selon les chiffres d'une étude IPSOS conduite en 2021[123], 15% des 18-24 ans ont déjà été confrontés à la publication de photos dégradantes ou intimes. Plus largement, 12% des français déclarent avoir déjà été victimes d'une telle situation. En outre, en 2023, Point de contact a relevé une augmentation de plus de 1187% des contenus relevant de cette infraction[124]. Ce phénomène s'inscrit dans le contexte plus général des violences sexuelles et sexistes puisqu'il touche principalement les femmes et les jeunes filles qui sont exposées à 59% des violences en ligne[125] et sont de 1,5 à 2 fois plus touchées par le cybersexisme que les garçons[126].

---

[119] Définition par l'association #Stopfisha.

[120] À cet égard, l'article 223-1-1 du Code pénal créé par la Loi n°2021-1109 du 24 août 2021 confortant le respect des principes de la République prévoit une incrimination visant le fait de révéler, de diffuser ou de transmettre, par quelque moyen que ce soit, des informations relatives à la vie privée, familiale ou professionnelle d'une personne permettant de l'identifier ou de la localiser aux fins de l'exposer ou d'exposer les membres de sa famille à un risque direct d'atteinte à la personne ou aux biens, que l'auteur ne pouvait ignorer, punie de trois ans d'emprisonnement et de 45 000 euros d'amende en vertu du nouvel article 223-1-1 du Code pénal.

[121] UK Safer Internet Centre, Cyberflashing : Supporting victims of cyberflashing and giving preventative advice, 2022.

[122] Z. Ward, Revenge Porn Helpline Report, 2022, p. 15. Une analyse du contenu des sites pornographiques en 2021 a mentionné qu'"un titre sur huit (…) décrivait une activité sexuellement violente ou non consensuelle : v. Children's Commissioner, "A lot of it is actually just abuse", UK Children's Commissioner, January 2023.

[123] IPSOS, Cyberviolences et cyberharcèlement : état des lieux d'un phénomène répandu, 2021.

[124] Point de Contact, Rapport annuel 2023, p.51.

[125] e-Enfance,Revenge porn et Fisha, des violences en ligne à l'égard des jeunes femmes en hausse en 2020 sur la plateforme d'assistance 3018 gérée par l'Association e-Enfance, 2021.

[126] CIVIISE, Violences sexuelles faites aux enfants, Repérer et signaler, 2022.

4.2. CADRE JURIDIQUE

4.2.1. France et Union européenne

Mesures répressives. Depuis la Loi pour une République numérique du 7 octobre 2016[127], l'article 226-2-1 Code pénal incrimine le fait, en l'absence d'accord de la personne pour la diffusion, "*de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant des paroles ou images présentant un caractère sexuel, obtenu avec le consentement exprès ou présumé de la personne ou par elle-même*". La qualification du délit est caractérisée et ce, indépendamment de l'intention de l'auteur ou des moyens techniques de diffusion utilisés. Il suffit de diffuser un contenu sexuel en l'absence d'accord de la personne - ce qui vise également la diffusion secondaire-, étant précisé que le consentement à la captation n'emporte pas accord de diffusion dans les cas visés à l'article 226-2-1 du Code pénal. Les peines encourues peuvent aller jusqu'à 2 ans d'emprisonnement et 60 000 euros d'amende. Il convient toutefois de relever que la victime peut rencontrer des difficultés pour rapporter la preuve d'un partage non consenti de ses contenus intimes surtout lorsque le contenu est partagé de manière privée, notamment par le biais de technologies de transfert de fichiers sans fil (ex : Airdrop), ou encore lorsque le contenu est partagé au moyen de services de messagerie cryptées[128]. Dans l'hypothèse où le contenu est manipulé ou généré artificiellement à l'aide d'un système d'IA générative, les dispositions prévues à ce titre trouveront à s'appliquer[129].

Si la victime est un mineur, la diffusion non consentie d'images intimes pourra être qualifiée de pédocriminalité, passible de sanctions plus sévères. L'article 227-23 du Code pénal incrimine ainsi *"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"*. Si l'image ou la représentation concerne un mineur âgé de moins de 15 ans, le texte précise que la qualification de l'infraction est caractérisée même si elle n'a pas été commise dans le but de diffuser le contenu[130]. Les peines encourues sont de 5 ans d'emprisonnement et 75 000 euros d'amende et sont portées à 7 ans d'emprisonnement et 100 000 euros d'amende lorsqu'un

---

[127] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Avant 2016, l'application des textes du Code pénal posait difficulté dès lors que les articles 226-1 et 2 du Code pénal prohibaient le fait de porter à la connaissance du public ou d'un tiers l'image d'une personne se trouvant dans un lieu privé lorsque le document a été réalisé sans son consentement, visant ici la conservation, l'utilisation ou la diffusion de tout enregistrement ou document. Alors que quelques juridictions de fond avaient pourtant condamné certaines de ces pratiques sur ce fondement, la Cour de cassation a pour sa part écarté l'application de ce texte en pareille hypothèse, en raison de l'application du principe d'interprétation stricte de la loi pénale pour affirmer que "*n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement*" (Cass. Crim. 16 mars 2016, n°15-82676).

[128] C. Debarge, J. Prtorić, "The European-wide battle to crack down on revenge porn", *Equal times,* 23 February 2022.

[129] Sur ce point, v. infra Chapitre 6 "Deepfakes et atteinte à l'intimité".

[130] Ibid.

réseau de communications électroniques a été utilisé pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé.

Dans ces différentes situations, le juge pourra également ordonner une peine dite de "*suspension des comptes*" introduite par la Loi SREN[131].

Il convient en outre de relever que la Directive 2024/1385 du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique prévoit une disposition spécifique relative au "partage non consenti de matériels intimes ou manipulés". Ainsi, selon son article 5, "*Les États membres veillent à ce que les comportements intentionnels suivants soient passibles de sanctions en tant qu'infractions pénales :*
a) le fait de rendre accessibles au public, au moyen des technologies de l'information et de la communication (TIC), des images, des vidéos ou des matériels similaires montrant des activités sexuellement explicites ou les parties intimes d'une personne, sans le consentement de cette personne, lorsque ce comportement est susceptible de causer un préjudice important à cette personne ;
b) le fait de produire, de manipuler ou de modifier puis de rendre accessibles au public, au moyen des TIC, des images, des vidéos ou des matériels similaires donnant l'impression qu'une personne se livre à des activités sexuellement explicites, sans son consentement, lorsque ce comportement est susceptible de causer un préjudice important à cette personne ;
c) le fait de menacer de se livrer aux comportements visés au point a) ou b) afin de contraindre une personne à accomplir un acte déterminé, à y consentir ou à s'en abstenir".

Obligations incombant aux fournisseurs de service. En cas de diffusion d'un contenu intime non consenti sur un réseau social, en application de l'article 6 du DSA, le fournisseur du service est tenu de supprimer promptement le contenu dès lors qu'il est clairement illicite au regard de la notification qui lui est adressée, en particulier en cas de signalement réalisé par un signaleur de confiance[132]. En cas d'image ou de représentation d'un mineur présentant un caractère pornographique au sens de l'article 227-23 du Code pénal, il devra en outre le signaler aux autorités compétentes en application l'article 6 IV-A de la LCEN. Il convient par ailleurs de rappeler qu'en application de l'article 28 du DSA, les plateformes sont tenues d'une obligation de "Safety by design" en vertu de laquelle elles doivent 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[133]. Les très grandes plateformes doivent en outre réaliser une analyse de risques (article 34) et mettre en œuvre des mesures d'atténuation afin de protéger les droits de l'enfant ainsi que leur santé physique et mentale (article 35)[134]. Il convient de relever à cet égard que le premier rapport du European Board of Digital Services publié le 18 novembre 2025 mentionne au titre des risques systémiques majeurs la diffusion de contenus illicites tels que le partage non consensuel

[131] Pour plus de précisions, v. supra, Chapitre 3 "Cyberharcèlement".
[132] Sur ce point, v. 1ère partie de l'étude, développements consacrés au DSA et obligations de modération.
[133] Sur ce point, v. Chapitre 11 et développements consacrés à la conception et précisions relatives aux lignes directrices de l'article 28 du DSA du 14 juillet 2025.
[134] Sur ce point, Chapitre 2, pt. 2.1.2.4. consacrés aux analyses de risques.

d'images ou d'enregistrements intimes, les représentations de relations sexuelles non consensuelles, la pornographie illégale et l'exploitation sexuelle[135].

4.2.2. États-Unis

Droit fédéral. Au niveau fédéral, en vertu du 15 U.S. Code § 6851[136], les victimes de diffusion non consentie d'images intimes peuvent intenter une action civile afin de demander le retrait du contenu ainsi que l'allocation de dommages-intérêts compensatoires et punitifs, tout en préservant l'anonymat du plaignant ; le texte précise explicitement que le consentement de la personne représentée concernant la réalisation d'une image doit être distingué du consentement à sa diffusion. En outre, compte tenu du nombre croissant de signalements de partages non consentis de contenus intimes dont sont victimes en particulier les femmes et les mineurs, et afin de renforcer la protection de ces victimes et de prévenir de telles atteintes, le droit fédéral a été très récemment complété de nouvelles incriminations et d'obligations imposées aux fournisseurs de service.

Au titre des incriminations, le Tools to Address Known Exploitation by Immobilizing Technological Deepfakes On Websites and Networks (TAKE IT DOWN) Act adopté définitivement par le Congrès le 28 avril 2025[137] prohibe l'utilisation d'un *interactive computer service* pour publier sciemment la représentation visuelle intime d'une personne identifiable sans son consentement (*non consensual intimate visual depiction*), en distinguant la représentation authentique de la représentation générée artificiellement[138]. Une disposition spécifique incrimine le partage non consenti d'une représentation visuelle intime d'un mineur - âgé de moins de 18 ans - dans l'intention de (i) l'abuser, l'humilier, le harceler ou le dégrader, ou (ii) de susciter ou

---

[135] European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025, pt. 3.1.

[136] 15 USC 6851 - Civil action relating to disclosure of intimate images, modifié par le Violence Against Women (VAWA) Act 2022.

[137] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes On Websites and Networks (TAKE IT DOWN) Act, Public Law No. 119-12 (05/19/2025). Pour une explication du texte et de sa conformité à la Constitution, et en particulier au First amendment, v. le Memorandum The TAKE IT DOWN ACT: A Constitutional, targeted approach to addressing the spread of non consensual intimate imagery online, 8 April 2025.

[138] TAKE IT DOWN Act, s. 2, (2) A. : "*it shall be unlawful for any person, in interstate or foreign commerce, to use an interactive computer service to knowingly publish an intimate visual depiction of an identifiable individual who is not a minor if ': '(i) the intimate visual depiction was obtained or created under circumstances in which the person knew or reasonably should have known the identifiable individual had a reasonable expectation of privacy; '(ii) what is depicted was not voluntarily exposed by the identifiable individual in a public or commercial setting; "(iii) what is depicted is not a matter of public concern; and "(iv) publication of the intimate visual depiction "(I) is intended to cause harm or "(II) causes harm, including psychological, financial, or reputational harm, to the identifiable individual*" - Sur le partage non consenti de contenus générés par IA, v. infra, Chapitre 6 "Deepfakes et atteinte à l'intimité".

satisfaire le désir sexuel de toute personne[139], les peines encourues étant des peines d'amende et/ou de 3 ans d'emprisonnement[140].

Concernant les fournisseurs de service, il convient de rappeler qu'en vertu de la Section 230 du Communications Decency Act[141], ils ne peuvent voir leur responsabilité engagée du fait des contenus publiés par les utilisateurs et bénéficient d'une « immunité du bon samaritain » leur permettant de restreindre ou supprimer de bonne foi des contenus que le fournisseur du service ou l'utilisateur considère "*obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected*", sans engager leur responsabilité. Néanmoins, de nouvelles obligations sont désormais imposées aux plateformes par le TAKE IT DOWN Act afin de renforcer la protection des victimes. Elles seront tenues de mettre en place des mécanismes de signalement de partage non consenti de représentation visuelle intime faciles d'accès[142]. En cas de signalement et demande de retrait de la victime ou de son représentant respectant les conditions posées par le texte, elles se verront imposer une obligation de retirer le contenu au plus vite et au plus tard dans un délai de 48 heures[143]. Par ailleurs, le Kids Online Safety Act[144] (KOSA), en cours de discussion, propose d'introduire un devoir de vigilance ("*duty of care"*) en matière de protection des mineurs qui enjoindrait aux plateformes, en ce qui concerne la conception et l'exploitation de leurs services, de prendre des mesures d'atténuation des risques, notamment pour les cas de *sexual exploitation and abuse*[145] .

Au-delà, la diffusion de contenus représentant des personnes âgées de moins de 18 ans peut tomber sous le coup des dispositions particulières visant l'exploitation sexuelles de mineurs. Ainsi, la pédopornographie est sanctionnée au titre du United States Code[146] (USC) qui interdit la production, la distribution, la réception et la possession d'une image de pédopornographie (suffisamment explicite sur le plan sexuel) ; son paragraphe 2251 vise tout particulièrement le fait de persuader, d'inciter, de séduire ou de contraindre un mineur à se livrer à un comportement sexuellement explicite dans le but de produire des représentations visuelles de ce comportement. Il convient par ailleurs de relever que plusieurs textes ont été adoptés ou sont en cours de discussion afin de renforcer la lutte contre la diffusion de Child sexual abuse material (CSAM). À cet égard, le Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act[147], en cours de discussion, vise à criminaliser la distribution de représentations visuelles d'un mineur nu ; il s'agit ainsi de compléter le cadre légal pré-existant pour saisir les cas où les images exploitées ne répondent pas à la définition légale d'un comportement sexuellement explicite qui constitue de la pornographie enfantine. En outre, le Revising Existing Procedures On Reporting via Technology

[139] TAKE IT DOWN Act, s. 2, (2) B, modifiant le 47 USC 223.
[140] TAKE IT DOWN Act, s. 2, (4) B, modifiant le 47 USC 223.
[141] 47 USC 230: Protection for private blocking and screening of offensive material.
[142] TAKE IT DOWN Act, s.3 (2), modifiant le 47 USC 223.
[143] TAKE IT DOWN Act, s.3 (3). Sur les limites du texte, v. notamment CCRI, Statement on the Passage of the TAKE IT DOWN Act (S. 146), April 28 2025.
[144] Kids Online Safety Act (KOSA), S.1409 - 118th Congress (2023-2024).
[145] Sur ce point, v. Chapitre 11 " Conception des services".
[146] 18 USC 2251 : Sexual exploitation of children
[147] Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act, S.412 - 118th Congress (2023-2024).

(REPORT) Act[148] a modifié le cadre fédéral relatif au signalement des délits liés à l'exploitation sexuelle des enfants en ligne pour imposer de nouvelles obligations aux fournisseurs de services tenus de soumettre des rapports au National Center for Missing and Exploited Children (NCMEC)[149] lorsqu'ils ont connaissance d'infractions liées à l'exploitation sexuelle d'enfants en ligne[150].

Droit étatique. 49 des 50 États ont adopté une loi pour lutter contre la diffusion non consentie d'images intimes. Dans la majorité des États, la diffusion de contenus intimes non-consensuels constitue une infraction pénale si le défendeur a agi avec une intention spécifique ou en ayant connaissance de ce que la personne représentée n'avait pas consenti à la divulgation du contenu. En outre, plusieurs lois étatiques prévoient une incrimination des "abus sexuels de mineurs", notamment en ce qui concerne l'État de Virginie[151] et du Texas[152].

4.2.3. Angleterre et Pays de Galles

Définition. En Angleterre et Pays de Galles, la diffusion non consentie d'images intimes est définie par la Section 66B du Sexual Offences Act 2003[153] comme "*la divulgation d'une photographie ou d'un film sexuel réalisé sans le consentement de la personne qui y apparaît*". Tout d'abord, une image est qualifiée de *"privée"* si elle présente un contenu qui n'est pas habituellement visible en public. Ensuite, le contenu est considéré comme *"sexuel"* si une personne raisonnable juge qu'il l'est ou s'il montre tout ou partie des organes génitaux ou de la région pubienne d'une personne exposée. Enfin, la notion de *"divulgation"* peut être retenue dès lors que le contenu susmentionné est divulgué, présenté ou rendu disponible par quelque moyen que ce soit.

Mesures répressives. Le système judiciaire en Angleterre et au Pays de Galles reconnaît la nécessité d'un traitement différencié pour les enfants par rapport aux adultes. Lorsque la diffusion

[148] Revising Existing Procedures On Reporting via Technology (REPORT) Act, S.474, 118th Congress (2023-2024).
[149] Organisme américain de protection de l'enfance qui centralise les signalements des fournisseurs d'internet relatifs à l'exploitation en ligne des enfants, principalement via l'outil CyberTipline : http://www.cybertipline.com/.
[150] V. également le STOP CSAM Act of 2023 (S. 1199, 118th Congress (2023-2024)) - Strengthening Transparency and Obligation to Protect Children Suffering from Abuse and Mistreatment -, texte en cours de discussion qui vise à renforcer la protection des enfants victimes dans le cadre d'actions en justice, les actions de signalements dans le cadre de la CyberTipline, consacrer la responsabilité des plateformes en cas d'hébergement, stockage, promotion ou facilitation de CSAM en toute connaissance de cause, et prévoir la mise en place d'un programme de signalement et de retrait sur les plateformes et consacrer des possibilités de recours en cas de non retrait du contenus.
[151] Code of Virginia, Title 18.2 - Chapter 8 - Article 5 - §18.2-374.1:1. Possession, reproduction, distribution, solicitation, and facilitation of child pornography; penalty.
[152] Texas, Penal Code, Title 9 - Chapter 43. Public Indecency.
[153] Sexual Offences Act 2003, s. 66B.

non consentie d'images intimes implique un enfant de moins de 16 ans, elle est considérée comme un contenu d'abus sexuel sur mineur (CSAM). Ainsi, en application de la Section 1 du Protection of Children Act[154], sont interdits la création, la possession, la diffusion et le téléchargement d'images indécentes d'enfants de moins de 16 ans - qualifiées de Matériaux d'abus sexuel sur un mineur (CSAM) - en vue de leur distribution et ce, même si l'enfant a consenti à la création de cette image (par ex. à la prise d'une photographie intime le représentant) ; la peine maximale encourue est de 10 ans d'emprisonnement. La Section 160 du Criminal Justice Act de 1988[155] précise que la simple possession de ce type de matériel est illégale, et prévoit une peine maximale de 5 ans d'emprisonnement pour son auteur. De plus, les personnes condamnées pourront être inscrites au registre des délinquants sexuels et aux listes d'exclusion des enfants et des adultes.

La Section 66B du Sexual Offences Act 2003[156] définit les différentes infractions au titre du partage non consenti de contenus intimes (image ou vidéo) représentant une personne de plus de 16 ans. La diffusion non consentie d'images intimes peut être sanctionnée par une peine maximale de 2 ans d'emprisonnement et/ou une amende (selon la *mens rea* de l'auteur). Les menaces de diffuser ce contenu, qu'elles soient proférées en ligne ou hors ligne, sont passibles de la même peine que la diffusion sans qu'il soit nécessaire de prouver l'existence de l'image intime[157].

En outre, il convient de souligner qu'au-delà de la possibilité de poursuivre ces agissements sur le fondement d'une infraction pénale, plusieurs recommandations visent à consacrer la possibilité pour les victimes d'agir sur le fondement d'une action civile pour obtenir réparation du préjudice subi et le retrait des contenus visés[158].

Mesures préventives. L'Angleterre et le Pays de Galles adoptent plusieurs approches pour prévenir la diffusion non consentie d'images intimes tels le PSHE curriculum[159] (Personal, Social, Health and Economic education) qui permettent aux établissements scolaires d'intégrer des modules sur la sécurité en ligne, le consentement et le respect de la vie privée. Sont également promues des campagnes gouvernementales et associatives. A ce titre, l'outil gratuit "*StopNCII.org*"[160] (Stop Non-Consensual Intimate Images) opéré par le Revenge Porn Helpline permet aux victimes de signaler et de bloquer de manière préventive la diffusion de leurs images en ayant recours à la technique de hachage.

---

[154] Protection of Children Act 1978, s.1.
[155] Criminal Justice Act 1988, s. 160.
[156] Sexual Offences Act 2003, s 66B modifiée par le Online Safety Act 2023, Chapter 50, Part 10, s. 188.
[157] À cet égard, il convient de relever que l'incrimination du sexting pouvait précédemment poser difficulté. En effet, il est illégal pour un mineur de produire, posséder et distribuer des images sexuelles de lui-même ou d'autres mineurs, ce contenu pouvant être qualifié de CSAM. Compte tenu de l'augmentation des cas d'envoi de "nudes" entre enfants, le ministère de l'Intérieur britannique a lancé l'initiative "Outcome 21" en 2016 dans le but d'éviter la criminalisation des enfants pratiquant le "sexting" de manière innocente et consensuelle.
[158] House of Commons, Tackling non-consensual intimate image abuse, 2024-25, HC 336, March 2025, pt. 71.
[159] Gov.UK, Guidance Personal, social, health and economic (PSHE) education, 2021.
[160] V. https://stopncii.org/.

Obligations incombant aux fournisseurs de service. Au titre de l'Online Safety Act 2023[161], les fournisseurs de service sont tenus de supprimer les contenus illicites ayant fait l'objet d'un signalement ou dont ils ont connaissance d'une autre manière. Ils sont soumis à des obligations renforcées en matière de modération des contenus à caractère sexuel, notamment la diffusion non consentie d'images et les contenus d'abus sexuels sur mineur[162].

À cet égard, il convient de mentionner le rôle joué par le Revenge Porn Help Line qui propose un service de signalement et demande de retrait prioritaire auprès des réseaux sociaux ; pour renforcer l'effectivité de la lutte contre le partage de contenus intimes non consentis, des propositions préconisent désormais la création d'un organisme spécialisé dans la défense des victimes agissant comme signaleurs de confiance, sur le modèle du e-Safety Commissioner en Australie[163]. Par ailleurs, il est intéressant de relever que le Codes of practice publié par l'OFCOM recommande, en ce qui concerne les CSAM, de recourir au hachage perceptuel pour identifier ce type de contenus afin de les supprimer[164]. Les plateformes en ligne sont également tenues, en vertu de la Section 9 de l'Online Safety Act 2023, de procéder à une analyse des risques pour évaluer le risque de diffusion non consentie d'images intimes et de CSAM. Conformément à la Section 10, elles doivent prendre des mesures proportionnées pour atténuer et gérer efficacement ces risques ; elles doivent veiller à ce que le service ne soit pas utilisé pour la commission ou la facilitation de ces pratiques, et doivent recourir à des systèmes et des processus proportionnés conçus pour minimiser la durée de présence d'images intimes non consenties et de CSAM.

4.2.4. Australie

En Australie, la diffusion non consentie d'images intimes est abordée par un ensemble de dispositions législatives à la fois fédérales et étatiques, qui visent à pénaliser les menaces et la diffusion non consentie de contenus intimes, en particulier lorsqu'ils sont diffusés par des moyens de communication électronique. Ainsi, au niveau fédéral, la Section 474.17A du Criminal Code Act 1995 incrimine l'utilisation d'un "*carriage service*" pour diffuser du contenu à caractère sexuel représentant une personne majeure sans son consentement[165]. Cette infraction est passible d'une peine d'emprisonnement de 6 ans.

Lorsque la victime est une personne mineure, les faits seront poursuivis au titre des infractions relatives au Child Sexual Abuse Material (CSAM) sur le fondement des Sections 474.22, 474.22A et 474.23 qui incriminent l'utilisation d'un "*carriage service*" pour accéder à, rendre disponible, transmettre, promouvoir ou solliciter du matériel d'abus sexuel sur mineur ou encore la détention ou diffusion de ce type de contenus. Ces infractions sont toutes passibles d'une peine de 15 ans d'emprisonnement.

---

[161] Online Safety Act 2023, Chapter 50, Part. 3, Chapter 2, s. 10.
[162] Online Safety Act 2023, Chapter 50, Part. 3, Chapter 7, s. 59.
[163] House of Commons, rapport préc. pts. 75&s.
[164] OFCOM, Illegal content Codes of Practice for user-to-user services, 24 February 2025, pt. ICU C9.
[165] Criminal Code Act, v. 2.

En outre, l'article 75 de l'Online Safety Act 2021 (OSA)[166] interdit la publication en ligne ou la menace de publication d'images intimes d'une personne sans son consentement, ce qui ne vise pas la création de ce type de contenu. L'eSafety Commissioner se voit reconnaître plusieurs prérogatives pour lutter contre leur diffusion notamment sur les réseaux sociaux[167] en application de l'OSA. Ainsi, un système d'"*objection notice"* permet à toute personne de déposer une plainte auprès de l'eSafety Commissioner en cas de diffusion non consentie d'une image intime. L'eSafety peut alors conduire une enquête, notamment pour obtenir du fournisseur de service des informations appropriées telles que l'identité et les coordonnées de l'utilisateur final. De plus, l'eSafety Commissioner peut envoyer des avis aux plateformes en ligne et aux utilisateurs finaux ("*end user notice"*) afin d'obtenir le retrait d'une image intime dans un délai de 24 heures. En vertu de ses pouvoirs d'instruction corrective, l'eSafety Commissioner peut également exiger d'un utilisateur final qu'il prenne des mesures spécifiques pour réduire le risque de récidive, telles que la suppression des images en ligne et sur un appareil. Le non-respect des mesures correctives imposées par l'eSafety Commissioner peut entraîner des mesures coercitives.

[166] Online Safety Act, 2021.

[167] Online Safety Act, 2021 - eSafety Commissioner, Image-Based Abuse Scheme Regulatory Guidance, February 2024.

HACHAGE

Le hachage numérique est une solution technique qui peut être utilisée pour limiter la diffusion de contenus intimes. Selon la CNCDH[168], le hachage perceptuel peut être particulièrement efficace : en générant une empreinte numérique unique pour chaque image, il va permettre de détecter des contenus similaires même si ces derniers ont été légèrement modifiés. Cette méthode faciliterait le suivi et le retrait rapide des contenus issus d'une diffusion non consentie en ligne.

Le hachage numérique est utilisé par StopNCII[169] ou par le programme DISRUPT afin d'aider les victimes à protéger leur intimité en ligne en leur permettant de faire supprimer des contenus diffusés sans leur consentement. Ces dispositifs s'appuient sur une base de données répertoriant les signatures numériques des contenus signalés par les internautes. Cette base de hachage est ensuite mise à disposition des plateformes et réseaux sociaux partenaires afin de comparer les signatures numériques des contenus publiés sur leurs services avec celles enregistrées. Si une correspondance est détectée, le contenu est immédiatement identifié comme une image intime diffusée sans consentement, et sa publication est automatiquement bloquée.

QU'EST-CE QUE LE HACHAGE ?

Le hachage est un concept informatique utilisé pour créer des empreintes digitales de fichiers sur un système informatique.

La comparaison entre ces empreintes, stockées dans une base de données, est appelée correspondance de hachage. Il existe deux types principaux de correspondance de hachage : le hachage cryptographique, qui permet d'identifier des correspondances exactes entre les hachages (i), et le hachage perceptuel, qui permet de déterminer si les images ou vidéos sont très similaires, même si elles ont été modifiées (ii). Le hachage perceptuel évalue la similarité entre les contenus visuels et est utilisé pour détecter des contenus modifiés mais similaires. Ce dernier est souvent préféré pour identifier la diffusion non consentie d'images intimes.

Les fonctions de hachage perceptuel visent à générer des hachages très similaires pour des fichiers d'entrée très semblables, cherchant ainsi à refléter le niveau de similitude perçu par les humains à travers la distance entre les hachages perceptuels. Cette similarité est évaluée à l'aide d'une métrique de distance telle que la distance de Hamming, qui mesure le nombre de positions où les symboles correspondants diffèrent entre deux chaînes de symboles de même longueur. En utilisant une fonction de hachage perceptuelle, une métrique de distance de chaîne et un seuil de similitude acceptable, il est possible de déterminer si deux contenus sont perceptuellement similaires ou non. Le seuil de similitude acceptable peut varier en fonction du contexte.

Ces codes numériques générés sont ensuite stockés dans une base de données de hachages et partagés avec toutes les plateformes en ligne et les partenaires industriels participants au programme de hachage afin qu'ils identifient proactivement les contenus dans leurs services et les retirent plus rapidement. Lorsqu'un auteur tente de télécharger un contenu haché, les systèmes de filtrage basés sur les hachages analysent le contenu. Si une correspondance est trouvée dans

la base de données des hachages, le contenu est automatiquement bloqué et ne peut pas être diffusé en ligne.

Projet DISRUPT

Il s'agit d'un outil lancé par Point de Contact dans le cadre du Laboratoire de la protection de l'enfance le 9 novembre 2023 pour lutter contre la diffusion non consentie d'images intimes en permettant, par le recours à la technique de hachage, de retirer ou faire retirer des contenus déjà en ligne et d'anticiper une éventuelle diffusion en ligne[170].

Cet outil permet aussi de générer une empreinte des contenus concernés par le recours à la technologie de hachage. Après un signalement sur la plateforme DISRUPT, les contenus sont systématiquement vérifiés et hachés par la modération de Point de Contact. Si le contenu est publié en ligne, cette technologie permet à Point de Contact de l'identifier proactivement et d'œuvrer plus rapidement à son retrait. La signature numérique d'un contenu pourra être transmise aux partenaires de Point de Contact (dont les réseaux sociaux) afin qu'ils identifient proactivement les contenus et les retirent plus rapidement. Enfin, le contenu sera supprimé directement après traitement par les équipes, et seule une signature numérique (exemple de format : x12354ad) sera enregistrée et transmise.

[168] CNCDH, Avis sur la protection de l'intimité des jeunes en ligne, 2025, p.18.
[169] StopNCII, StopNCII.org.
[170] Point de contact, Laboratoire de la Protection de l'Enfance en ligne : lancement du projet DISpositif d'interRUPTion de diffusion de contenus intimes (DISRUPT).

ALGORITHME DE DÉTECTION DE NUDITÉ

Le plus souvent, les victimes de partage non consenti d'images intimes ne sont pas informées du fait que leurs images ont été téléchargées en ligne, ce qui les empêche de les signaler.

Le recours à des algorithmes de détection de la nudité permet de détecter proactivement cette diffusion non consentie afin d'en minimiser les conséquences en analysant les images et les vidéos à caractère sexuellement explicite qui impliquent généralement une certaine forme de nudité. En utilisant des bases de données étendues d'images explicites et des espaces de couleur, ces algorithmes peuvent identifier les tons de peau dans le spectre des couleurs, ce qui leur permet de traiter efficacement ce type de contenu. Le principal objectif de la détection ou de la classification de la couleur de la peau est de construire une règle de décision qui discrimine entre les pixels de peau et les pixels ne contenant pas de peau[171]. En traçant des "polygones de délimitation" autour des zones de pixels de tons de peau, ces algorithmes analysent l'intensité, le nombre et la proximité des pixels de peau, ainsi que le pourcentage de pixels de peau par rapport à la taille de l'image. Les grandes zones de pixels de peau ininterrompus sont souvent un indicateur de nudité. Une fois le contenu extrait et analysé, les systèmes de filtrage de la nudité utilisent des algorithmes pour classifier le contenu en fonction de sa nature "nue" ou "pornographique". Les plateformes en ligne peuvent ensuite prendre les mesures appropriées, telles que le retrait du contenu s'il s'agit d'une image intime non consentie ou son étiquetage en tant que "sensible".

4.3. PRÉCONISATIONS

Préconisation 8 - Renforcer les mesures de prévention et les mécanismes de modération
a. Envisager les mesures pertinentes à mettre en place afin de sensibiliser et responsabiliser les utilisateurs (mineurs) aux risques de détournement pouvant résulter de la publication d'un contenu intime et à l'exigence d'une preuve de consentement des personnes concernées, en veillant à respecter la vie privée et le secret des correspondances.
b. Informer l'utilisateur lorsqu'une capture d'écran de conversation ou de contenu échangé via son compte est réalisée et envisager le développement de solutions technologiques empêchant les captures d'écran. Réglez les comptes pour mineurs au plus haut niveau de confidentialité, de sûreté et de sécurité par défaut. Il s'agit notamment de concevoir des paramètres par défaut de manière à garantir des paramètres sûrs et adaptés à l'âge des mineurs, en tenant compte de l'évolution de leurs capacités. Ces paramètres doivent garantir que, par défaut pour tous les mineurs, au minimum : i. Les comptes n'autorisent que les interactions telles que les likes, les tags, les commentaires, les messages directs, les reposts et les mentions par des comptes qu'ils ont précédemment acceptés. ii. Aucun compte ne peut télécharger ou prendre des captures d'écran des informations de contact, de localisation ou de compte, ou du contenu téléchargé ou partagé par des mineurs sur la

[171] R. Ap-apid, "An Algorithm for Nudity Detection", *College of Computer Studies De La Salle University*, 2005 (citation originale : *"the main goal of skin colour detection or classification is to build a decision rule that will discriminate between skin and non-skin pixels"*).

plateforme. iii. Seuls les comptes que le mineur a précédemment acceptés peuvent voir son contenu, ses publications et ses informations de compte. iii. Personne ne peut voir les activités du mineur telles que « aimer » le contenu ou « suivre » un autre utilisateur (*Commission européenne, Lignes directrices, 14 juillet 2025, 6.3.1- 57.b*).

c. Encourager les plateformes à adopter des outils de hachage perceptuel et cryptographique pour identifier et bloquer automatiquement les contenus intimes non consentis avant leur diffusion. Développer des moyens techniques de hachage des contenus pédocriminels afin qu'ils ne soient pas re-diffusés sur des réseaux pédocriminels. (*Commission européenne, Lignes directrices, 14 juillet 2025, 6.7- 72.g*)

Sources : projet DISRUPT - OFCOM, Illegal content Codes of Practice for user-to-user services, pt. ICU C9.

c. Étudier l'opportunité d'inciter les réseaux sociaux à mettre en œuvre des algorithmes d'apprentissage automatique de détection de la nudité afin de limiter le partage non consenti de contenus intimes.

d. Étudier l'impact du programme Lantern ayant mis en place une coopération entre différentes plateformes[172] afin de permettre que, lorsqu'un compte, une adresse mail ou un numéro de téléphone relié à un compte est supprimé pour grooming, cela emporte le blocage des comptes détenus sur d'autres plateformes partenaires reliés à ces mêmes identifiants ; au-delà, envisager la faisabilité de bloquer l'adresse IP d'un utilisateur qui tente de recréer un compte signalé et supprimé pour grooming.

Préconisation 9 - S'assurer que la diffusion non consentie d'images intimes et les abus sexuels d'enfant en ligne soient inclus dans les analyses de risques imposées aux très grandes plateformes et moteurs de recherche au titre de l'article 34 du DSA et suffisamment documentés dans les rapports annuels publiés par ces opérateurs. Les mesures d'atténuation des risques prévues au titre de l'article 35 du DSA pourraient inclure le recours à la technologie de hachage.

Source : OFCOM, Illegal content Codes of Practice for user-to-user services, pt. ICU9.

Préconisation 10 - Abandonner le terme "Revenge Porn" pour privilégier celui de "diffusion non consentie d'images intimes" (NCII), qui est plus précis et moins stigmatisant dès lors que la diffusion n'est pas toujours motivée par la vengeance ni assimilable à de la pornographie. L'expression peut renforcer le "victim-blaming" et masquer d'autres motivations, comme l'humiliation, le chantage ou la gratification personnelle (des organismes comme Point de Contact et la Commission juridique britannique soulignent l'inadéquation du terme).

[172] Le programme LANTERN porté par plusieurs opérateurs comme Meta, Snapchat, TikTok, X, Discorde, Google, Microsoft, Amazon, Yubo ou encore Roadblox, en partenariat avec le National Center for Missing and exploiting children, le Safe Online et le We Protect Global Alliance propose de lutter contre le grooming et la sextorsion. Ce programme prévoit une coopération entre les plateformes afin de permettre de bloquer des adresses mail/identifiants d'une personne auteure de grooming et éviter que cette dernière puisse se recréer un compte.

CHAPITRE 5 : CHANTAGE ET EXPLOITATION DE MINEURS EN LIGNE (SEXTORSION)

5.1. PRATIQUES

La sextorsion est définie comme une forme de chantage par laquelle une personne exploite la menace de rendre public un contenu intime - images ou vidéos à caractère sexuel - afin d'obtenir de la victime des faveurs sexuelles, de l'argent ou tout autre avantage[173].

Les auteurs de sextorsion ciblent souvent leurs victimes par le biais de services numériques tels que les applications de rencontres, les réseaux sociaux ou les services de jeu en ligne[174]. Dans de nombreux cas, ces individus créent de fausses identités pour établir une relation de confiance avec la victime avant de la manipuler et de l'extorquer[175]. Ainsi, l'auteur prend généralement contact avec sa victime sous une fausse identité et instaure une relation de confiance afin d'obtenir des images intimes[176]. Une fois en possession de ces contenus, il exerce un chantage en menaçant de les diffuser, notamment à l'entourage de la victime, pour obtenir de l'argent (sextorsion à des fins financières) ou l'envoi d'autres contenus (sextorsion à but sexuel).

Dans le cas spécifique des mineurs, la sextorsion est généralement le fait d'une personne majeure et constitue alors un "chantage sexuel d'enfants"[177]. Cette pratique consiste pour le majeur à utiliser un contenu sexuel représentant le mineur, obtenu avec ou sans son consentement, "*en vue de lui extorquer des faveurs sexuelles (en ligne ou hors ligne), de l'argent, ou tout autre avantage, en le menaçant de partager ce contenu sans son consentement*"[178]. Elle peut alors être associé au grooming qui 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*"[179].

Il convient de relever que la sextorsion est une pratique "genrée" autrement dit que les femmes/jeunes filles sont davantage confrontées à une forme de sextorsion à but sexuel alors que

---

[173] Point de contact, La Sextorsion - Focus. Prévenir, identifier et agir face aux violences sexuelles sur mineurs en ligne.

[174] eSafety Commissioner, Dealing with sexual extortion.

[175] EPCAT, Quels dangers existent sur internet ?

[176] Sur le recours à l'IA générative pour générer des contenus hypertruqués à de nature sexuelle à des fins de chantage v. les développements relatifs aux deepfakes.

[177] Francopol et L'Organisation internationale de la francophonie, Guide pratique : La lutte contre l'abus et l'exploitation sexuel d'enfants en ligne, 2022, p. 32.

[178] Ibid.

[179] CNCDH, Avis sur la protection de l'intimité des jeunes en ligne, janvier 2025, p. 5. - V. également, https://www.pointdecontact.net/wp-content/uploads/2023/05/FicheGrooming.pdf.

les hommes/garçons sont pour la plupart exposés à une forme financière de cette pratique. Cette dernière forme de sextorsion constitue l'essentiel des signalements[180] et résulte essentiellement de pratiques d'acteurs agissant en bande organisée depuis l'étranger[181]. Il convient toutefois de relever que la sextorsion peut également être perpétrée par des individus isolés, en particulier de pédocriminels pour la sextorsion à des fins sexuelles, voire entre mineurs[182].

Les études attestent de ce que le phénomène de sextorsion est en constante croissance depuis ces dernières années. Entre octobre 2021 et mars 2023, le FBI et Homeland Security Investigations ont reçu plus de 13 000 signalements de sextorsion financière en ligne impliquant des mineurs avec une augmentation de 20 % des signalements de sextorsion à des fins financières entre octobre 2022 et mars 2023 par rapport à l'année précédente[183] ; cette forme de criminalité a concerné plus de 12 600 victimes, principalement des garçons, et a conduit à au moins 20 suicides. En Australie, l'eSafety Commissioner a rapporté plus de 1 700 plaintes pour sextorsion en 2023, un chiffre qui représente plus du double que l'année précédente[184]. L'IWF a relevé que, au Royaume-Uni, les signalements d'abus sexuels sur enfants liés à l'extorsion sexuelle ont augmenté de 19 % au cours des 6 premiers mois de 2024 par rapport à la même période en 2023 et que les victimes sont de plus en plus jeunes : les signalements impliquant des jeunes de 14 à 15 ans ont augmenté de 25 % par rapport à l'année précédente, certains signalements concernant des enfants âgés de 11 à 13 ans ; si les garçons représentent toujours la majorité des victimes, le nombre de signalements impliquant des filles a augmenté de 2 600 %[185]. En 2023, le NCMEC a reçu 26 718 signalements de cas de sextorsion à des fins financières, contre 10731 en 2022[186] ; en 2024, le NCMEC a dénombré plus de 500 signalements pour des cas de sextorsion par semaine[187]. Pour la France, les chiffres de l'Office mineurs (OFMIN) attestent de cette même augmentation des cas de sextorsion signalés : 1 400 plaintes en 2022, 12 000 en 2023, et 28 767 en 2024 ; une autre évolution est notable pour 2024 dès lors que, parmi les signalements dénombrés, 20 000 avaient une IP « auteur » géolocalisée en France.

---

[180] Sur le cas de mineurs Pour l'Australie, le eSafety Commissioner relève que 90 % des victimes sont des jeunes hommes, souvent âgés de moins de 18 ans (eSafety Commissioner, Sexual extortion and child abuse reports almost triple) - v. également en ce sens l'IWF, Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports, March 2024.

[181] Observatoire de l'IA de Paris 1, Entretien avec Véronique Béchu sur les deepfakes et la sextorsion.

[182] Ibid.

[183] FBI, Sextortion: A Growing Threat Targeting Minors.

[184] eSafety Commissioner, Sexual extortion and child abuse reports almost triple.

[185] IWF, Exponential increase in cruelty' as sextortion scams hit younger victims, August 2024.

[186] E. Henderson Vaughan, NCMEC Releases New Sextortion Data, April 2024. Par ailleurs, le Cyber Tipline report 2023 relève une augmentation de plus de 300% entre 2021 et 2023 des cas de "Online enticement" ("form of exploitation involving an individual who communicates online with someone believed to be a child with the intent to commit a sexual offense or abduction).

[187] NCA, National Crime Agency launches online campaign to tackle 'sextortion' among young teenage boys, March 2025.

5.2. CADRE JURIDIQUE

5.2.1. France et Union européenne

Afin de lutter contre les pratiques de sextorsion dont le nombre va croissant, le droit français et de l'Union européenne ont été récemment enrichis de différentes dispositions afin d'incriminer ces pratiques et imposent plusieurs obligations aux fournisseurs de service de réseaux sociaux.

Mesures répressives. En droit français, une nouvelle incrimination a été consacrée par l'article 17 de la Loi SREN du 21 mai 2024[188] afin de sanctionner plus efficacement l'auteur de ces pratiques. Ainsi, l'article 312-10 du Code pénal est modifié pour sanctionner de 7 ans d'emprisonnement et 100 000 euros d'amende tout chantage exercé par un service de communication en ligne "*au moyen d'images ou de vidéos à caractère sexuel"* (1) *; "en vue d'obtenir des images ou des vidéos à caractère sexuel*" (2). La consécration de cette nouvelle circonstance aggravante à l'incrimination de chantage doit être saluée dans la mesure où les faits de sextorsion n'étaient préalablement appréhendés que sur des fondements d'escroquerie financière et d'incitation à accomplir un acte de nature sexuelle. Cette nouvelle disposition permet désormais de couvrir de manière plus claire ce type de faits dès lors que les éléments constitutifs de l'infraction seront plus aisés à caractériser.

Néanmoins, pour assurer une meilleure protection des plus jeunes utilisateurs victime de sextorsion, il serait en outre nécessaire, comme le propose la CNCDH dans son avis sur la protection de l'intimité des jeunes en ligne, de compléter l'article 312-10 du Code pénal "*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 suraggravation quand ils l'ont été en bande organisée*"[189].

En ce qui concerne les victimes mineures, il convient toutefois de relever que les peines prévues au titre de la pratique de grooming pourront trouver à s'appliquer. A cet égard, depuis la modification du Code pénal par la Loi du 21 avril 2021 visant à protéger les mineurs des crimes et délits sexuels et de l'inceste, l'article 227-22-2 du Code pénal incrimine le fait pour un majeur d'inciter par un moyen de communication électronique un mineur à commettre tout acte de nature sexuelle, soit sur lui-même, soit sur ou avec un tiers, y compris si cette incitation n'est pas suivie d'effet. Les peines encourues sont de 7 ans d'emprisonnement et 100 000 euros d'amende, et de 10 ans d'emprisonnement et 150 000 euros d'amende si les faits ont été commis sur un mineur de moins de 15 ans, ainsi que 10 ans d'emprisonnement et 1 million d'euros d'amende s'ils ont été commis en bande organisée.

Par ailleurs, selon l'article 227-22-1 du Code pénal, le fait pour un majeur de faire des propositions sexuelles à un mineur de moins de 15 ans ou à une personne se présentant comme telle en utilisant

[188] Auparavant, la sextorsion était sanctionnée sur le fondement du chantage (articles 312-10 et suivants du Code pénal) ou de l'extorsion (articles 312-1 et suivants du Code pénal) en cas de diffusion de contenu.

[189] CNCDH, avis préc., recommandation n°18. Il est proposé que la rédaction retenue s'inspire de celle de l'article 227-23-1, alinéa 2, du Code pénal.

un moyen de communication électronique est puni de 2 ans d'emprisonnement et de 30 000 euros d'amende ; les peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre. Cette infraction de grooming vise avant tout à prévenir des comportements beaucoup plus graves en réprimant de façon autonome la simple prise de contact et en dissuadant les adultes d'entreprendre de telles démarches. Toutefois, il n'est pas toujours aisé de caractériser un tel comportement. Ainsi, la Cour d'appel d'Aix-en-Provence[190] a retenu l'application de l'article 227-22-1 du Code pénal a l'encontre d'un homme qui a dialogué sur un forum de discussion avec une fillette de dix ans et lui a demandé de se dénuder et de se livrer a des gestes obscènes devant la webcam, alors même que ce comportement est généralement réprimé au titre de la corruption de mineurs. Selon une décision du 29 mai 2012[191], se rend ainsi coupable de corruption de mineur, un majeur faisant des propositions sexuelles à une mineure de 15 ans en utilisant un moyen de communication électronique. En l'espèce, l'adulte se faisait passer pour une adolescente bisexuelle et demandait à ses victimes de se déshabiller et de pratiquer des actes de nature pornographique devant leur webcam. Une décision du 8 février 2017[192] précise que le délit de corruption de mineur suppose l'intention de pervertir la sexualité du mineur. Dans une autre décision[193], la corruption de mineur aggravée avait été constituée dès lors que les propositions sexuelles ont été suivies d'une rencontre avec la personne se présentant comme un mineur.

En outre, au titre de l'article 227-23-1 du Code pénal, le fait pour un majeur de solliciter auprès d'un mineur la diffusion ou la transmission d'images, vidéos ou représentations à caractère pornographique dudit mineur est puni de 7 ans d'emprisonnement et de 100 000 euros d'amende. L'auteur encourt jusqu'à 10 ans d'emprisonnement et 150 000 euros d'amende lorsque les faits ont été commis à l'encontre d'un mineur de moins de 15 ans. Les peines sont portées à 10 ans d'emprisonnement et à un million d'euros d'amende lorsque les faits ont été commis en bande organisée[194]. Le juge pourra également ordonner une peine de "suspension des comptes" en application de l'article 131-35-1 du Code pénal[195].

Il convient en outre de souligner que la Directive 2011/93[196] définit les infractions liées à la pédopornographie et sollicitation d'enfant à des fins sexuelles et impose aux plateformes une suppression rapide des pages internet diffusant des contenus à caractère pédopornographiques[197]. Cette directive sera révisée avec l'adoption de la proposition de Règlement CSAM[198] actuellement en cours de discussion. Ce projet de texte fait l'objet d'importantes discussions compte tenu notamment des difficultés pour trouver un équilibre dans l'encadrement des mécanismes de chiffrement de bout en bout et les pouvoirs d'enquête afin de garantir la protection des mineurs

[190] Aix-en-Provence, 26 oct. 2011, nº 586/J/2011.
[191] Colmar, 29 mai 2012.
[192] Cass. crim, 8 février 2017, n°16-80.102.
[193] Cass. crim 25 janvier 2023, n°2283.997.
[194] Code pénal, article 227-23-1.
[195] Pour plus de précisions, v. supra les développements consacrés au Cyberharcèlement.
[196] Directive 2011/93 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, 13 décembre 2011.
[197] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 6.
[198] Proposition de Règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, 11 mai 2022, 2022/0155.

dans le cadre de la lutte contre les abus sexuels et le respect des droits et libertés fondamentaux des utilisateurs des services numériques[199].

Obligations incombant aux fournisseurs de service. Afin de lutter plus efficacement contre ces pratiques, le DSA vient également imposer différentes obligations aux fournisseurs de services de réseaux sociaux. Ils doivent bloquer l'accès ou supprimer tout contenu illicite notifié conformément à l'article 6[200]. Pour le cas particulier de la sextorsion/grooming, les comptes des auteurs de chantage pourront être supprimés. En outre, les fournisseurs de services sont tenus d'une obligation de "Safety by design" en vertu de laquelle, conformément à l'article 28 du DSA, il leur revient 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[201]. De plus, les réseaux sociaux désignés comme très grandes plateformes doivent réaliser une analyse de risque (article 34) et mettre en œuvre des mesures d'atténuation afin de protéger les droits de l'enfant ainsi que leur santé physique et mentale (article 35)[202] ; on peut souligner ici que le premier rapport du European Board of Digital Services publié le 18 novembre 2025 mentionne au titre des risques systémiques majeurs l'exposition des utilisateurs au grooming et au chantage sexuel[203].

5.2.3. États-Unis

Droit fédéral. Alors qu'aucune loi fédérale ne sanctionnait jusqu'alors la sextorsion en tant que telle, le fort accroissement des cas signalés et la nécessité de renforcer la protection des victimes a conduit à l'adoption du Tools to Address Known Exploitation by Immobilizing Technological Deepfakes On Websites and Networks (Take it Down Act)[204]. Le texte consacre une nouvelle incrimination relative à la sextorsion en visant la menace de partage d'une image "*for the purpose of intimidation, coercion, extortion, or to create mental distress*", en distinguant la menace impliquant une représentation visuelle intime de la personne de nature authentique ("*authentic intimate visual depiction"*) de celle impliquant une représentation de nature synthétique ("*digital*

[199] V. notamment, EDPB, Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse - v. également sur les critiques : Global Encryption Coalition, Joint Statement on the danger of the May 2024 Council of the EU compromise proposal on EU CSAM, May 2024.

[200] Sur ce point, v. Chapitre 2, pt. 2.1.2.5., développements consacrés au signalement.

[201] Sur ce point, v. Chapitre 11, développements consacrés à la conception et les précisions relatives aux lignes directrices de l'article 28 du DSA du 14 juillet 2025.

[202] Sur ce point, Chapitre 2 pt. 2.1.2.5., développements consacrés à l'analyse de risques.

[203] European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025, pts. 3.1 et 3.4.

[204] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes On Websites and Networks (TAKE IT DOWN) Act, Public Law No. 119-12 (05/19/2025). Pour une explication du texte et de sa conformité à la Constitution, et en particulier au premier amendement, v. le Memorandum THE TAKE IT DOWN ACT: A CONSTITUTIONAL, TARGETED APPROACH TO ADDRESSING THE SPREAD OF NON CONSENSUAL INTIMATE IMAGERY ONLINE, 8 April 2025.

forgery")[205]. Les peines encourues varient en fonction de ces différentes hypothèses : le texte renvoie à celles prévues au titre du partage non consenti d'image intime lorsque le contenu est authentique, soit des peines d'amende et/ou de 2 ans d'emprisonnement si la victime de la menace est majeure allant jusqu'à 3 ans en cas de victime mineure ; des peines spécifiques sont prévues en cas de contenu synthétique ("*digital forgery"*), à savoir des peines d'amende et/ou de 18 mois d'emprisonnement dans l'hypothèse où la victime de la menace est majeure allant jusqu'à 30 mois d'emprisonnement si la victime est mineure[206].

Cette pratique peut également relever de la loi fédérale sur le cyberharcèlement ("*cyberstalking"*) et être sanctionnée au titre du CSAM lorsque la victime est un mineur[207]. A cet égard, il convient de relever que le National Center for Missing & Exploited Children (NCMEC) propose la CyberTipline, un système de signalement centralisé permettant aux individus de signaler des cas présumés d'exploitation sexuelle des enfants[208].

Droit étatique. De nombreux États ont adopté des lois sur la sextorsion, la vengeance pornographique, le sexting. À titre d'exemple, l'Utah sanctionne la sextorsion à des fins sexuelles et financières et prévoit une circonstance aggravante si la victime est une personne mineure[209].

5.2.4. Angleterre et Pays de Galles

Mesures répressives. Le Sexual Offences Act précise qu'une personne commet une infraction si elle partage intentionnellement une photographie ou une vidéo qui montre, ou semble montrer, une autre personne dans un état intime dans le but d'obtenir une gratification sexuelle de la personne ou d'une autre personne, que la personne ne consent pas au partage de la photographie ou du film; cette disposition s'applique lorsque la victime est âgée de plus de 16 ans[210]. Pour les victimes âgées de moins de 16 ans, l'incrimination de CSAM trouvera à s'appliquer[211].

En outre, la Section 15A du Sexual Offences Act 2003[212] incrimine le grooming c'est-à-dire le fait, pour une personne majeure, de communiquer de manière sexuelle avec un enfant de moins de 16

---

[205] *Digital forgery* : "*any intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual*" : TAKE IT DOWN Act, s. 2.

[206] TAKE IT DOWN Act, s. 6.

[207] Sur ces points, v. infra Chapitre 3 cyberharcèlement et Chapitre 4 partage non consenti d'image intime, Etats-Unis.

[208] National Center for Missing & Exploited Children, CyberTipline - Sur les CSAM, v. les développements supra.

[209] Utah Code, Title 76 - Chapter 5b - Part 2 - Section 204.

[210] Sexual Offences Act 2003, s. 66B modifiée par le Online Safety Act 2023, Chapter 50, Part 10, s. 188.

[211] Sur ce point, v. infra, Chapitre 4 "Diffusion non consentie de contenus intimes", pt. 4.2.3, Angleterre et Pays de Galles.

[212] Sexual Offences Act 2003, s. 15A introduite par le Serious Crime Act 2015.

ans. L'infraction est constituée si l'adulte (1) dans le but d'obtenir une satisfaction sexuelle, communique intentionnellement avec une autre personne, (2) la communication est de nature sexuelle ou vise à encourager le mineur à entretenir une communication de nature sexuelle. Il faut également que l'adulte ne croit pas raisonnablement que l'enfant a 16 ans ou plus. Une communication est considérée comme sexuelle si elle porte sur une activité sexuelle ou si une personne raisonnable la percevrait comme telle, indépendamment de l'intention réelle de l'auteur. L'auteur est passible de peines d'amende et de deux ans d'emprisonnement. Afin de renforcer la protection des victimes, il est actuellement discuté la possibilité de consacrer une aggravation des peines dès lors qu'une infraction sexuelle commise sur un enfant a été facilitée par une pratique de grooming[213].

Obligations de fournisseurs de services. Comme précédemment mentionné concernant le partage non consenti de contenu intime[214], en application de l'Online Safety Act 2023[215], les services numériques sont soumis à des obligations renforcées en matière de modération des contenus à caractère sexuel. Concernant les mesures à mettre en œuvre mentionnées par l'OFCOM dans le Codes of practice publié en février 2025, certaines visent à limiter le grooming en agissant en particulier sur le paramétrage des comptes[216]. Il est ainsi mentionner (1) la définition de paramétrages par défaut plus sûrs pour les utilisateurs mineurs afin de rendre plus difficile pour les inconnus de trouver et d'interagir avec des enfants en ligne, par exemple en limitant la réception de message privé - "*direct message"* - par l'utilisateur mineur, ou encore (2) l'envoi de message destinés aux enfants lorsqu'ils naviguent en ligne, afin de leur permettre de faire des choix sûrs, par exemple lorsqu'ils désactivent les paramètres par défaut ou reçoivent un message d'un utilisateur pour la première fois. Les fournisseurs de service sont en outre tenus de conduire des analyses de risques pour identifier la probabilité et l'impact de l'exploitation et des abus sexuels concernant des enfants apparaissant sur leur service et doivent prendre des mesures pour atténuer les risques identifiés.

5.2.5. Australie

En Australie, la sextorsion est considérée comme une infraction pénale propre aux États et aux Territoires pour le partage non consenti d'image intime ainsi que pour l'extorsion ou le chantage. Cette pratique est également couverte par les infractions fédérales relatives à l'utilisation d'un "*carriage service"* pour menacer, harceler ou offenser en vertu de la section 474.17 du Criminal Code Act 1995[217]. Une version aggravée de l'infraction existe si une personne commet une infraction impliquant la transmission, la mise à disposition, la publication, la distribution, la

[213] Crime and Policing Bill (2025), proposition d'article 43 et le rapport de recherche détaillant la proposition : W. Downs, S. Lipscombe, J. Dawson, F. Cooney, Crime and Policing Bill 2024-25, House of Communs Library, March 2025.
[214] V. infra.
[215] Online Safety Act 2023, Chapter 50, Part. 3, Chapter 7, s. 59.
[216] OFCOM, Illegal content Codes of Practice for user-to-user services, 24 February 2025, pts. ICU F1 et ICU F2.4.
[217] Criminal Code Act, v. 2.

publicité ou la promotion de matériel sexuel privé. La création, la possession, la diffusion et le téléchargement d'images indécentes d'enfants seront également qualifiées de CSAM[218].

Outre les obligations de modération imposées aux fournisseurs de service, l'Online Safety Act 2021 consacre un système de sanctions civiles permettant au eSafety Commissioner de retirer des images en ligne et, dans certains cas, de prendre des mesures à l'encontre de la personne qui a partagé ou menacé de partager une image intime sans consentement.

5.3. PRÉCONISATIONS

Préconisation 11 - **Renforcer les mesures de prévention**

a. Afin d'empêcher les inconnus de trouver les enfants en ligne et d'interagir avec eux, consacrer à la charge des fournisseurs de services de réseaux sociaux en application de l'article 28 du DSA une obligation de paramétrage par défaut des comptes utilisateurs mineurs notamment l'activation du "*mode privé*" par défaut et le blocage de la réception des messages directs d'utilisateurs inconnus. Les enjoindre à accompagner les mineurs dans le paramétrage de leurs interfaces tout au long de leurs utilisations du réseau social, notamment par l'envoi de messages de sensibilisation aux risques de la sextorsion en cas de modification par l'utilisateur mineur des paramétrages par défaut précités. Réglez les comptes pour mineurs au plus haut niveau de confidentialité, de sûreté et de sécurité par défaut. Il s'agit notamment de concevoir des paramètres par défaut de manière à garantir des paramètres sûrs et adaptés à l'âge des mineurs, en tenant compte de l'évolution de leurs capacités. Ces paramètres doivent garantir que, par défaut pour tous les mineurs, au minimum : i. Les comptes n'autorisent que les interactions telles que les likes, les tags, les commentaires, les messages directs, les reposts et les mentions par des comptes qu'ils ont précédemment acceptés. ii. Aucun compte ne peut télécharger ou prendre des captures d'écran des informations de contact, de localisation ou de compte, ou du contenu téléchargé ou partagé par des mineurs sur la plateforme. iii. Seuls les comptes que le mineur a précédemment acceptés peuvent voir son contenu, ses publications et ses informations de compte. iii. Personne ne peut voir les activités du mineur telles que "*aimer*" le contenu ou "*suivre*" un autre utilisateur (*Commission européenne, Lignes directrices sur l'article 28, 10 octobre 2025, 6.3.1- 57.b*).
Sources : OFCOM, Illegal content Codes of Practice for user-to-user services, pt. ICU F1 et CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°13

b. Conduire des campagnes de sensibilisation nationales aux risques de la sextorsion.

Préconisation 12 - **Améliorer la réponse pénale**

a. Mieux sanctionner toute sextorsion en facilitant l'accueil des victimes, en favorisant leur dépôt de plainte et en conduisant des enquêtes fouillées que les sextorsions soient à caractère sexuel ou

[218] Sur ce point, v. infra, Chapitre 4 "Diffusion non consentie de contenus intimes".

à des fins financières, quel qu'en soit le préjudice matériel dans la mesure où le préjudice subi par la victime dépasse le seul préjudice financier même modique (inférieur à 500 euros) compte tenu du retentissement psychologique et du sentiment d'insécurité qu'il peut durablement générer pour la victime.

Augmenter par ailleurs les ressources humaines et techniques dédiées à la lutte contre la sextorsion et la diffusion non consentie d'images intimes pour assurer une prise en charge efficace et des enquêtes approfondies, ce qui inclut une meilleure formation des enquêteurs, le développement d'unités spécialisées et l'amélioration des outils de détection et d'identification des auteurs.

b. 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 nouveaux alinéas aggravants les peines encourues, la compréhension de son champ d'application afin de saisir ce phénomène en pleine croissance et d'encourager les parquets à y apporter une réponse rapide, systématique et efficace.

Les enjeux d'une telle infraction visent, d'une part, à favoriser la compréhension des interdits dans une société qui se déploie dans l'espace numérique (fonction expressive de la loi pénale), d'autre part, à punir les auteurs de sextorsion (fonction répressive) et, enfin, à garantir une protection pour les victimes en faisant reculer le sentiment d'impunité des auteurs tout en réaffirmant les impacts de leurs actions sur la santé et la sécurité des personnes.

c. Favoriser la diffusion de l'information relative au phénomène de sextorsion et l'appropriation de la nouvelle rédaction de l'article 312-10 du Code pénal par les magistrats par le biais de formations dédiées tant en formation initiale qu'en formation continue
d. Compléter la nouvelle rédaction de l'article 312-10 du Code pénal par une aggravation des peines lorsque les faits ont été commis à l'encontre d'un mineur de moins de 15 ans et prévoir une aggravation supplémentaire lorsqu'ils l'ont été en bande organisée. La rédaction retenue pourrait s'inspirer de celle de l'article 227-23-1 alinéa du Code pénal.
Source : *CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°18*

e. Veiller à ce que le Code pénal et le Code de procédure pénale prévoient la possibilité d'inscrire au Fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS) les auteurs condamnés pour sextorsion sur le fondement de l'article 312-10 du Code pénal et favoriser l'interconnexion des fichiers judiciaires relatant les auteurs d'infractions sexuelles sur mineur pour le moins au niveau européen.

f. Étendre la portée extraterritoriale des enquêtes et des plaintes en coopération avec INTERPOL et EUROPOL pour tenir compte de la localisation fréquente des réseaux criminels à l'étranger. Renforcer la coordination mondiale entre les différentes autorités policières et judiciaires en facilitant la conduite des enquêtes à l'étranger.

Préconisation 13 - Améliorer le signalement

a. S’assurer de la mise à disposition par toute plateforme d’un onglet de signalement spécifique à la sextorsion, en expliquant la pratique et les étapes à suivre si une victime y est confrontée (recommander de bloquer la personne, couper tout contact avec cette dernière, ne pas payer et appeler le 3018).

b. Renforcer la collaboration des plateformes avec des signaleurs de confiance afin de favoriser le signalement des cas d’usurpation d’identité et de piratage de comptes utilisés à des fins de sextorsion et d’escroquerie.

c. En outre, les signalements effectués par des mineurs devraient être prioritaires (*Commission européenne, Lignes directrices sur l’article 28, 10 octobre 2025, 6.7- 72c*).

CHAPITRE 6 : DEEPFAKES ET ATTEINTE À L'INTIMITÉ

6.1. PRATIQUES

Alors que les outils d'IA générative connaissent une adoption rapide, plusieurs risques peuvent découler de leur utilisation malveillante à grande échelle[219], notamment en ce qui concerne le bien-être et la sécurité des mineurs en ligne[220]. Parmi ces formes d'utilisation malveillante, l'*International AI Safety Report* publié dans le cadre du AI Action Sumit de février 2025 relève différents cas d'atteinte aux individus sur la base de contenus falsifiés, soulignant que "*Les acteurs malveillants peuvent actuellement utiliser l'IA à usage général pour générer du faux contenu qui nuit aux individus de manière ciblée. Ces utilisations malveillantes incluent la création de "deepfakes pornographiques sans consentement, la génération de matériel pédopornographique par IA, la fraude financière par usurpation de voix, le chantage pour extorsion, le sabotage de réputations personnelles et professionnelles, ainsi que les abus psychologiques*", et observe que les enfants sont généralement victimes de cette dernière catégorie d'usage malveillant[221]. Dès 2023, l'UNICEF avait constaté l'utilisation croissante de ces contenus hypertruqués à des fins d'exploitation sexuelle des enfants en ligne[222].

Ces pratiques peuvent reposer sur la création et la diffusion de contenu généré par IA, définis comme un contenu audio, textuel ou visuel, produit ou manipulé par un système d'intelligence artificielle générative. Ces contenus sont qualifiés de deepfakes ou contenus hypertruqués lorsqu'ils représentent des personnes, des événements ou des lieux d'une manière qui diffère de la réalité[223].

L'un des principaux risques résulte de la génération de contenus hypertruqués à caractère sexuel ou représentant une personne dénudée à des fins malveillante ou trompeuse. En effet, les "*deepfakes nudes*" ou deepfakes à caractère sexuel sont des contenus synthétiques qui représentent

---

[219] UNICEF, Generative AI: Risks and opportunities for Children, 2023.

[220] Ibid.

[221] AI Action Summit, *rapport préc.*, p.63. Le rapport cite différents exemples et en particulier pour Blackmail/extorsion : "*Generating fake content of an individual, such as intimate images, without their consent and threatening to release them unless financial demands are met*" ; pour le sabotage : "*Generating fake content that presents an individual engaging in compromising activities, such as sexual activity or using drugs, and then releasing that content in order to erode a person's reputation, harm their career, and/or force them to disengage from public-facing activities (e.g. in politics, journalism, or entertainment)*" ; pour les abus psychologiques et harcèlement: "*Generating harmful representations of an individual for the primary purpose of abusing them and causing them psychological trauma*".

[222] UNICEF, Generative AI: Risks and opportunities for Children, 2023.

[223] AI Action Summit, International AI Safety report, janvier 2025, p.62, par exemple, un contenu représentant faussement des personnes réelles comme faisant ou disant quelque chose qu'elles n'ont pas réellement fait ou dit.

des personnes réelles dans des situations sexuellement suggestives ou explicites[224]. Ces contenus peuvent être générés à partir de la technique du "swapping" qui permet de faire figurer le visage d'une personne sur le corps d'une autre personne dénudé ou en ayant recours à une application de dénudage qui utilise l'IA pour altérer l'image d'une personne y figurant habillée afin de générer un contenu où elle apparaît dénudée.

Différentes études relèvent que la démocratisation de ces outils d'IA générative facilite ces pratiques malveillantes. Ainsi, l'UNESCO observe, dans un rapport de 2024, que "*L'IA générative permet la création de fausses images et de faux contenus audio, texte et vidéo à une vitesse et une échelle impressionnante. Cela signifie que les harceleurs disposent désormais de mécanismes sophistiqués et automatisés avec lesquels ils peuvent faire subir à leurs cibles un harcèlement durable, avec un niveau de compétence technique requis minimal*"[225]. Il est toutefois encore difficile de mesurer précisément ce phénomène en l'absence de données statistiques relatives à ce type d'impact[226]. On relève cependant un usage important des applications de dénudage, accessible au plus grand nombre sur les moteurs de recherche et magasins d'application [227], dont certaines font l'objet de campagnes publicitaires sur TikTok[228].

En ce qui concerne l'usage malveillant de deepfake à caractère sexuel représentant une personne mineure, les motivations des auteurs peuvent être de différentes natures.

En ce qui concerne les auteurs majeurs, les études soulignent en particulier le recours à la production et/ou diffusion de ces contenus à des fins de chantage et/ou d'abus sexuel sur mineurs. Les auteurs de ces pratiques de chantage sexuel peuvent désormais utiliser des photos existantes, souvent issues de réseaux sociaux, pour générer des deepfakes sexuels, dans lesquels le visage de la victime est manipulé pour créer des images à caractère sexuel ; pour créer ces deepfakes, le visage des victimes peuvent être superposés sur ceux d'acteurs pornographiques, créant ainsi l'illusion qu'elle a participé à l'acte. L'objectif est ensuite de harceler et de faire chanter la victime. La technologie deepfake peut également être utilisée pour créer de fausses identités à des fins de

[224] THORN, Deepfake Nudes & Young People Navigating a new frontier in technology-facilitated nonconsensual sexual abuse and exploitation, 2025, p.8.

[225] UNESCO, Ton avis ne compte pas de toute façon : Dénoncer la violence de genre facilitée par la technologie à l'ère de l'intelligence artificielle générative, 2024, p. 16. - également en ce sens, v. Ministère de l'intérieur, Rapport annuel sur la cybercriminalité 2024, p. 27.

[226] AI Action Summit, rapport préc., p.63.

[227] S. Dunn, "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI", *Mc Gill Law Journal*, vol. 69, 2024. v. également OFCOM, Deepfake Defences. Mitigation the Harms of Deceptive Deepfakes, 2024, p. 6&s. Pour des exemples, v. la présentation de l'ONG MyImageMyChoice, Deepfake Abuse. Landscape Analysis, 2024, qui relève par exemple que l'application *Undress.ai* a traité 600 000 images de personnes ordinaires dans les 21 premiers jours suivant son lancement. Ce document relève par ailleurs le nombre croissant de consultations des sites spécialisés dans les contenus deepfakes totalisant 4 milliards de vues.

[228] House of Commons, Tackling non-consensual intimate image abuse, 2024-25, HC 336, March 2025, pt. 130.

chantage et d'abus sexuels sur mineurs[229]. Par exemple, un adulte peut dissimuler sa véritable identité, en transformant son propre visage en celui d'un enfant ou d'un mineur, exposant ainsi la victime à un risque d'exploitation[230]. A cet égard, EUROPOL alertait dès 2020 que 96 % des vidéos deepfakes en ligne étaient liées à de la pornographie non consensuelle, illustrant la manière dont les technologies de manipulation numérique peuvent être utilisées pour commettre des abus graves[231]. Une récente alerte du FBI[232] a relevé en particulier une augmentation des cas de sextorsion, y compris ceux impliquant des mineurs, via des images générées par intelligence artificielle. Enfin, le Parlement européen mentionne qu'il est estimé que 8 millions de deepfakes seront partagés durant l'année 2025, contre seulement 500 000 en 2023[233], et qu'environ 98 % de ces deepfakes concernent du contenu pornographique.

Il convient également d'observer une utilisation croissante de l'IA générative pour la création de contenus pédocriminels[234]. Les systèmes d'IA permettent désormais de générer rapidement et facilement des images et des vidéos d'abus sexuels sur des enfants. Le nombre de signalements pour de tels actes est en constante augmentation. Ainsi, alors que l'on observe une augmentation de 12 000% des signalements pour des contenus pédocriminels en dix ans[235], plus de 20 000 images générées par l'IA ont été publiées sur le dark web pédocriminel[236] et plus de 4700 contenus pédocriminels impliquant l'IA générative ont été signalés au NCMEC en 2023[237]. Comme l'a relevé le rapport de la Fondation pour l'enfance "L'IA générative, nouvelle arme de la pédocriminalité"[238], cette évolution est source de nombreux risques. Il en résulte notamment la difficulté pour les autorités de discerner les images authentiques des images synthétiques, ce qui complique la détection et la prévention des abus[239] ; les contenus d'abus sexuels commis sur des enfants générés par l'IA contribuent à la normalisation des comportements délictueux et risquent de créer un environnement plus permissif pour les auteurs, mettant en danger un nombre toujours plus grand d'enfants. Europol alerte à ce titre que, d'ici 2026, 90 % du contenu en ligne pourrait être généré par intelligence artificielle[240]

Des usages malveillants de contenus hypertruqués à caractère sexuel peuvent être également observés entre mineurs. Ainsi, différents cas de production de contenus générés à partir

[229] UNICRI, EC3, Malicious Uses and Abuses of Artificial Intelligence, 2020.
[230] Fondation pour l'enfance, Rapport l'IA générative, nouvelle arme de la pédocriminalité, oct. 2024, p.18.
[231] EUROPOL, Facing reality ? Law enforcement and the challenge of deepfake, 2020.
[232] FBI, Alerte numéro I-060523-PSA, 5 juin 2023.
[233] European Parliament, Children and deepfakes, July 2025.
[234] NCMEC, Generative AI CSAM is CSAM, 2024 - également, UNICRI, Generative AI - A new threat for online child sexual exploitation, 2024 - Fondation pour l'enfance, *rapport préc*.
[235] Fondation pour l'enfance, *rapport préc*., p. 6.
[236] Fondation pour l'enfance, *rapport préc*., p. 7.
[237] NCMEC, Generative AI CSAM is CSAM, 2024.
[238] Fondation pour l'enfance, *rapport préc*.
[239] En ce sens, v. également Observatoire de l'IA de Paris 1, Entretien avec Véronique Béchu sur les deepfakes et la sextorsion, juil. 2024.
[240] Europol, Facing reality? Law enforcement and the challenge of deepfakes, 2024.

d'applications de dénudage puis diffusés sur les réseaux sociaux ou groupes de messagerie privée ont été relevés notamment à des fins de cyberharcèlement entre élèves[241]. Par exemple, en Espagne, le tribunal pour mineurs de Badajoz a eu à se prononcer dans une affaire où quinze mineurs avaient utilisé des applications de dénudage pour obtenir des images manipulées de leurs camarades d'école, de telle sorte que les visages des filles, obtenus à partir de leurs profils sur les réseaux sociaux, étaient superposés à des images d'autres corps féminins dénudés ; les images ont été ensuite diffusées sur deux groupes de messagerie privée (WhatsApp)[242]. En France, en mars 2025, une enquête a été ouverte en mars 2025 par le parquet de Coutance dans la Manche après qu'une douzaine de collégiennes ont été victimes de deepfake à caractère sexuel[243].

Plus généralement, plusieurs études ont relevé que ces contenus hypertruqués sont massivement utilisés à des fins de violence sexuelles et sexistes[244].

6.2. CADRE JURIDIQUE

6.2.1. France et Union européenne

Compte tenu du phénomène précédemment décrit, le droit français et de l'Union européenne ont été récemment enrichis de nouvelles dispositions visant en particulier à appréhender les atteintes à la personne résultant de la diffusion de deepfakes.

Mesures répressives. Tout d'abord, de nouvelles interdictions sont désormais consacrées par le Code pénal pour viser explicitement les hypertrucages générés par les outils d'IA générative afin de compléter le cadre légal préexistant.

---

[241] AI Action summit, International AI Safety report, janvier 2025, p.64 - également, relevant ce phénomène croissant, THORN, Deepfake Nudes & Young People Navigating a new frontier in technology-facilitated nonconsensual sexual abuse and exploitation, 2025, p.9.

[242] Sentencia del 20 de junio juzgado de Menores de Badajoz, Imponen la medida de libertad vigilada durante un año a los 15 menores acusados de manipular y difundir imágenes de menores desnudas en Badajoz : le jugement du 20 juin 2024 a reconnu les auteurs responsables de vingt délits de pornographie infantile et de vingt délits contre l'intégrité morale. Sur l'utilisation de montage à caractère sexuel à des fins de cyberharcèlement, v. déjà au Royaume-Uni l'affaire Mia Jamin.

[243] V. le communiqué de l'Association e-Enfance, l'Association e-Enfance/3018 alerte sur les dangers des deepfakes à caractère sexuel, 17 mars 2025.

[244] V. notamment SIPA Center Columbia University, It's Everyone's Problem: Mainstreaming Responses to Technology-Facilitated Gender-Based Violence, 2024. Cette étude relève que 98% des vidéo deepfake accessibles en ligne sont des vidéo pornographiques et 99% des personnes ciblées par ces vidéo sont des femmes.

En effet, il avait été observé que les "*diverses infractions d'atteinte à la vie privée ou d'atteinte à la représentation de la personne ne permettent pas de pénaliser efficacement la publication d'images ou de vidéos hypertruquées à caractère sexuel*"[245].

La Loi SREN du 21 mai 2024 consacre ainsi un élargissement du délit de montage de parole ou d'image "*trompeur*" non consenti prévu par l'article 226-8 Code pénal pour punir "*le fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore généré par un traitement algorithmique et représentant l'image ou les paroles d'une personne, sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un contenu généré algorithmiquement ou s'il n'en est pas expressément fait mention*". Le texte introduit par ailleurs une circonstance aggravante visant la diffusion au moyen d'un "service de communication au public en ligne" ce qui vise à répondre aux enjeux de viralité de ces montages (article 15 de la Loi SREN).

En outre, l'article 21 de la Loi SREN introduit un nouveau délit relatif aux montages à caractère sexuel en insérant dans le Code pénal un nouvel article 226-8-1 visant "*le fait de porter à la connaissance du public ou d'un tiers par quelque voie que ce soit un montage à caractère sexuel réalisé avec les paroles ou l'image d'une personne, sans son consentement. Est assimilé à l'infraction mentionnée au présent alinéa et puni des mêmes peines le fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique et reproduisant l'image ou les paroles d'une personne, sans son consentement*". Plusieurs éléments sont déterminants. Tout d'abord, en visant "le fait de porter à la connaissance du public ou d'un tiers", le texte prohibe la diffusion de deepfakes à caractère sexuel, ce dont il résulte que "*la personne responsable est celle qui a diffusé le montage et non celle qui l'a créé*"[246]. De plus, il n'est pas exigé d'établir l'intention de tromper sur le caractère authentique du contenu. Enfin, on relèvera que ce nouveau texte complète l'incrimination de partage non consenti de contenus intimes prévu à l'article 226-2-1 qui vise, quant à elle, la diffusion de contenus authentiques.

Par ailleurs, le Code pénal prévoit une incrimination spécifique aux contenus pédocriminels. Ainsi, selon l'article 227-23 du Code pénal, "*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 est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation".* Le texte prévoit que les peines sont portées à 7 ans d'emprisonnement et à 100 000 euros d'amende *"lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination*

[245] Assemblée nationale, Rapport sur le projet de loi, adopté par le Sénat, après engagement de la procédure accélérée, visant à sécuriser et réguler l'espace numérique (n°1514 rectifié), n° 1674, déposé le jeudi 21 septembre 2023 - V. sur ce point, C. Langlais-Fontaine, "Démêler le vrai du faux : étude de la capacité du droit actuel à lutter contre les deepfakes", *La Revue des droits de l'homme*, 18I2020.

[246] E. Raschel, "Retour sur les principales dispositions répressives de la loi SREN : deepfake et bannissement numérique", *Légipresse* 2025 p. 21.

d'un public non déterminé, un réseau de communications électroniques", et 10 ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée. Le texte est également applicable *"aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image*".

Concernant le droit de l'Union européenne, la Directive 2024/1385 du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique vise à consacrer de nouvelles infractions dont l'une porte sur le partage non consenti de matériels intimes ou manipulés. Ainsi, selon son article 5, "*les États membres veillent à ce que les comportements intentionnels suivants soient passibles de sanctions en tant qu'infractions pénales: b) le fait de produire, de manipuler ou de modifier puis de rendre accessibles au public, au moyen des TIC, des images, des vidéos ou des matériels similaires donnant l'impression qu'une personne se livre à des activités sexuellement explicites, sans son consentement, lorsque ce comportement est susceptible de causer un préjudice important à cette personne; c) le fait de menacer de se livrer aux comportements visés au point a) ou b) afin de contraindre une personne à accomplir un acte déterminé, à y consentir ou à s'en abstenir*". Le considérant 19 précise que "*l'infraction devrait aussi couvrir la production, la manipulation ou la modification non consenties, par exemple par l'édition d'images, notamment à l'aide de l'intelligence artificielle, de matériels donnant l'impression qu'une personne se livre à des activités sexuelles, dès lors que les matériels sont ensuite rendus accessibles au public, au moyen de TIC, sans le consentement de la personne en question. Cette production, manipulation ou modification devrait inclure la fabrication d'infox vidéos (deepfakes), dans lesquelles le matériel présente une ressemblance avec une personne, des objets, des lieux ou d'autres entités ou événements existants, montre les activités sexuelles d'une personne et pourrait donner faussement à croire qu'il est authentique ou véridique. Dans le but de protéger efficacement les victimes d'un tel comportement, le fait de menacer de se livrer à celui-ci devrait être couvert également*".

La proposition de Règlement CSAM du 6 février 2024 de la Commission européenne prévoit également d'actualiser les définitions des infractions pénales en prenant en compte le matériel relatif à des abus sexuels sur enfants présent dans des deepfakes ou dans des contenus générés par intelligence artificielle. Cette nouvelle proposition vise la production et la diffusion de deepfakes (hypertrucages) à caractère pornographique.

Si ces évolutions législatives doivent être saluées, il convient néanmoins de relever que la réponse pénale pourrait être encore améliorée pour renforcer la protection des victimes mineures. En ce sens, la CNCDH recommande[247] de revoir la rédaction de l'article 226-8-1 du Code pénal afin d'interdire ce type de contenu lorsqu'il concerne des mineurs de moins de 15 ans pour interdire les deepfakes à caractère sexuel 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. Plus généralement, à l'instar des

[247] CNCDH, Avis sur la protection de l'intimité des jeunes en ligne, A-2025-1, janvier 2025, recommandation n°20.

propositions du gouvernement britannique[248], 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. Par ailleurs, une proposition de loi visant à lutter contre la création de contenus pédocriminels via l'intelligence artificielle générative, déposée au Sénat le 6 février 2025, vise à modifier l'article 227-23 du Code pénal pour sanctionner le fait de créer, de diffuser ou de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique lorsqu'il s'agit de la représentation de l'image ou de la parole d'un mineur. Il est également proposé d'introduire un nouvel article 226-24-1 dans le Code pénal, sanctionnant de 5 ans d'emprisonnement et de 75 000 euros d'amende le fait de collecter, détenir, traiter ou détourner des données à caractère personnel, afin de créer, générer ou mettre à disposition du public ou d'un tiers un modèle de traitement algorithmique dans le but de permettre la création de contenus visuels ou sonores à caractère sexuel représentant un mineur ou de fichiers à caractère pédopornographique.

Mesures préventives. Le droit français prévoit des dispositifs de sensibilisation qui pourraient renforcer les actions de prévention relatives aux atteintes aux personnes pouvant résulter de la diffusion des contenus hypertruqués. Ainsi, l'article 7 de la Loi SREN modifie l'article L. 312-9 du Code de l'éducation relatif à la formation à l'utilisation responsable des outils et des ressources numériques dispensée dans les écoles et les établissements d'enseignement notamment pour que les élèves de l'école primaire et du collège reçoivent une attestation certifiant qu'ils ont bénéficié d'une sensibilisation au bon usage des outils de l'intelligence artificielle, de tous types de contenus générés par ceux-ci et des réseaux sociaux ainsi qu'aux dérives et aux risques liés à ces outils et aux contenus générés par l'intelligence artificielle ainsi qu'à la lutte contre la désinformation. Il est désormais précisé que *"cette attestation est obligatoire pour tous les élèves à l'issue de la première année de collège et doit être renouvelée à l'issue de la dernière année de collège"*. Par conséquent, il convient de souligner l'importance que ces dispositifs de formation relatifs à l'utilisation de l'intelligence artificielle incluent, outre les risques relatifs à la désinformation, les risques tenant aux atteintes aux personnes.

Obligations incombant aux fournisseurs de services. Au-delà, des dispositions du droit de l'Union européenne viennent également encadrer l'activité des opérateurs dont les services peuvent être utilisés pour générer ou diffuser ce type de contenus.

Concernant les fournisseurs et déployeurs de systèmes d'Intelligence artificielle, différentes obligations sont ainsi imposées au titre du Règlement Intelligence artificielle (RIA) du 13 juin 2024.

Ainsi, certaines dispositions du RIA visent expressément la production de deepfakes que le texte définit comme "*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 authentique ou véridique*". Ainsi, le texte consacre une obligation de transparence visant à identifier explicitement ces contenus

[248] V. en ce sens, le paragraphe suivant "Angleterre et Pays de galle" (pt. 6.2.3).

hypertruqués, étant précisé que ces dispositions entreront en vigueur en août 2026[249]. L'article 50.2 du RIA impose tout d'abord aux fournisseurs de SIA une obligation d'apposer un tatouage sur les contenus hyper truqués[250]. L'article 50.4 du RIA soumet ensuite les déployeurs de SIA à une obligation d'informer les utilisateurs de la nature "hypertruquée" du contenu[251]. Cette

[249] Pour anticiper l'entrée en vigueur de ces dispositions, une proposition de loi visant à permettre d'identifier les images générées par IA sur les réseaux sociaux a été déposée à l'Assemblée nationale le 3 décembre 2024 visant à modifier la LCNE pour préciser en son article 6-6 que "*toute personne publiant sur un réseau social une image générée ou modifiée par un système d'intelligence artificielle est tenue d'en mentionner explicitement l'origine. Cette obligation inclut un avertissement clair et visible précisant l'utilisation d'un modèle d'intelligence artificielle pour créer ou modifier l'image.Les services de plateforme en ligne au sens du i de l'article 3 du 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 (DSA) sont tenues de mettre en place des moyens techniques pour détecter les contenus générés par intelligence artificielle et vérifier la conformité de leur étiquetage. Elles doivent également informer leurs utilisateurs sur les obligations en vigueur et fournir un outil de signalement pour les contenus suspects*".

[250] RIA, article 50.2 : *"Les fournisseurs de systèmes d'IA, y compris de systèmes d'IA à usage général, qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA. Les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet, compte tenu des spécificités et des limites des différents types de contenus, des coûts de mise en œuvre et de l'état de la technique généralement reconnu, comme cela peut ressortir des normes techniques pertinentes. Cette obligation ne s'applique pas dans la mesure où les systèmes d'IA remplissent une fonction d'assistance pour la mise en forme standard ou ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique, ou lorsque leur utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière".* Sur la présentation spécifiques des techniques de watermarking, v. LINC, Le tatouage numérique, une mesure de transparence salutaire ?, 2023 et, sur les limites du tatouage, v. Parlement européen, Generative AI and watermarking, 2023.

[251] RIA, article 50.4: *"Les déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage indiquent que les contenus ont été générés ou manipulés par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière. Lorsque le contenu fait partie d'une œuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre. Les déployeurs d'un système d'IA qui génère ou manipule des textes publiés dans le but d'informer le public sur des questions d'intérêt public indiquent que le texte a été généré ou manipulé par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, ou lorsque le contenu généré par l'IA a fait l'objet d'un processus d'examen humain ou de contrôle éditorial et lorsqu'une personne physique ou morale assume la responsabilité éditoriale de la publication du contenu".* L'article 50.5 du RIA précise que ces informations sont *"fournies aux personnes physiques concernées de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition. Les informations sont conformes aux exigences applicables en matière d'accessibilité".*

exigence de transparence constitue une mesure d'atténuation visant à réduire au maximum les effets manipulateurs des deepfakes.

Dans certains cas, les contenus hypertruqués peuvent être la source de préjudices significatifs pour les personnes et tomber sous le coup de l'interdiction prévue à l'article 5 paragraphe 1 a) et b) du RIA[252]. En effet, ce texte prévoit une liste limitative des pratiques interdites en matière d'IA, parmi lesquelles les systèmes d'IA qui déploient des techniques subliminales, délibérément manipulatrices ou trompeuses qui sont significativement nuisibles et influencent matériellement le comportement de personnes physiques ou de groupes de personnes[253]ou qui exploitent les vulnérabilités dues à l'âge, à un handicap ou à une situation socio-économique particulière[254]. Les lignes directrices de la Commission européenne pour l'application de l'article 5 du RIA[255], précisent que ces interdictions qui sont entrées en vigueur le 2 février 2025 visent à prévenir les comportements préjudiciables susceptibles de constituer ou d'entraîner des infractions pénales dont la production et la diffusion de contenus illicites, tels que les contenus pédopornographiques et les "deepfakes" sexuellement explicites.

D'autres obligations sont encore imposées aux fournisseurs de modèles d'IA à usage général présentant un risque systémique pourraient par ailleurs permettre d'appréhender la production de contenus hypertruqués, en particulier les deepfakes à caractère sexuel représentant une personne sans son consentement et les contenus synthétiques pédocriminels. En effet, en vertu de l'article 55 du RIA, les fournisseurs de modèles d'IA à usage général sont tenus de réaliser une évaluation des risques systémiques[256] et de mettre en œuvre les mesures de prévention et d'atténuation appropriées[257]. Ils pourront s'appuyer sur des codes de bonnes pratiques au sens de l'article 56 du RIA pour démontrer qu'ils respectent ces obligations[258]. À cet égard, le projet de Code de bonnes pratiques générales en matière d'IA[259] prévoit, dans sa version du 11 mars 2025, que les risques

[252] Commission européenne, Communication de la Commission, Lignes directrices sur les pratiques interdites en matière d'intelligence artificielle au sens de l'article 5 du Règlement UE 2024/1689 (Règlement sur l'IA) , 29 juillet 2025, p. 22-23.
[253] RIA, article 5, 1, a).
[254] RIA, article 5, 1, b.
[255] Lignes directrices sur les pratiques interdites en matière d'intelligence artificielle, préc., p.57 - v. également, Petition No 1256/2023 by Lorena Portabales Rodríguez (Spanish) on Artificial Intelligence and child pornography, 6 août 2024 évoquant, au titre de ces interdictions, les systèmes d'IA qui génèrent du matériel pédopornographique d'abus sexuels sur des enfants en tant que systèmes qui exploitent les vulnérabilités des enfants et peuvent être utilisées pour contraindre, forcer, menacer les enfants ou influencer leur comportement d'une manière susceptible de leur nuire gravement, notamment en mettant en danger leur sécurité, leur intégrité physique et psychologique et leur développement personnel ainsi que les applications d'IA générant des images de femmes à caractère sexuel sans leur consentement.
[256] RIA, article 55, 1, a) .
[257] RIA, article 55, 1, b).
[258] RIA, Article 55, 2.
[259] EI AI ACT : GENERAL PURPOSE AI, Code of Practices, Draft 11 March 2025.

portant atteinte aux droits fondamentaux doivent faire l'objet d'une analyse approfondie[260]. Au titre de ces risques, le projet mentionne notamment les atteintes à la vie privée, les violences fondées sur le genre, les abus sexuels sur mineurs (CSAM) ainsi que la diffusion non consentie d'images intimes (NCII)[261]. De manière générale, les signataires du projet de code doivent prendre des mesures proportionnelles pour atténuer au mieux ces risques systémiques en mettant en œuvre des mesures techniques telles que : "*(1) filtering and cleaning training data; (2) monitoring and filtering the inputs and outputs of such models; (3) changing the behaviour of such a model in the interests of safety, such as fine-tuning the model to refuse certain requests; (4) restricting the availability of such a model on the market, such as restricting model access to vetted users; (5) offering countermeasures or other safety tools to other actors; (6) implementing high-assurance quantitative safety guarantees concerning the behaviour of such a model; and (7) implementing infrastructure that could help promote safe ecosystems of AI agents, such as a reputation system, specialised communication protocols, or incident monitoring tools*"[262]. Le code de bonnes pratiques sur l'IA à finalité générale fournira aux signataires davantage de détails sur la manière de garantir le respect de ces obligations.

En ce qui concerne la diffusion de ces contenus hypertruqués à caractère sexuel et des contenus pédocriminels, les plateformes tels que les réseaux sociaux sont tenues en application de l'article 6 du DSA de supprimer promptement ces contenus dès lors qu'ils sont clairement illicites après réception d'une notification dans les conditions prévues par le texte, en particulier lorsque le signalement leur a été adressé par un signaleur de confiance. S'il s'agit de l'image ou représentation d'un mineur de nature pédocriminelle au sens de l'article 221-23 du Code pénal, le fournisseur du service doit de plus signaler le contenu à l'autorité compétente, et lui fournir des informations pour identifier les auteurs en application de l'article 6 IV-A de la LCEN ; au titre de l'article 6-1 de la LCEN, l'autorité administrative peut également demander à toute personne dont l'activité est d'éditer un service de communication au public en ligne ou aux fournisseurs de services d'hébergement de retirer ces contenus dans les 24 heures. Il convient en outre de rappeler que le DSA vient également imposer différentes obligations aux fournisseurs de services de réseaux sociaux afin de responsabiliser ces opérateurs. Il leur revient ainsi de respecter une obligation de "*Safety by design*" ; selon l'article 28 du DSA, ils sont ainsi tenus 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[263]. A cet égard, les lignes directrices de l'article 28 précisent que les fournisseurs de services doivent mettre en œuvre des solutions techniques visant à empêcher que les systèmes d'intelligence artificielle de leur plateforme ne permettent aux utilisateurs d'accéder, de générer et de diffuser des contenus préjudiciables à la vie privée, à la sécurité et/ou à la sûreté des mineurs[264]. C'est sur ce fondement que la Commission européenne a

[260] Code of Practices, Draft 11 March 2025, Annexe 1.2. Autres types de risques à prendre éventuellement en compte dans la sélection des risques systémiques.
[261] Ibid.
[262] Code of Practices, 11 Draft March 2025, Technical risk mitigation for providers of GPAISR.
[263] Sur ce point, v. Chapitre 11 "Conception des services", Safety by design.
[264] Commission européenne, COMMUNICATION DE LA COMMISSION, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, p.27, pt. 72, h.

lancé une enquête le 10 octobre 2025 à l'encontre d'Apple et Google concernant leur magasin d'applications pour "obtenir des informations sur la manière dont ils gèrent le risque que les utilisateurs, y compris les mineurs, puissent télécharger des applications illégales ou autrement préjudiciables, comme des outils pour créer du contenu sexualisé non consensuel, les "*applications nudify*""[265], alors qu'il avait été recommandé par la CNCDH que les magasins d'application et moteurs de recherche se trouvent contraints de bloquer l'accès à ce type d'application afin de mieux protéger l'intimité des mineurs en ligne[266].

Les réseaux sociaux désignés comme très grandes plateformes doivent en outre réaliser une analyse de risque (article 34) et mettre en œuvre des mesures d'atténuation afin de protéger les droits de l'enfant ainsi que leur santé physique et mentale (article 35)[267].

6.2.2. États-Unis

Droit fédéral. Compte tenu du nombre de plus en plus important d'atteintes à la personne résultant de la diffusion de deepfake à caractère sexuel, notamment de plusieurs célébrités ainsi que d'élèves et étudiants, et des conséquences "*catastrophiques et impensables*"[268] pouvant en résulter, différentes évolutions du droit fédéral ont été envisagées pour encadrer le recours à ces contenus hypertruqués et renforcer la protection des victimes[269].

Ainsi, le Tools to Address Known Exploitation by Immobilizing Technological Deepfakes On Websites and Networks (TAKE IT DOWN) Act, adopté par le Congrès le 28 avril 2025[270] et signé par le président le 19 mai 2025, consacre de nouvelles incriminations portant sur la diffusion ou menace de diffusion de "*digital forgery"* définie comme *"any intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual*"[271]. Tout d'abord, est prohibé le fait pour toute personne d'utiliser un "*interactive*

[265] Commission européenne, Communiqué de presse, 10 octobre 2025.
[266] CNCDH, Avis préc., recommandation n°17.
[267] Sur ce point, v. Chapitre 2, pt. 2.1.2.4. analyses de risques.
[268] Memorandum THE TAKE IT DOWN ACT: A CONSTITUTIONAL, TARGETED APPROACH TO ADDRESSING THE SPREAD OF NON CONSENSUAL INTIMATE IMAGERY ONLINE, 8 April 2025, p. 4.
[269] En faveur de cette évolution, v. notamment M.A. Franks, A.E. Waldman, "Sex, Lies, and Videotape : Deep Fakes and Free Speech Discussions", 78 *Md. L. Rev.* 892 (2019) et D.K. Citron, R. Chesney, "Deep Fakes : A Looming Challenge for Privacy, Democracy, and National Security", 107 *California Law Review* 1753 (2019).
[270] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes On Websites and Networks (TAKE IT DOWN) Act, Public Law No. 119-12 (05/19/2025). Pour une explication du texte et de sa conformité à la Constitution, et en particulier au premier amendement, v. le Memorandum préc.
[271] TAKE IT DOWN Act, s. 2.

computer service"[272] afin de publier sciemment une "*digital forgery"* d'une personne majeure identifiable sans son consentement dans l'intention de lui causer un préjudice ou lui causant un préjudice, y compris un préjudice psychologique, financier ou réputationnel[273]. Est également prohibé le fait d'utiliser ces mêmes services afin de publier une "*digital forgery"* d'une personne mineure identifiable dans l'intention (i) de l'abuser, l'humilier, la harceler ou la dégrader ou (ii) de susciter ou satisfaire le désir sexuel de toute personne. Le texte prévoit des peines d'amendes et/ou de 2 ans d'emprisonnement lorsque la diffusion de *digital forgery* implique une personne majeure, et des peines d'amende et/ou de 3 ans d'emprisonnement si elle implique une personne mineure[274]. Par ailleurs, sont spécifiquement incriminés les cas de sextorsion lorsque la menace implique ce type de contenu[275].

Le Preventing Deepfakes of Intimate Images Act[276], déposé au Congrès, vise quant à lui à interdire la divulgation non consensuelle d'images intimes modifiées numériquement et à reconnaître que le partage de ces images est un délit pénal ainsi qu'à garantir que le consentement d'une personne à la création de l'image ne constitue pas un consentement au partage ou à la divulgation de l'image. Le texte propose en outre de reconnaître un droit d'action privé pour les victimes afin d'obtenir réparation de leurs préjudices et de consacrer des protections supplémentaires pour préserver leur anonymat.

Droit étatique. Trente-sept États ont incriminé les images d'abus sexuels d'enfants générées ou modifiées par l'IA, en modifiant les lois existantes sur les images d'abus sexuels d'enfants ou en en adoptant de nouvelles[277]. À titre d'exemple, depuis janvier 2025, le Code pénal de Californie interdit la création, la vente, la possession et la distribution de tout "*contenu modifié numériquement ou généré par l'intelligence artificielle*" représentant une personne de moins de 18 ans se livrant à un comportement sexuel ou simulant un tel comportement[278]. Par ailleurs, en octobre 2025, le gouverneur de Californie a signé plusieurs projets de loi visant à renforcer le cadre légal de cet État en matière de protection des enfants en ligne[279]. Parmi ce paquet législatif, figurent

---

[272] 47 USC §230 : "*The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions"*, ce qui inclut les réseaux sociaux.

[273] TAKE IT DOWN Act, s. 2, (3) A.

[274] TAKE IT DOWN Act, s. 2, (3) B.

[275] TAKE IT DOWN Act, s. 6 - Sur ce point, v. supra.

[276] Preventing Deepfakes of Intimate Images Act, HR.1941 - 119th Congress, 2025.

[277] Au 9 janvier 2025, 32 États ont promulgué des lois concernant la création ou la distribution de deepfakes représentant des actes sexuels explicites ou d'autres contenus sensibles. Ces législations ciblent notamment la création et la diffusion de matériel pédopornographique, ainsi que la production et la distribution non consensuelles d'images intimes d'adultes (chiffres cités par le site BallotPedia, Section pornographic materials).

[278] California, Penal Code, Part. 1, Title 9, Chapter 7.5, 311.11 modifié par le AB 1831, Berman. Crimes: child pornography.

[279] Governor Newsom signs bills to further strengthen California's leadership in protecting children online, 13 October 2025.

notamment des dispositions[280] relatives à des sanctions plus sévères concernant la "*deepfakes pornography*" en élargissant le champ d'application de l'action en justice afin de permettre aux victimes, y compris les mineurs, de demander une réparation civile pouvant aller jusqu'à 250 000 dollars par action contre des tiers qui facilitent ou aident sciemment la distribution de contenu sexuellement explicite non consensuel.

6.2.3. Angleterre et Pays de Galles

S'agissant du droit de l'Angleterre et du Pays de Galles, une distinction doit être réalisée selon que l'image représente un adulte ou un mineur.

Mesures répressives. Concernant les personnes majeures, l'Online Safety Act 2023 a consacré une nouvelle infraction (*criminal offence*) visant le partage d'images intimes non consensuelles. Ainsi, depuis le 31 janvier 2024, date d'entrée en vigueur du texte, est prohibée la diffusion de deepfake à caractère sexuel sans le consentement de la personne figurant sur le montage, les deepfakes étant définis comme les "*photographies ou films authentiques qui ont été modifiés d'une manière ou d'une autre, et ceux qui ont été entièrement fabriqués*"[281]. Afin de mieux lutter contre les atteintes résultant de ce type de contenus, le gouvernement a en outre annoncé en janvier 2025[282] promouvoir la consécration d'une nouvelle infraction pénale visant, au-delà de la diffusion, la création d'une image intime d'un adulte générée par l'IA, avec des sanctions pouvant aller jusqu'à 2 ans d'emprisonnement pour les auteurs, proposition désormais discutée dans le cadre du Data (Use and Access) Bill[283].

En outre, il est important de souligner que les deepfakes contenant des images sexuelles d'enfants (toute personne de moins de 18 ans) sont qualifiés de contenus illégaux au titre des CSAM[284].

Obligations des fournisseurs de service. En application de l'Online Safety Act 2023, les services numériques sont soumis à des obligations renforcées en matière de modération des contenus à caractère sexuel. Il est intéressant de relever que, dans ses lignes directrices sur l'évaluation des risques publiées en décembre 2024[285], l'OFCOM recommande aux services en ligne de prendre en compte le risque spécifiquement lié à la diffusion de deepfakes. À ce titre, les plateformes sont

---

[280] Bill Text: CA AB621 | 2025-2026

[281] Sexual Offences Act, Section 66B modifié par le Online Safety Act (2023).

[282] Ministry of Justice (2025), Government cracks down on 'deepfakes'creation. Si ce texte n'a pas pu être adopté lors de la dernière législature, le Parti travailliste s'est engagé à poursuivre et à incriminer la création de deepfakes sexuellement explicites d'adultes : Labour Party (2024), Change: Labour Party Manifesto.

[283] Data(Use and Access) Bill [HL], volume 843, 28 January 2025.

[284] Sur ce point, v. supra, Chapitre 4 "Diffusion non consentie de contenus intimes", Angleterre et Pays de Galle (pt. 4.2.3).

[285] Protecting people from illegal harms online - Risk Assessment Guidance and Risk Profiles, 16 December 2024, en particulier point 5.E ('*user-to-user services*').

tenues d'évaluer dans quelle mesure leurs services permettent ou facilitent la création ou la diffusion de deepfakes à caractère illégal.

6.2.4. Australie

En Australie, différentes évolutions du cadre légal ont visé à renforcer la protection des victimes de diffusion de deepfakes à caractère sexuel non consentie. Ainsi, le Criminal Code Amendment (Deepfake Sexual Material) Act 2024, entré en vigueur en septembre 2024, est venu modifier le Criminal Code Act 1995 pour préciser que l'incrimination visant la diffusion de contenu à caractère sexuel représentant une personne majeure sans son consentement couvre également les contenus synthétiques[286]. Lorsque la victime du partage non consenti du contenu hypertruqué est une personne mineure, les faits seront poursuivis au titre des infractions consacrées par le Criminal Code Act 1995 relatives au Child Sexual Abuse Material (CSAM)[287].

Par ailleurs, en application de l'Online Safety Act 2021[288], toute personne peut déposer une plainte auprès de l'eSafety Commissioner concernant la publication ou menace de publication non consentie d'image intime, ce qui inclut les contenus deepfakes[289]. L'eSafety Commissioner peut adresser un avis de retrait à l'auteur, au service en ligne ou au fournisseur de services d'hébergement. Les auteurs peuvent également recevoir des instructions leur imposant de prendre des mesures correctives spécifiques concernant le contenu. Des sanctions peuvent être appliquées ou demandées en cas de non-respect d'un avis de retrait ou d'une mesure corrective[290].

---

[286] Criminal Code Amendment (Deepfake Sexual Material) Act 2004, n°78, 2024, modifiant la Section 474.17.A. - v. également la Section 474.17.AA sur les cas d' "*aggravate offences*".

[287] Sur ces différents points, v. infra, Chapitre 4 développements relatifs au partage non consenti de contenus intimes.

[288] Online Safety Act, 2021.

[289] Les deepfakes sont définis comme "*a digital photo, video or sound file of a real person that has been edited to create an extremely realistic but false depiction of them doing or saying something that they did not actually do or say. Deepfakes are created using artificial intelligence software that currently draws on a large number of photos or recordings of the person to model and create content*" : eSafety Commissioner, Deepfakes trends and challenges - position statement, 19 September 2024. Sur l'applicabilité de ce système de plainte en cas de contenus deepfakes, v. eSafety Commissioner, eSafety Submission: Senate Standing Committee on Legal and Constitutional Affairs, Legislation Committee, Criminal Code Amendment (Deepfake Sexual Material Bill) 2024, 23 July 2024, p 2.

[290] Par exemple : eSafety Commissioner v Rotondo (No 3) [2023] FCA 1590 (6 December 2023). En 2023, une personne a fait l'objet d'une enquête par le eSafety Commissioner concernant la publication non consensuelle d'images intimes hypertruquées de plusieurs femmes sur un site web. Un délégué de l'eSafety Commissioner a émis un avis de retrait et une mesure corrective à l'encontre de cette personne, lui imposant à l'auteur, entre autres, de retirer le matériel du site et de s'abstenir de publier d'autres images intimes des femmes sans leur consentement. L'individu n'a pas respecté la mesure corrective et s'est ensuite rendu en Australie depuis son lieu de résidence habituel aux Philippines. L'eSafety Commissioner a entamé une procédure à son encontre devant la Cour fédérale d'Australie afin d'obtenir une injonction et une sanction civile. Le tribunal a ordonné à l'individu de retirer les

Au-delà, le rapport de la revue de l'Online Safety Act 2021 recommande que le gouvernement australien étudie la meilleure façon d'interdire aux moteurs de recherche et aux magasins d'applications d'afficher, de vendre ou de distribuer des applications et services de "dénudage" ainsi que des applications de cyber-espionnage indétectables[291].

6.3. PRÉCONISATIONS

Préconisation 14 - **Renforcer la réponse pénale**

a. Incriminer, en complément de la diffusion de deepfake à caractère sexuel sans le consentement de la personne telle que visée à l'article 226-8-1 du Code pénal, la création de ce type de contenu.

Source : CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°20

b. Renforcer la protection des mineurs en (1) érigeant en circonstance aggravante la minorité de la victime et (2) pour les mineurs de moins de 15 ans, en interdisant ce type de contenu sans référence dans ce cas à leur consentement éventuel.

Source: CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°19

Préconisation 15 - **Responsabiliser les opérateurs dont les réseaux sociaux et les fournisseurs de système d'IA**

a. S'assurer du suivi de l'évaluation des risques par les très grandes plateformes au titre du DSA et par les fournisseurs de modèles de fondation à finalité générale comportant des risques systémiques au titre du Règlement IA ainsi que de l'adoption des mesures d'atténuation de ces risques en ce qui concerne l'impact sur les victimes (et en particulier l'atteinte à leurs droits fondamentaux, leur santé et leur bien-être) résultant de la création et de la diffusion de deepfake à caractère sexuel.

b. Développer le recours aux techniques de filigrane et de hachage en partenariat avec les générateurs de deepfakes (cf. StopNCII, DISRUPT…).

c. S'assurer que les fournisseurs de systèmes d'IA générative bride la capacité du système à produire des deepfakes à caractère sexuel mettant en scène des enfants et mettent en place les moyens suffisants pour en garantir l'effectivité ; il s'agira notamment de vérifier que le système ne peut pas être ou n'a pas été détourné en testant sa robustesse et en mettant en place des mécanismes de réponse adaptés pour corriger tout risque de contournement

images du site web et de s'abstenir de publier ou d'envoyer des images intimes non consensuelles. Cette personne ne s'est pas conformée à ces ordonnances et a été inculpée de trois chefs d'accusation d'outrage au tribunal, condamné à des amendes d'un montant total de 25 000 dollars.

[291] Delia Rickard PSM, Report of the Statutory Review of the Online Safety Act 2021, October 2024, Recommandation 27.

Sources : CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°16 - v. également Commission européenne, Lignes directrices, 14 juillet 2025, 6.7-72h

d. S'assurer du déréférencement sur les moteurs de recherche des sites et des applications dédiés aux deepfakes à caractère sexuel, ainsi que du blocage sur les magasins d'applications de toute application de dénudage concernant les mineurs

Source : CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°17

Préconisation 16 - Favoriser le signalement de deepfake à caractère sexuel en créant une classification de contenus "Atteinte à l'intimité des personnes" (vidéo, audio, images) les incluant tant (1) dans les dispositifs de signalements proposés par les réseaux sociaux que (2) dans les catégories de signalement proposées sur la plateforme PHAROS

Source : CNCDH, Avis protection de l'intimité des jeunes en ligne, recommandation n°24

Préconisation 17 - Développer les actions de sensibilisation concernant les risques relatifs aux deepfakes, en particulier concernant les deepfakes à caractère sexuel (v. les recommandations générales) notamment dans le cadre de la formation prévue à l'article L. 312-9 du Code de l'éducation.

CHAPITRE 7 : EXPOSITION À DES CONTENUS VIOLENTS ET À CARACTÈRE PORNOGRAPHIQUE

Les pratiques des mineurs en ligne les conduisent, de manière plus ou moins volontaire, à être exposés à des contenus inappropriés en particulier sur les réseaux sociaux, et notamment à des contenus violents et à caractère pornographique. Les recherches menées montrent une tolérance de la part des enfants à l'égard de ces contenus, qu'ils considèrent de plus en plus comme un "risque normal" de la vie en ligne[292]. Leur acceptation, bien qu'elle témoigne d'un certain réalisme, nuit aux efforts d'éducation à l'autoprotection et réduit la fréquence des signalements. En outre, ces contenus sont susceptibles de heurter leur sensibilité ou de porter atteinte à leur santé mentale ou physique[293].

7.1. PRATIQUES

Parmi les différents contenus inappropriés pour les mineurs, les inquiétudes se cristallisent tout particulièrement autour des contenus pornographiques. Une enquête menée en 2024[294] sur les 11-18 ans révèle que plus d'un tiers des enfants de cette tranche d'âge (33 %) ont déjà été confrontés à des scènes pornographiques. L'âge moyen du premier visionnage de ce type de contenu, qu'il soit accidentel ou volontaire, se situerait désormais autour de 10 ou 11 ans. L'étude réalisée en mars 2023 par l'Arcom sur la fréquentation des sites "adultes" par les mineurs confirme l'ampleur du phénomène puisqu'environ 2,3 millions de mineurs en France consulteraient chaque mois des sites pornographiques et, parmi eux, 10 % s'y rendraient quotidiennement. Cette fréquentation a connu une augmentation marquée en l'espace de 5 ans, avec 600 000 mineurs supplémentaires concernés, soit une hausse de 36 %[295]. La majorité des consultations (75 %) se fait via un téléphone portable, ce qui rend le contrôle parental d'autant plus difficile[296]. En outre, il convient de souligner que "*ces contenus sont toujours plus choquants, violents, et non contrôlés, et sont donc d'autant*

---

[292] Eurochild, The rights of children in the digital environment, 2025 - Commission européenne, BIK plus Strategy 2025, First évaluation of the European Strategy Better Internet for Kids (BIK +), February 2025 - 5Rights Foundation Disrupted Childhood: The cost of persuasive design, 2024 - OFCOM, Understanding Pathways to Online Violent Content Among Children Qualitative Research Report, March 2024.

[293] OFCOM, Understanding Pathways to Online Violent Content Among Children Qualitative Research Report, préc.

[294] Génération numérique, Enquête sur les contenus choquants accessibles aux mineurs, janv. 2024.

[295] Arcom, Étude sur la Fréquentation des sites adultes par les mineurs, 2023 : selon l'étude, la fréquentation des sites adultes concerne 21% des garçons de 10-11 ans, 51% pour les 12-13 ans (31% pour les filles), 59% pour les 14-15 ans (27% pour les filles) et 65% pour les 16-17 ans (31% pour les filles.

[296] Ibid.

plus inadaptés à un public mineur, qui parfois n'a pas explicitement cherché ce contenu et se l'est vu imposé, ou y a eu accès alors qu'il cherchait à se renseigner sur la sexualité"[297].

En pratique, on observe que les réseaux sociaux sont devenus de nouveaux canaux de la diffusion de contenus pornographiques, outre l'émergence récente de plateformes dédiées au partage et à la monétisation de contenus à caractère sexuel (ex : MYM ou Onlyfans) ; les messageries privées telles que WhatsApp sont également de plus en plus utilisées pour les échanges et téléchargements de contenus pornographiques, particulièrement au sein du public adolescent[298].

Or, le Haut Conseil à l'Égalité entre les femmes et les hommes souligne que cette exposition peut avoir des conséquences sur le développement psychologique et émotionnel des mineurs, alimentant la misogynie, la confusion entre sexualité et violence, et peut même être qualifiée de "*viol psychique*" chez les plus jeunes[299].

Il convient toutefois d'observer, comme le relève le rapport de la mission "Enfants et écrans" que "l*es jeunes aujourd'hui n'accèdent que très peu, voire plus, à des contenus qui répondent à leurs besoins de découverte et d'éveil à la vie sexuelle et affective. Leur seule option reste bien souvent la consultation de contenus pornographiques. Il manque ainsi un entre-deux, entre des sites pornographiques très "trash*", *et l'absence de tout soutien à des questions que se posent légitimement les jeunes, en particulier à l'adolescence. Il nous faut donc disposer de contre-mesures informationnelles pour diffuser des contenus différents sur la vie affective, l'amour, la*

[297] Mission Enfants et Ecrans, À la recherche du temps perdu, 2024, p. 48.

[298] Selon un sondage Ifop de 2021, 31 % des adolescents de 15 à 17 ans ont eu accès à de la pornographie sur des réseaux sociaux et 24 % via des messageries, c'est-à-dire, dans ce dernier cas au moins, directement entre jeunes (IFOP, Étude sur les effets et conséquences de la loi du 30 juillet 2020 sur le visionnage de contenus pornographiques par les adolescents français, 2021) - v. également, Sénat, Porno : l'envers du décor, Rapport d'information n° 900 (2021-2022)202, p. 84.

[299] HCE, CP - Fréquentation en hausse des sites pornographiques par les mineur·es : urgence à agir !, 25 mai 2023. V. également, HCE, Rapport annuel 2024 sur l'état des lieux du sexisme en France, p. 29 ou encore HCE, Pornocriminalité : Mettons fin à l'impunité de l'industrie pornographique, 2023. 44 % des jeunes ayant déjà eu un rapport sexuel déclarent avoir essayé de reproduire des scènes ou des pratiques vues dans des films ou vidéos pornographiques (Service public, Je protège mon enfant de la pornorgaphie). Il convient à cet égard de relever que l'essor des "tubes", de véritables fournisseurs d'images pornographiques, a transformé l'économie de l'industrie pornographique, qui reposait autrefois principalement sur une consommation payante, avec un accès relativement encadré et réglementé à des contenus vidéos produits de manière plus "classique" par des entreprises fonctionnant sur le modèle de grandes productions cinématographiques. Le besoin massif de nouveaux contenus pour alimenter ces plateformes a contribué à des pratiques favorisant les violences sexistes et sexuelles envers les femmes, leur exploitation sexuelle, ainsi que la production de contenus de plus en plus explicites et violents pour répondre aux intérêts économiques de l'industrie du sexe : v. Sénat, Porno : l'envers du décor, rapport préc.

sexualité et le consentement"[300]. On constate par ailleurs que l'éducation à la sexualité dispensée dans le cadre de l'Education nationale est déficiente[301].

Par ailleurs, l'exposition des jeunes à des contenus violents en ligne est aujourd'hui importante et particulièrement préoccupante. Selon l'enquête menée par Génération numérique en janvier 2024 auprès des 11-18 ans, 3 jeunes sur 10 ont déjà été confrontés à des contenus choquants sur Internet ou sur les réseaux sociaux. 45% d'entre eux ont été exposés à des scènes de maltraitance animale et 25 % à des contenus d'une violence extrême, incluant des scènes de guerre, de torture ou d'exécution[302].

7.2. CADRE JURIDIQUE

La volonté de protection des mineurs a conduit les législateurs européen et français à consacrer un cadre juridique concernant les contenus inappropriés, qui appréhende l'exposition à des contenus violents et pornographiques.

Ainsi, en droit français, l'article 227-24 du Code pénal incrimine la fabrication, la diffusion ou le commerce d'un "*message à caractère violent, incitant au terrorisme, pornographique, y compris des images pornographiques impliquant un ou plusieurs animaux, ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger (…) lorsque ce message est susceptible d'être vu ou perçu par un mineur*", y compris si l'accès du mineur à ce message "*résulte d'une simple déclaration de celui-ci indiquant qu'il est âgé d'au moins dix-huit ans*". Le fournisseur de service de réseau social doit supprimer promptement de tels contenus dès lors qu'ils lui sont notifiés dans les conditions prévues par l'article 6 du DSA ; il doit en outre les signaler aux autorités compétentes en vertu de l'article 6, IV, A de la LCEN et leur auteur peut être soumis à une peine complémentaire de bannissement[303].

---

[300] Rapport de la Mission enfants-écrans, A la recherche du temps perdu, préc. p.91.

[301] A. Toullier, N. Gautier, Pour une véritable éducation à la sexualité. Les recommandations de la société civile aux pouvoirs publics, Livre Blanc, les recommandations de la société civile, 2023.

[302] Génération numérique, Enquête sur les contenus choquants accessibles aux mineurs, Janvier 2024. Selon une étude de l'OFCOM pour le Royaume Uni, les enfants interrogés ont déclaré avoir été accidentellement exposés à des contenus violents sur la plupart des réseaux sociaux, des services de partage de vidéos et de messagerie, ainsi que sur des forums de discussion, des salons de chat et des services pornographiques, mentionnant le plus souvent mentionné TikTok, Instagram, Snapchat, YouTube, Twitter (X) et Facebook. Les enfants ont également expliqué qu'il existait des comptes privés, souvent anonymes, destinés uniquement à partager des contenus violents, le plus souvent des bagarres dans les écoles ou dans la rue. Presque tous les enfants interrogés dans le cadre de cette étude ayant interagi avec ces comptes ont déclaré les avoir trouvés sur Instagram ou Snapchat : OFCOM, Understanding Pathways to Online Violent Content Among Children Qualitative Research Report, March 2024.

[303] Code pénal, art. 131-35-1, II, 4°.

Par ailleurs, la Directive 2018/1808 Services de médias audiovisuels (SMA) prévoit l'obligation de protéger les mineurs des programmes, vidéos créées par l'utilisateur et communications commerciales audiovisuelles susceptibles de nuire à leur épanouissement physique, mental ou moral, soulignant que la pornographie et la violence gratuite devront "*faire l'objet des mesures les plus strictes*" (article 6 bis). La Directive SMA ne prévoit pas de sanction, mais dispose que les États membres doivent en assurer la mise en œuvre effective au moyen de sanctions efficaces et proportionnées (article 4 bis) et conformément aux codes de conduites nationaux.

S'agissant en particulier de l'exposition des mineurs à des contenus à caractère pornographique par le biais de services en ligne, d'autres dispositions trouveront également à s'appliquer. En particulier, le droit français a été récemment modifié pour limiter l'exposition des mineurs à des contenus pornographiques en imposant un contrôle de l'âge[304]. De plus, les sites pornographiques sont désormais soumis aux dispositions du DSA. Ainsi, conformément à l'article 28 de ce texte, il leur revient 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[305]. En outre, plusieurs ont été qualifiés par la Commission européenne de très grandes plateformes - en décembre 2023[306] : PornHub, Stripchat, XVideos ; en juillet 2024[307]: XNXX - ce qui leur impose notamment de réaliser des analyses de risques et de prendre des mesures de limitation des risques[308], notamment au moyen d'outils de vérification de l'âge.

7.3. PRÉCONISATIONS

Outre les préconisations relatives au contrôle de l'âge s'agissant de l'accès aux contenus pornographiques[309]:

Préconisation 18 - Assurer le suivi des mesures de responsabilisation prévues par le DSA en particulier pour les sites pornographiques qualifiés de très grandes plateformes

Préconisation 19 - Développer des moyens de signalement et d'accompagnement consacrés aux contenus pornographiques. Envisager notamment à ce titre la mise en place d'un bouton de signalement accessible aux enfants pour signaler leur accès accidentel à des contenus pornographiques ; si tel est le cas, renvoyer vers une ligne d'écoute ainsi qu'à des ressources.
Source : Conseil de l'Europe, Pour une évaluation des moyens et des dispositifs de lutte contre l'exposition des enfants aux contenus pornographiques, pt. 6.6

Préconisation 20 - Soutenir la recherche et la mise en place de mesures de sensibilisation liés aux effets nocifs de la pornographie.

---

[304] Sur ce point, v. le Chapitre 12 "Condition d'accès au service tenant à l'âge".
[305] Sur ce point, v. Chapitre 11 "Conception des services" (Safety by design).
[306] Commission européenne, Communiqué de presse, 20 décembre 2023.
[307] Commission européenne, Communiqué de presse, 10 juillet 2024.
[308] Sur ce point, v. Chapitre 2, pt. 2.1.2.4, développements consacrés à l'analyse de risques.
[309] Sur ce point, v. Chapitre 13, "Condition d'accès au service tenant à l'âge".

Insérer des avertissements juridiques et sanitaires sur les sites pornographiques (sur les traumatismes que cela peut causer, de l'impact de la pornographie sur le développement cérébral des enfants, le risque de dysfonctions sexuelles et la réduction de la capacité à construire des relations sexuelles saines par la suite). Promouvoir la recherche sur les effets de l'exposition des enfants à la pornographie et sur les moyens de la prévenir, ainsi que concernant les moyens de lutter contre les effets nocifs d'une potentielle exposition.
Source : Conseil de l'Europe, Pour une évaluation des moyens et des dispositifs de lutte contre l'exposition des enfants aux contenus pornographiques, pts. 6.8 et 6.10

Préconisation 21 - Assurer l'accès à des ressources de qualité en matière de sexualité et d'éducation sexuelle
Sources : Livre blanc Pour une véritable éducation à la sexualité - CNNum, Éveil à la vie affective relationnelle et sexuelle - Donner le pouvoir d'agir - Mission Enfants et Ecrans, À la recherche du temps perdu

CHAPITRE 8 : INCITATION À DES CONDUITES À RISQUE

8.1. PRATIQUES

Les contenus accessibles sur les réseaux sociaux peuvent inciter directement ou indirectement les mineurs à adopter des comportements présentant un risque sanitaire. Il en est ainsi des incitations à la consommation de substances (alcool, tabac, stupéfiants notamment[310]), à certaines conduites sexuelles, aux troubles du comportement alimentaire, à la commission de crimes ou délits, à la pratique de jeux présentant un danger physique, ou à l'automutilation voire au suicide.

À cet égard, la pratique des "challenges" dont la viralité est amplifiée sur les réseaux sociaux fait l'objet d'une attention particulière. Ceux-ci peuvent être définis comme des défis à relever par une personne ou un groupe, et s'expliquent au mieux par l'exemple. Ainsi, le "blackout challenge" consiste à retenir sa respiration le plus longtemps possible tandis que le "labello challenge" peut inciter à la scarification[311].

8.2. CADRE JURIDIQUE

La lutte contre les incitations à des conduites à risque affectant des mineurs comprend des mesures à la fois répressives et éducatives. En droit français et de l'Union européenne, de nouvelles obligations sont imposées aux fournisseurs de service telles que celles enjoignant aux fournisseurs de plateformes de partage de vidéos de prendre les mesures appropriées pour s'assurer qu'aucun contenu susceptible de nuire à l'épanouissement physique, mental ou moral des mineurs ne leur soit accessible, ou qu'il ne soit pas mis à disposition du public lorsque la nuisance potentielle est "grave" (qui apparaissent toutefois dépourvues de sanction directe)[312] ou imposant aux fournisseurs de très grandes plateformes en ligne d'évaluer les risques systémiques présentés par leurs services et de les atténuer[313].

Mesures répressives. De nombreuses incitations à des comportements à risque sont prohibées en droit français ; pour la plupart, elles disposent d'un large champ d'application et ne s'appliquent

[310] Pour une mise en cause du réseau social Snapchat en tant que facilitateur du trafic de drogue auprès des jeunes, v. R. Buller, "Their kids died after buying drugs on Snapchat. Now the parents are suing", *The Guardian*, 18 October 2023.

[311] Sur les « challenges » identifiés sur le réseau social TikTok, v. not. M. Vallet, C. Malhuret, *Rapport n° 831 fait au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence*, 4 juill. 2023, pp. 127-129.

[312] Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), art. 60, I, 1° et 15 lus conjointement ; Directive SMA révisée, art. 28 ter.

[313] DSA, art. 34 et 35.

qu'incidemment aux réseaux sociaux et aux mineurs. Il est possible de distinguer les dispositions visant à interdire ou restreindre certaines formes de publicité ou propagande et les activités exercées par les influenceurs des incitations et provocations ne s'inscrivant pas dans un cadre commercial.

La propagande ou publicité en faveur de certains produits ou services est interdite – concernant le tabac, les produits assimilés et le vapotage[314] – ou restreinte, en particulier en matière d'alcool[315] ou, lorsque la promotion est effectuée par un influenceur, d'actes ou interventions à visée esthétique[316], de thérapies alternatives[317], de jeux d'argents et de hasard[318]. Est également interdite la propagande ou la publicité en faveur de produits, d'objets ou de méthodes préconisés comme moyens de se donner la mort[319].

En dehors de la sphère de l'influence commerciale, il existe diverses dispositions réprimant l'incitation à des conduites à risque[320]. Concernant tout d'abord la consommation de substances, est incriminée la provocation directe d'un mineur à la consommation excessive ou habituelle

[314] V. l'interdiction de la propagande ou publicité, directe ou indirecte, en faveur du tabac, ses produits ou ingrédients (Code de la santé publique, art. L. 3512-4 al. 1) ou des produits du vapotage (Code de la santé publique, art. L. 3513-4 al. 1), dont l'applicabilité aux influenceurs est expressément affirmée (Loi n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux, art. 3). V. aussi l'interdiction de la promotion directe ou indirecte, par des influenceurs, des produits considérés comme produits de nicotine (Loi du 9 juin 2023 préc., art. 4, III).

[315] Code de la santé publique, art. L. 3323-2, 9° : autorisation restreinte de la propagande ou publicité, directe ou indirecte, en faveur de boissons alcooliques, notamment sur les « services de communications en ligne à l'exclusion de ceux qui [...] apparaissent comme principalement destinés à la jeunesse », dont l'applicabilité aux influenceurs est rappelée par la Loi du 9 juin 2023 préc., art. 3 ; Code de la santé publique, art. L. 3342-1, al. 2 portant interdiction de l'offre, à titre gratuit ou onéreux, à un mineur de tout objet incitant directement à la consommation excessive d'alcool. Pour une application récente aux réseaux sociaux, v. Tribunal judiciaire de Paris (Procédure accélérée au fond), 5 janv. 2023, n° 22/57472, *ANPAA c/ Meta Platforms Ireland Limited* ; E. Andrieu, « Le jugement *Meta* : faux départ pour la jurisprudence sur les influenceurs et la loi Evin », *Légipresse* 2023 p.172.

[316] Loi du 9 juin 2023 préc., art. 4, I portant interdiction de la promotion directe ou indirecte, par des influenceurs, d'actes ou interventions à visée esthétique et renvoyant à la définition de ces actes et interventions du Code de la santé publique, art. L. 1151-2 et L. 6322-1 respectivement.

[317] Loi du 9 juin 2023 préc., art. 4, II : interdiction de la promotion directe ou indirecte, par des influenceurs, de procédés présentés comme comparables, préférables ou substituables à des procédés thérapeutiques.

[318] Loi du 9 juin 2023 préc., art. 4, VII : autorisation de la promotion des jeux d'argents et de hasard par des influenceurs uniquement sur les plateformes en ligne offrant la possibilité technique d'exclure de l'audience dudit contenu tous les utilisateurs mineurs et si ce mécanisme d'exclusion est activé par l'influenceur, avec mention signalant l'interdiction du contenu aux mineurs.

[319] Code pénal, art. 223-14.

[320] Pour une analyse de la plupart de ces infractions de provocation, v. J.-Y. Lassalle, « Provocation », *Rép. pén. Dalloz*, sept. 2021.

d'alcool[321], à l'usage illicite de stupéfiants, leur détention ou autre[322], ou à l'usage détourné d'un produit de consommation courante pour ses effets psychoactifs[323]. Il est également interdit de provoquer des mineurs à commettre un crime ou un délit[324] ou de transmettre un message de nature à les inciter à se livrer à des jeux les mettant physiquement en danger, dès lors qu'il est susceptible d'être vu ou perçu par un mineur[325] – cette dernière infraction étant susceptible de saisir les pratiques de "challenges". En outre, le fait d'inciter un mineur à se soumettre à une mutilation sexuelle ou d'inciter directement autrui à la commettre, lorsque celle-ci n'a pas été réalisée, est réprimé pénalement[326].

Au regard des pratiques sexuelles, sont incriminées diverses sollicitations ou incitations à caractère sexuel de la part d'un majeur[327], ainsi que la corruption de mineurs[328] ou encore la détention ou diffusion de contenus pédocriminels[329].

---

[321] Code pénal, art. 227-19, auquel renvoie explicitement le Code de la santé publique, art. L. 3353-4.

[322] Code pénal, art. 227-18 (provocation directe d'un mineur à l'usage illicite de stupéfiants) et 227-18-1 (provocation directe d'un mineur au transport, détention, offre ou cession de stupéfiants). V. aussi, sans qu'il soit nécessaire que le propos soit adressé à un mineur, Code de la santé publique, art. L. 3421-4 al. 1 et 2 : délit de provocation à l'usage illicite de stupéfiants (ou de substances présentées comme ayant un effet similaire) ou à diverses infractions en lien avec le trafic de stupéfiants, même non suivie d'effet ; délit de présentation sous un jour favorable de ces infractions.

[323] Code de la santé publique, art. L. 3611-1 : provocation d'un mineur à faire un usage détourné d'un produit de consommation courante pour en obtenir des effets psychoactifs.

[324] Code pénal, art. 227-21 : provocation directe d'un mineur à commettre un crime ou un délit. V. également en matière de provocation publique, sans qu'il soit besoin de viser un mineur : Loi du 29 juillet 1881 sur la liberté de la presse, art. 23 et 24 al. 1 à 4.

[325] Code pénal, art. 227-24, précisant que l'infraction est constituée même si l'accès d'un mineur aux messages résulte d'une simple déclaration de celui-ci indiquant qu'il est âgé d'au moins dix-huit ans.

[326] Code pénal, art. 227-24-1 : offre, promesse, proposition d'avantages quelconques, pression ou contrainte afin qu'un mineur se soumette à une mutilation sexuelle, lorsque cette mutilation n'a pas été réalisée ; ou incitation directe d'autrui, par les mêmes moyens, à commettre une mutilation sexuelle sur un mineur lorsque cette mutilation n'a pas été réalisée.

[327] Code pénal, art. 227-22-1 (propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique) ; art. 227-22-2 (incitation d'un mineur, par un moyen de communication électronique, à commettre tout acte de nature sexuelle, soit sur lui-même, soit sur ou avec un tiers, y compris si cette incitation n'est pas suivie d'effet, excluant les cas de viol et d'agression sexuelle) ; art. 227-23-1 (sollicitation auprès d'un mineur de la diffusion ou la transmission d'images, vidéos ou représentations à caractère pornographique dudit mineur) ; art. 227-22 (organisation de réunions comportant des exhibitions ou des relations sexuelles auxquelles un mineur assiste ou participe ou d'assister en connaissance de cause à de telles réunions).

[328] Code pénal, art. 227-22.

[329] Code pénal, art. 227-23 : fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation à caractère pornographique d'un mineur et, s'il s'agit d'un mineur de moins 15 ans, même sans visée de diffusion ; ou encore de rendre disponible ou diffuser cette image, de consulter habituellement ou contre paiement un site pédopornographique, de détenir une telle image.

Certaines infractions, bien que pensées indifféremment de l'âge de la victime, poursuivent les mêmes objectifs : il en est ainsi de l'incrimination de la provocation au suicide, si elle est suivie du suicide ou d'une tentative en ce sens[330], et de l'abus de faiblesse[331]. Seule cette dernière pourrait sembler à même de saisir certains cas d'incitation aux troubles du comportement alimentaire ou à l'automutilation, de manière très imparfaite.

Lorsqu'elles constituent des contenus illicites, les incitations à des conduites à risques doivent être supprimées promptement par le fournisseur de service de réseau social dès lors qu'elles lui sont notifiées dans les conditions prévues par l'article 6 du DSA. Certains de ces contenus relèvent en outre de l'obligation de signalement, de la part du fournisseur de service et à destination des autorités compétentes, énoncée par l'article 6, IV, A de la LCEN[332] et peuvent faire l'objet d'une peine complémentaire de bannissement[333].

Mesures éducatives. En vertu du Code de l'éducation, les élèves doivent recevoir une information et éducation à la sexualité[334], à l'alimentation et à la lutte contre le gaspillage alimentaire[335], de même qu'une information sur les réalités de la prostitution et les dangers de la marchandisation du corps[336]. Plus particulièrement sur la consommation de substances, ils doivent disposer d'une information sur les conduites addictives et leurs risques, notamment concernant les effets neuropsychiques et comportementaux du cannabis[337]. Le Code de la santé publique y ajoute une information de nature sanitaire prophylactique et psychologique dans les établissements scolaires, incluant une sensibilisation au risque tabagique obligatoire dans les cycles primaire et secondaire[338].

---

330 Code pénal, art. 223-13.

331 Code pénal, art. 223-15-2 : abus frauduleux de l'état d'ignorance ou de la situation de faiblesse, notamment d'un mineur, pour le conduire à un acte ou à une abstention qui lui sont gravement préjudiciables.

332 Tel est le cas de la provocation directe d'un mineur à l'usage illicite de stupéfiants (Code pénal, art. 227-18) ; au transport, détention, offre ou cession de stupéfiants (227-18-1) ; à la consommation excessive ou habituelle d'alcool (art. 227-19) ; à commettre un crime ou un délit (art. 227-21). En matière sexuelle, sont également concernées diverses sollicitations ou incitations à caractère sexuel de la part d'un majeur (art. 227-22 al. 2, 227-22-1, 227-22-2, 227-23-1), la corruption de mineurs (art. 227-22) et la détention ou diffusion de contenus pédocriminels (art. 227-23). Il en est enfin ainsi de la provocation au suicide, si elle est suivie du suicide ou d'une tentative en ce sens (art. 223-13).

333 Code pénal, art. 131-35-1, II, 4° et 6°.

334 Code de l'éducation, art. L. 312-16 al. 1, devant être dispensées dans les écoles, collèges et lycées à raison d'au moins trois séances annuelles et par groupes d'âge homogène.

335 Code de l'éducation, art. L. 312-17-3.

336 Code de l'éducation, art. L. 312-17-1-1, devant être dispensée dans les établissements secondaires, par groupes d'âge homogène.

337 Code de l'éducation, art. L. 312-18, devant être dispensée dans les collèges et les lycées, à raison d'au moins une séance annuelle, par groupes d'âge homogène.

338 Code de la santé publique, art. L. 3511-2.

Enfin, la formation à l'utilisation responsable des outils et des ressources numériques doit contenir une sensibilisation à l'usage des dispositifs de signalement des contenus illicites et au bon usage des outils numériques et des réseaux sociaux ainsi qu'aux dérives et aux risques y afférents[339], tandis que l'enseignement moral et civique doit notamment former les élèves à acquérir un comportement responsable dans l'utilisation des outils interactifs, à maîtriser leur image publique et souligner les dangers de l'exposition de soi et d'autrui ainsi que les droits qu'ils tiennent du RGPD[340].

8.3. PRÉCONISATIONS

Préconisation 22 - Assurer l'effectivité des incriminations existantes.
L'enjeu de l'incitation des mineurs à des conduites à risques est déjà amplement saisi par le droit, par des mesures applicables de manière incidente aux contenus accessibles sur les réseaux sociaux. Le souci premier est dès lors de s'assurer de l'effectivité des infractions existantes, du point de vue tant théorique – au regard de leur formulation et portée – que pratique, en raison des problèmes d'identification des utilisateurs mineurs, des auteurs de l'infraction, du faible recours au signalement ou aux mécanismes de plainte et des lacunes dans la modération. Cela supposerait également de recenser le nombre de poursuites engagées au titre des dispositions précitées et leur taux de succès.

Préconisation 23 - Assurer l'effectivité des mesures éducatives.

Il importe de rendre effectives les mesures éducatives, lesquelles doivent être pensées de concert avec les enseignants concernés, en portant une attention particulière à la formation, aux moyens et au temps dont ils disposent réellement afin de sensibiliser les élèves. À cet égard, il convient de tenir le plus grand compte des propositions formulées notamment en matière d'éducation à la sexualité[341] et d'éducation au numérique[342].

Préconisation 24 - Mener une étude sur la dangerosité perçue des "challenges" en ligne et d'éventuelles mesures de sensibilisation à adopter.

---

[339] Code de l'éducation, art. L. 312-9, al. 1 et 3 respectivement.
[340] Code de l'éducation, art. L. 312-15 al. 7.
[341] V. not. A. Toullier, N. Gautier, Pour une véritable éducation à la sexualité. Les recommandations de la société civile aux pouvoirs publics, Livre Blanc, les recommandations de la société civile, 2023.
[342] V. not. C. Goetschy-Bolognese, H. Saulignac, Rapport d'information n° 1681 fait au nom de la délégation aux droits des enfants en conclusion des travaux d'une mission d'information sur éducation et numérique, 27 oct. 2023 ; v. plus généralement les travaux du Centre pour l'éducation aux médias et à l'information (CLEMI).

CHAPITRE 9 : MODIFICATION DE LA PERCEPTION DE SOI

9.1. PRATIQUES

Les pratiques saisies au titre de la modification de la perception de soi par le mineur se concentrent principalement sur l'exposition à deux types de contenus : d'une part, ceux qui véhiculent une image idéalisée du corps et, d'autre part, ceux qui présentent sous un jour favorable les troubles du comportement alimentaire, l'automutilation et le suicide, voire y incitent.

Concernant les contenus exprimant une image idéalisée du corps, ceux-ci peuvent porter sur le corps d'autrui ou le sien propre, par des retouches, l'utilisation de filtres mis à disposition sur les réseaux sociaux ou la promotion d'actes à visée esthétique.

Plusieurs études consacrées aux contenus relatifs aux troubles du comportement alimentaire sur les plateformes en ligne ont opéré un travail de recensement des pratiques. Un premier rapport commandité par l'autorité de régulation des médias irlandaise (Coimisiún na Meán) relatif aux plateformes de partage de vidéo a ainsi identifié les contenus dits "thinspiration" incitant à la maigreur (par exemple, des citations inspirantes) ; la comparaison entre pairs quant au corps, à l'image du corps, à la perte de poids et autres actes ; l'acceptation par les pairs pour trouver un sens de communauté ou d'appartenance ; la présentation des troubles du comportement alimentaire comme un choix de vie ; la pression par les pairs (comportement compétitif, fixation d'objectifs extrêmes, insultes ou critiques) ; les stratégies de soutien (pour dissimuler ses symptômes, réduire l'appétit ou maigrir) ; les conseils pratiques ; l'approbation de contenus dépeignant des personnes atteintes de ces troubles ; les récits de contre-culture[343]. Une enquête commissionnée par l'OFCOM évoque quant à elle des instructions pour restreindre les calories (régimes à très basses calories, jeûnes extrêmes et sport excessif) ; de manière moins récurrente que les restrictions d'alimentation, certains des jeunes interrogés ont également mentionné des contenus valorisant l'alimentation excessive[344]. Parmi les contenus valorisant des conduites alimentaires à risque, on peut en outre relever la récente tendance *#SkinnyTok*, faisant l'apologie de la maigreure extrême.

Les pratiques relatives à l'automutilation et au suicide peuvent également présenter une grande diversité. Le rapport effectué pour la Coimisiún na Meán énumère ainsi la désinformation relative à la santé mentale ; les communautés qui encouragent l'automutilation ; celles qui glorifient des personnes suicidées ; la diffusion en direct d'automutilation et suicide ; les contenus "éduquant" les utilisateurs à effectuer des actes d'automutilation ou un suicide ; les pactes de suicide entre

[343] PA Consulting, Video-Sharing Platform Services: Online Harms Evidence Review, provided to inform Coimisiún na Meán's approach to VSPS regulation, September 2023, p. 28.
[344] Ipsos UK, TONIC, Online Content: Qualitative Research – Experiences of children encountering online content relating to eating disorders, self-harm and suicide, March 2024, enquête commissionnée par l'OFCOM, p. 20.

membres d'une communauté en ligne ; le contenu visuel dépeignant l'automutilation ou le suicide généré par un système d'IA[345]. L'OFCOM y ajoute les images ou vidéos de cicatrices ou blessures ; les instructions pour s'automutiler efficacement, quels outils utiliser, et comment le dissimuler pour ne pas alerter ses proches ; la publication d'expériences personnelles ou des "*venting posts*" (traduits imparfaitement comme des contenus de défoulement) demandant à autrui des stratégies pour résister à une pulsion d'automutilation[346].

Enfin, l'association Samaritans au Royaume-Uni évoque des citations ou récits d'expérience d'automutilation ou de suicide ; leur représentation par des œuvres d'art ou "memes" ; des défis relatifs à ces actes ; des fils d'information ou de discussion sur des évènements récents, par exemple après un suicide médiatisé ou la diffusion d'une émission télévisée ou d'un film avec des thèmes similaires ; des pages commémoratives pour les personnes suicidées ; la présentation de l'automutilation et du suicide comme des moyens efficaces de mettre fin à une détresse et l'incitation d'autrui à ces comportements, ce qui est susceptible de détourner l'attention des ressources disponibles en matière de soutien psychologique[347].

Les études aboutissent également à des constats transversaux. L'étude commanditée par l'OFCOM sur les contenus en ligne relatifs aux troubles du comportement alimentaire, à l'automutilation et au suicide conclut notamment que les jeunes gens de l'échantillon étaient fortement familiers avec de tels contenus, généralement présentés sous la forme de contenus audiovisuels courts[348] (vidéos, images et chansons ; plus précisément des "*shorts, réels, slideshows et stories*"[349]). De plus, ces messages peuvent être intégrés à des contenus apparemment inoffensifs ou communiqués par des messages cachés ; l'enquête a également relevé que certaines tendances en ligne ou certains défis érigeaient un symbole apparemment anodin en signal pour indiquer le début d'un défi ou la manière dont quelqu'un devrait mettre fin à sa vie[350]. Les contenus relatifs à l'automutilation et au suicide tendent en outre, selon cette étude, à devenir plus extrêmes et plus fréquents de nuit[351].

L'étude de ces contenus et de leurs effets potentiels sur les utilisateurs, y compris mineurs, doit prendre en compte leur ambiguïté inhérente ainsi que leur sensibilité. En effet, certains d'entre eux relèvent d'un comportement préjudiciable (lorsqu'il s'agit d'exhorter autrui à l'une de ces pratiques par exemple), alors que beaucoup d'autres contenus peuvent poursuivre un but de sensibilisation, ou simplement rechercher du soutien entre pairs quant à des enjeux de santé mentale. Le partage d'expérience personnelle, y compris les "*recovery content*" qui consistent en un récit de guérison – mais dont l'appellation est parfois détournée à des fins préjudiciables – appartiennent ainsi à une zone grise. L'utilisateur qui souhaite s'intégrer à une communauté de

---

345 PA Consulting, Video-Sharing Platform Services : Online Harms Evidence Review, *op. cit.*, p. 35.
346 Ipsos UK, TONIC, Experiences of children encountering online content relating to eating disorders, self-harm and suicide, *op. cit.*, p. 23.
347 Samaritans, Understanding self-harm and suicide content online, 2020, pp. 1-2.
348 Ipsos UK, TONIC, Experiences of children encountering online content relating to eating disorders, self-harm and suicide, *op. cit.*, pp. 9-10.
349 Ipsos UK, TONIC, préc. p. 19.
350 Ipsos UK, TONIC, préc. p. 26.
351 Ipsos UK, TONIC, préc. p. 35.

personnes dans une situation semblable, partager son régime excessif ou ses convictions quant à la santé mentale peut n'avoir aucune intention malveillante ; pour autant, il peut alimenter une masse de contenus normalisant ces troubles et étant susceptibles de heurter (dans le cas d'images graphiques d'automutilation par exemple) ou d'influencer les tiers. L'équilibre est alors éminemment délicat entre la protection des personnes amenées à consulter un tel contenu, et le souci de préserver une voie d'expression des troubles de la santé mentale, qui sont parfois perçus comme ne pouvant être partagés autrement.

L'OFCOM insiste sur la nécessité de prendre en compte cette ambivalence et, pour les services en ligne, d'évaluer "*les risques de préjudice à l'utilisateur ayant partagé le contenu de même qu'aux autres utilisateurs*"[352], étant entendu que les utilisateurs pourraient rechercher, interagir avec ou publier des contenus relatifs à l'automutilation et au suicide pour diverses raisons. Celles-ci inclut comprendre leurs propres sentiments et expériences, pouvoir parler ouvertement sans peur du jugement, lire des récits ou se lier à d'autres avec des expériences similaires, trouver du soutien auprès de ses pairs ou d'une communauté en ligne, trouver du soutien pour eux-mêmes ou un proche, trouver des supports d'aide ou de soutien, sensibiliser à la prévention, et avoir accès à un soutien immédiat, ce qui est "*particulièrement important pour les utilisateurs en crise ou en attente de soutien de la part d'un professionnel de santé*"[353]. Certains contenus, tels que les messages incitant à demander de l'aide, des récits d'espoir, de soutien et de guérison, des conseils pour la santé mentale et de l'information sur les sources de soutien, peuvent ainsi s'avérer bénéfiques[354].

Il découle de l'ambiguïté inhérente à une partie de ces contenus une seconde spécificité relative aux groupes d'utilisateurs à risque. Parmi les jeunes interrogés dans le cadre de l'étude commandée par l'OFCOM, une distinction est apparue entre ceux qui avaient souffert de tels troubles – et qui avaient proactivement cherché ces contenus, voire qui en avaient généré ou partagé – et ceux qui n'en avaient pas souffert, et avaient été exposés aux contenus par accident, notamment par des recommandations personnalisées ou par un partage entre pairs[355]. Les utilisateurs souffrant – ou ayant souffert, et étant de nouveau confrontés à ces contenus – de tels troubles et ceux n'en

---

[352] OFCOM, Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm, Consultation, November 2023, pp. 82-83 : "*Services should be aware that suicide or self-harm content varies and is not always shared with malicious intent. Users who share suicide or self-harm content may be suffering from mental health problems themselves, and use online spaces to express their feelings and seek support by connecting with others who may be having similar experiences. Services should therefore be mindful of this distinction when assessing this type of content, considering the risks of harm to the user who shares the content as well as to other users*". V. aussi p. 80 : "*some users may share this content to find supportive communities or to reflect their own experiences as part of a healing process. It can include users who suffer with suicidal or self-harm ideation, as well as those who have recovered or are recovering from mental health challenges*". V. également la deuxième version de la consultation : OFCOM, Protecting children from harms online. Volume 3: The causes and impacts of online harms to children, Consultation, May 2024, pp. 50-102 et pp. 302-323.

[353] Samaritans, Understanding self-harm and suicide content online, préc., p. 1.

[354] Samaritans, préc., p. 3.

[355] Ipsos UK, TONIC, Experiences of children encountering online content relating to eating disorders, self-harm and suicide, *op. cit*., p. 10 et p. 31 et s.

souffrant pas, mais étant exposés aux contenus, constituent donc des groupes distincts à protéger[356].

Les effets produits peuvent être exacerbés par certaines fonctionnalités ou particularités propres aux réseaux sociaux. L'Académie des troubles du comportement alimentaire a ainsi pu appeler les entreprises mondiales de réseaux sociaux à prendre leurs responsabilités pour réduire les risques posés par leurs plateformes[357].

La fonctionnalité des réseaux sociaux présentée comme la plus dangereuse à cet égard sont leurs systèmes de recommandation, pouvant conduire les utilisateurs à une "*spirale*" de contenus préjudiciables, ou un "*trou de lapin*" ("*rabbit hole"*).

L'étude Deadly by Design du Center for Countering Digital Hate relève ainsi que les comptes d'adolescents fictifs, créés sur TikTok par les chercheurs, ont reçu des recommandations de contenus relatifs aux troubles du comportement alimentaire et à l'automutilation en quelques minutes seulement de consultation du fil d'actualités "Pour toi"[358]. Le rapport *Poussé·e·s vers les ténèbres* d'Amnesty International constate quant à lui, à la suite d'une enquête technique menée avec l'Algorithmic Transparency Institute (National Conference on Citizenship) et AI Forensics, que "*les enfants et les jeunes qui regardent des contenus relatifs à la santé mentale sur la page "Pour toi" de la plateforme peuvent facilement tomber dans des "spirales de contenus potentiellement préjudiciables, notamment des vidéos qui idéalisent et encouragent les pensées dépressives, l'automutilation et le suicide*"[359]. Le constat commun est que la plateforme cible ces jeunes vulnérables avec bien plus de contenus préjudiciables. Si ces deux rapports ont été consacrés exclusivement au réseau social TikTok, la plainte engagée par 33 États contre Meta évoque également ces enjeux[360].

---

[356] OFCOM, Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm, *op. cit.*, p. 84.

[357] Academy for Eating Disorders, Urgent Responsibility to Reduce Harms Posed by Social Media on risk for Eating Disorders: An Open Letter to Facebook, Instagram, TikTok, and Other Global Social Media Corporations, November 2021.

[358] Center for Countering Digital Hate, Deadly by Design. TikTok pushes harmful content promoting eating disorders and self-harm into users' feeds, 2022, p. 7 affirmant que les contenus relatifs au suicide étaient recommandés en 2,6 minutes, aux troubles du comportement alimentaire en 8 minutes, et qu'un nouveau compte TikTok créé comme par un utilisateur de 13 ans qui regarde et aime les contenus sur l'image corporelle et la santé mentale se voit recommander ces contenus toutes les 39 secondes.

[359] Amnesty International, Poussé·e·s vers les ténèbres. Comment le fil « pour toi » encourage l'automutilation et les idées suicidaires, 2023, p. 7.

[360] *The People of the State of California and others v. Meta Platforms, Inc.; Instagram, LLC; Meta Payments, Inc.; and Meta Platforms Technologies, LLC*, Complaint for Injunctive and other Relief in the United States District Court for the Northern District of California, Case 4:23-cv-05448-YGR, Doc. 73-2, 22 nov. 2023, pt. 176 et s.

La dangerosité de cette fonctionnalité présente un lien indissociable avec le modèle d'affaires de ces plateformes, centré sur les mécanismes d'engagement et d'interaction des utilisateurs. À cet égard, il paraît crucial de souligner que si les contenus extrêmes relatifs aux troubles du comportement alimentaire, à l'automutilation ou suicide, ou plus largement au mal-être peuvent attirer des retours malveillants, ils suscitent également une vive inquiétude poussant certains utilisateurs à commenter le contenu pour offrir du soutien, des encouragements positifs ou des références vers des associations spécialisées. Les jeunes gens interrogés dans le cadre de l'étude commandée par l'OFCOM abondent en ce sens, signalant également que le caractère extrême de ces contenus incite à les regarder[361]. Pour autant, cet engagement bienveillant est perçu par la plateforme pour un signe d'intérêt pour ce genre de contenus, menant à davantage de recommandations personnalisées similaires, alors que telle n'était pas l'intention de l'utilisateur.

L'étude commandée par la Coimisiún na Meán sur les plateformes de partage de vidéo argumente en outre que les plateformes visuelles sont plus nocives en termes d'image corporelle que les plateformes centrées sur des contenus textuels[362]. Les contenus visuels permettent en effet une comparaison accrue, une diffusion en direct de certains actes de même que la mise à disposition de filtres pour altérer l'apparence physique dans le sens d'un standard de beauté irréaliste ou nocif, voire d'outils de retouche ou de génération artificielle d'images. Sur la question des filtres, les effets potentiellement nocifs du filtre "bold glamour" de TikTok[363], par exemple, ainsi que du filtre de Meta simulant des modifications du visage obtenues par chirurgie esthétique ont pu être soulignés[364].

Enfin, plusieurs des études relèvent les failles des mécanismes de modération des contenus, d'autant que les utilisateurs sont prompts à utiliser des noms de code ou d'autres techniques pour échapper à la détection de certains mots-clés[365].

Si les études scientifiques peinent à établir un lien de causalité entre la seule exposition à des contenus en ligne relatifs au suicide ou à l'automutilation et une augmentation du risque de tels comportements, l'OFCOM souligne néanmoins l'hypothèse selon laquelle des contenus promouvant les troubles du comportement alimentaire seraient associés à une augmentation de ces troubles, d'autant qu'ils découragent les appels à l'aide ; une intervention précoce étant cruciale pour un traitement efficace, tout délai dans le traitement ou les demandes d'aide produisent des

[361] Ipsos UK, TONIC, Experiences of children encountering online content relating to eating disorders, self-harm and suicide, *op. cit*., p. 34.
[362] PA Consulting, Video-Sharing Platform Services : Online Harms Evidence Review, *op. cit*., p. 32.
[363] M. Vallet, C. Malhuret, Rapport n° 831 fait au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, 4 juill. 2023, pp. 125-126.
[364] V. not. la plainte déposée par 33 États contre Meta : Case 4:23-cv-05448-YGR, Doc. 73-2, 22 nov. 2023, préc. pt. 339 à 368 exposant les demandes internes à Meta pour un retrait de ce filtre et l'indifférence de la direction à cet égard.
[365] PA Consulting, Video-Sharing Platform Services : Online Harms Evidence Review, *op. cit*., p. 33 et 40 ; Ipsos UK, TONIC, Experiences of children encountering online content relating to eating disorders, self-harm and suicide, *op. cit*., pp. 51-52.

effets significatifs[366]. En outre, dans le cas tragique du suicide de la jeune Molly Russell, l'enquête du Coroner (équivalent du médecin légiste) a conclu qu'elle était décédée "*d'un acte d'automutilation tout en souffrant d'une dépression et des effets négatifs de contenus en ligne"*, ajoutant qu'il est *"probable que les contenus visionnés par Molly, souffrant déjà d'un trouble dépressif et vulnérable en raison de son âge, aient négativement affecté sa santé mentale et contribué à sa mort d'une manière plus que minimale*"[367].

Plusieurs études recensent comme effets potentiels des contenus relatifs aux troubles du comportement alimentaire une insatisfaction liée au corps ; une baisse de l'estime de soi ; un comportement de contrôle du poids ou de sport excessif ; le développement ou l'aggravation d'un trouble d'anorexie, boulimie, orthorexie, bigorexie[368]. Pour les contenus liés à l'automutilation et au suicide, il s'agit d'une baisse de l'estime de soi et de l'humeur ; d'une idéalisation accrue ou d'une fréquence accrue des actes d'automutilation ; d'un état de dépression ou d'anxiété voire du suicide[369]. L'étude commandée par l'OFCOM fait état d'impacts émotionnels négatifs après consultation du contenu (anxiété, honte, peur) et souligne que, tandis que certains jeunes interrogés ont dit avoir été attirés par ce contenu en ligne parce qu'ils souffraient déjà du trouble, d'autres pensent que ces contenus ont développé ou aggravé leurs symptômes (en découvrant par exemple des techniques inconnues d'automutilation)[370]. Beaucoup des jeunes qui avaient eux-mêmes créé du contenu ont décrit leur motivation comme étant l'attention et la validation reçue par des contenus similaires[371]. Il apparaît en outre que la haute fréquence d'exposition à ces contenus contribue à une désensibilisation de la gravité de ces troubles, et à leur banalisation[372].

Il convient de souligner que la modification de l'image de soi peut également constituer un effet collatéral de certaines pratiques envisagées précédemment par deux biais. En premier lieu, par la seule diffusion de son image : cela fait écho à l'enjeu du *sharenting*[373], auquel s'ajoute le cas spécifique des enfants influenceurs dès lors que la loi impose que les enfants et représentants légaux reçoivent une information quant aux risques, notamment psychologiques, résultant de cette diffusion[374]. En second lieu, elle peut résulter d'une distorsion de la perception de soi causée, entre

---

366 OFCOM, *Protecting people from illegal harms online. Volume 2 : The causes and impacts of online harm*, *op. cit.*, pp. 85-86, spéc. pt. 6D.19 et 6D.25.

367 The Coroner's Service, *Regulation 28 Report to prevent future deaths*, 13 October 2022.

368 PA Consulting, *Video-Sharing Platform Services : Online Harms Evidence Review*, *op. cit*., p. 28.

369 PA Consulting, *Video-Sharing Platform Services : Online Harms Evidence Review*, *op. cit*., p. 36.

370 Ipsos UK, TONIC, Experiences of children encountering online content relating to eating disorders, self-harm and suicide, *op. cit*., p. 11 et p. 41 et s.

371 Ibid.

372 Ibid.

373 Sur le sharenting, v. Chapitre 1.

374 En cas de diffusion de l'image d'un mineur de seize ans non employé comme influenceur sur un service de plateforme de partage de vidéos, la loi prévoit dans certaines circonstances une information de ses représentants légaux par les autorités compétentes, tenant notamment aux risques psychologiques associés à la diffusion de son image (Loi n° 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne, art. 3, I et art. 3, II, 2°), ainsi que l'obligation pour les plateformes de partage de

autres, par le fait d'être victime de l'une des pratiques à caractère sexuel étudiées[375] ou de cyberharcèlement.

9.2. CADRE JURIDIQUE

9.2.1. France et Union européenne

Afin de saisir les contenus représentant le corps de manière idéalisée ou favorisant les troubles du comportement alimentaire, l'automutilation voire le suicide, le droit a tout d'abord encadré la diffusion de l'image corporelle, puis certains types de contenus, d'une manière incidemment applicable aux contenus accessibles sur les réseaux sociaux. De nouvelles obligations sont en outre imposées aux fournisseurs de service.

Encadrement de l'image corporelle. En ce qui concerne l'image corporelle, différentes dispositions trouvent à s'appliquer. Tout d'abord, le droit français énonce une obligation de transparence sur le caractère retouché ou artificiel de certaines images. La retouche, en soi, n'est cependant pas interdite ; il s'agit d'une simple obligation d'information. Ainsi, la mention "photographie retouchée" est obligatoire pour les photographies à usage commercial de mannequins dont l'apparence corporelle a été modifiée par un logiciel de traitement d'image afin d'affiner ou d'épaissir la silhouette[376]. Prenant acte du fait que cette disposition ne paraît pas susceptible de saisir les retouches relatives par exemple aux traits du visage, à l'éclat ou à la couleur de la peau[377], la récente loi dite "influenceurs" impose la mention "images retouchées" si un influenceur communique une image ayant fait l'objet d'une retouche visant à affiner ou à épaissir la silhouette ou à modifier l'apparence du visage[378]. En outre, la mention "images virtuelles" doit apparaître si un influenceur communique une image ayant fait l'objet d'une production par tous procédés d'intelligence artificielle visant à représenter un visage ou une silhouette[379].

Ensuite, l'exercice de l'activité de mannequinat est subordonné à la délivrance d'un certificat médical ; celui-ci doit attester que l'évaluation globale de l'état de santé du mannequin, notamment

vidéos d'adopter une charte sensibilisant à ces mêmes risques et informant le mineur des moyens de protection (Ibid., art. 4, 1° à 4, 3°).

[375] V. Chapitres 4, 5 et 6 pour les développements consacrés au grooming, à l'abus de contenus intimes et aux deepfakes à caractère sexuel.

[376] Code de la santé publique, art. L. 2133-2 al. 1.

[377] En ce sens, v. P. Morvan, « Santé publique – Le droit pénal face à l'anorexie mentale (Loi n° 2016-41 du 26 janvier 2016) », *Droit pénal* n° 3, mars 2016, étude 6.

[378] Loi du 9 juin 2023 préc., art. 5, II, 1°.

[379] Loi du 9 juin 2023 préc., art. 5, II, 2°.

au regard de son indice de masse corporelle, est compatible avec l'exercice de son métier[380]. Certaines critiques ont néanmoins pu souligner que "*la loi ne vise pas tant à protéger les mannequins exposés aux pressions de leurs employeurs ou de leur entourage professionnel qui les pressent de maigrir* » que "*de faire disparaître des médias les images de mannequins squelettiques*"[381]. Elle fait ainsi reposer sur les mannequins la charge d'internaliser deux injonctions contradictoires, d'une part l'exigence d'un certain indice de masse corporel (qui n'est pas toujours reflété par l'apparence physique) et d'autre part l'exigence de maigreur souvent inhérente à ce métier.

Enfin, la promotion directe ou indirecte par des influenceurs d'actes ou interventions à visée esthétique est interdite[382]. En outre, l'autorisation administrative donnée à un établissement dédié aux interventions de chirurgie esthétique peut être retirée en cas de communication commerciale, directe ou indirecte, déloyale, portant atteinte à la santé publique ou qui, par son caractère, sa présentation ou son objet, est susceptible d'inciter les mineurs à recourir aux prestations offertes par l'établissement, y compris en ligne[383].

Illicéité de certains contenus relatifs au suicide. Parmi les contenus envisagés, seuls certains propos relatifs au suicide sont incriminés en droit français. Il convient en outre de rappeler que le suicide en lui-même ne constitue pas une infraction. Ainsi, il existe un délit de provocation au suicide, si celle-ci est suivie du suicide ou d'une tentative en ce sens[384], et un délit de propagande ou publicité en faveur de produits, d'objets ou de méthodes préconisés comme moyens de se donner la mort[385].

Par ailleurs, en application de l'article 6 du DSA, le fournisseur de réseau social est tenu de supprimer promptement ces contenus lorsqu'ils lui sont notifiés dans les conditions prévues par le texte. C'est en revanche seulement au regard du délit de provocation au suicide qu'un signalement doit être effectué auprès des autorités compétentes en vertu de l'article 6, IV, 4 LCEN, et qu'une peine de bannissement peut être prononcée en application de l'article 131-35-1, II, 6° du Code pénal.

Il convient en outre de souligner que, en France, plusieurs actions en justice ont été initiées afin de voir reconnaître la responsabilité des plateformes de réseaux sociaux au titre des préjudices

[380] Code du travail, art. L. 7123-2-1 al. 1. La sanction est néanmoins encourue par « toute personne exploitant une agence de mannequins ou s'assurant, moyennant rémunération, le concours d'un mannequin » : art. L. 7123-27.

[381] P. Morvan, « Santé publique – Le droit pénal face à l'anorexie mentale (Loi n° 2016-41 du 26 janvier 2016) », art. préc.

[382] Loi du 9 juin 2023 préc., art. 4, I., renvoyant à la définition de ces actes et interventions contenue aux articles L. 1151-2 et L. 6322-1 du Code de la santé publique respectivement.

[383] Code de la santé publique, art. L. 6322-1 al. 4 ajouté par la loi n° 2023-171 du 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du travail, des transports et de l'agriculture, art. 23.

[384] Code pénal., art. 223-13.

[385] Code pénal., art. 223-14.

causés aux mineurs utilisateurs. Une première plainte a été déposée en septembre 2023 par la famille d'une jeune fille ayant mis fin à ses jours après avoir utilisé le service de TikTok[386]. En novembre 2024, à la suite de cette première action, des familles de victimes se sont réunies afin d'assigner ce même réseau social en justice en dénonçant la dégradation de l'état de santé physique et mentale de leurs enfants. En mars 2025, quatre nouvelles familles se sont ajoutées à cette plainte. Ces procédures sont en partie portées par le collectif "Algos Victima"[387] ayant pour ambition de responsabiliser les plateformes de réseau sociaux sur les sujets de conception et systèmes des applications, d'informations insuffisantes sur les risques systémiques ainsi que sur la défaillance dans la modération au regard des impacts importants pouvant en résulter sur la santé mentale et physique des mineurs, en particulier du fait de l'incitation à l'automutilation, à l'anorexie et au suicide.

Par ailleurs, le parquet de Paris a annoncé le 4 novembre 2025[388], avoir ouvert une enquête préliminaire le 11 septembre 2025 découlant d'un signalement du député Arthur Delaporte relatif aux dysfonctionnements constatés par la commission d'enquête parlementaire sur les effets psychologiques de TikTok[389].

Licéité des contenus relatifs aux troubles du comportement alimentaire et à l'automutilation : Le droit français n'incrimine pas expressément les propos promouvant ou incitant aux troubles du comportement alimentaire ou à l'automutilation. Une telle hypothèse a pourtant été envisagée par le passé : en effet, une proposition de loi visant à lutter contre les incitations à la recherche d'une maigreur extrême ou à l'anorexie avait été adoptée par l'Assemblée nationale en première lecture le 15 avril 2008[390]. Le texte consacrait deux nouveaux délits en son article unique : d'une part, il incriminait "*le fait de provoquer une personne à rechercher une maigreur excessive en encourageant des restrictions alimentaires prolongées ayant pour effet de l'exposer à un danger de mort ou de compromettre directement sa santé*"[391]. D'autre part, il prohibait "la *propagande ou la publicité, quel qu'en soit le mode, en faveur de produits, d'objets ou de méthodes préconisés comme moyens de parvenir à une maigreur excessive ayant pour effet de compromettre directement la santé*"[392]. Ainsi, le modèle de la provocation au suicide était clairement suivi ; la formulation de "maigreur excessive" permettait en outre d'exclure les jeûnes religieux, régimes, soins et grèves de la faim[393].
Cependant, un amendement déposé au Sénat au nom de la commission des affaires sociales a procédé à une réécriture complète de la proposition de loi, qui n'a jamais été débattue par la suite. La rédaction initiale était supprimée au profit de l'article unique suivant : "*l'apologie de troubles*

386 Sur ce point v. Chapitre 11 sur la conception des services.
387 Boutron-Marmion Associés, Algos Victima.
388 Parquet de Paris Tribunal judiciaire, Communiqué de presse, 4 novembre 2025.
389 Sur ce point v. Chapitre 11 sur la conception des services.
390 Proposition de loi visant à lutter contre les incitations à la recherche d'une maigreur extrême ou à l'anorexie, adoptée en 1ère lecture par l'Assemblée nationale le 15 avril 2008, TA n° 132.
391 Introduction proposée d'un article 223-14-1 du Code pénal
392 Introduction proposée d'un article 223-14-2 du Code pénal.
393 W. Roumier, « Mise en danger d'autrui – Création d'un délit de provocation à la maigreur excessive – Veille », *Droit pénal* n° 5, Mai 2008, alerte 26.

du comportement alimentaire, de l'automutilation ou de comportements mettant gravement et directement en danger la santé des personnes, faite auprès du public par tout moyen, est interdite"[394]. Le choix était assumé de ne pas l'assortir de sanctions pénales, de ne pas restreindre l'infraction à la seule anorexie et de supprimer le délit d'incitation à la maigreur excessive en raison de la crainte d'un contentieux impliquant des auteurs et autrices de contenus "pro-ana" jeunes et eux-mêmes malades[395].

Il semble toutefois envisageable de saisir certains de ces propos par l'infraction d'abus de faiblesse, constituée notamment en cas d'abus frauduleux de l'état d'ignorance ou de la situation de faiblesse d'un mineur pour le conduire à un acte ou à une abstention qui lui sont gravement préjudiciables[396]. Ce délit requiert néanmoins la connaissance par l'auteur de l'état d'ignorance ou de faiblesse de la victime ainsi que la volonté de l'exploiter "pour" la conduire à un acte ou à une abstention dont il sait le caractère gravement préjudiciable[397]. Il faudrait en outre que les troubles du comportement alimentaire ou l'automutilation atteignent un certain seuil pour être qualifiés de "gravement préjudiciables"[398].

Obligations des fournisseurs de services : Les plateformes sont tenues d'une obligation de modération pour les contenus illicites comme mentionné précédemment. Toutefois, on relève parfois une difficulté à définir les contenus préjudiciables d'autant que ceux-ci ne sont pas nécessairement qualifiés de contenus illicites. A cet égard, les lignes directrices de l'article 28 du DSA soulignent l'importance pour les fournisseurs de service de préciser cette définition dans leurs conditions générales d'utilisation et/ou les règles de la communauté pour permettre aux utilisateurs de comprendre dans quelle mesure ce type de contenus peut faire l'objet d'une modération de la part de la plateforme[399]. Cela est d'autant plus important que les plateformes sont tenues de respecter leurs CGU. Si ces contenus ne sont pas modérés, l'utilisateur pourra dès lors

---

[394] Sénat, Proposition de loi « anorexie », Première lecture du 4 juill. 2008, Article unique. V. également P. Schillinger, Rapport n° 439 fait au nom de la commission des Affaires sociales du Sénat sur la proposition de loi, adoptée par l'Assemblée nationale, visant à lutter contre les incitations à la recherche d'une maigreur extrême ou à l'anorexie, 2 juill. 2008.

[395] P. Schillinger, rapport préc. p. 32 : « votre rapporteure doute fortement que le fait de traduire un jeune anorexique en justice pour lui imposer une amende ou une peine de prison fasse beaucoup pour réduire la prévalence de la maladie ». V. aussi W. Roumier, « Mise en danger d'autrui – Lutte contre l'anorexie : la commission des affaires sociales préfère prévenir que pénaliser – Veille », *Droit pénal*, Septembre 2008, alerte 48.

[396] Code pénal, art. 223-15-2, al. 1. Sur cette infraction, v. not. P. Conte, *Droit pénal spécial*, LexisNexis, 6e ed., 2019, pp. 200-204, spéc. n° 281 à 284 ; M.-L. Rassat, *Droit pénal spécial. Infractions du Code pénal*, Dalloz, coll. « Précis », 8e ed., 2018, p. 362-366, spéc. n° 306.

[397] P. Conte, *Droit pénal spécial*, *op. cit.* p. 204, n° 283.

[398] Sur ce point, v. not. Cour d'appel Paris, 10e ch. correctionnelle, section B, 20 nov. 2008, *JurisData* n° 2008-004975, qualifiant d'actes gravement préjudiciables le fait pour de jeunes mineures fragiles psychologiquement, en l'espèce, de se laisser photographier et filmer nues pour diffusion en ligne, s'endetter lourdement, s'éloigner de leurs milieux familiaux, arrêter leurs études ou encore se priver de sommeil ou d'alimentation.

[399] Sur ce point, v. Chapitre "Conception des services", pt. 11.2.1.2.4.

agir pour non-respect de cet engagement, notamment au titre des pratiques commerciales déloyales (en cas de non-respect d'un engagement annoncé). Il paraît en outre souhaitable que les plateformes éclairent cette définition d'exemples précis pour faciliter l'action des utilisateurs, éventuellement en associant à ce travail de cartographie les associations de victimes et autres ONG pour assurer un meilleur suivi de l'évolution des usages. Un autre enjeu consiste à limiter l'amplification de tels contenus compte tenu des risques pouvant en résulter en particulier pour la santé mentale et physique du mineur ; en ce sens, les plateformes doivent "mettre en œuvre des mesures visant à prévenir l'exposition des mineurs aux recommandations de contenus susceptibles de présenter un risque pour leur sureté et leur sécurité, en particulier lorsqu'elles leur sont présentées de manière répétée, tels que des contenus promouvant des normes de beauté ou des régimes irréalistes, des contenus qui glorifient ou banalisent des problèmes de santé mentale, tels que l'anxiété et la dépression" [400]. Enfin, pour limiter les risques en lien à la modification de l'image de soi, les lignes directrices de l'article 28 du DSA relèvent la nécessité pour les plateformes accessibles aux mineurs de désactiver les filtres susceptibles d'être associés à des effets négatifs sur l'image du corps, l'estime de soi et la santé mentale[401].

En outre, les très grandes plateformes en ligne ont l'obligation d'effectuer un recensement, une analyse et une évaluation de "*tout risque systémique au sein de l'Union découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services"*[402]. Cette analyse doit notamment inclure quatre catégories de risques ; la deuxième recouvre tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux, en particulier relatifs aux droits de l'enfant[403]. Le considérant correspondant précise qu'il convient à cet égard d'examiner "*la manière dont ces derniers peuvent être exposés, par le biais de leur service, à des contenus pouvant nuire à leur santé ainsi qu'à leur épanouissement physique, mental et moral*"[404]. La quatrième catégorie comprend tout effet négatif réel ou prévisible lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes[405]. Les fournisseurs de très grandes plateformes en ligne doivent alors prendre en compte, entre autres, l'influence de la conception de leurs systèmes de recommandation et de tout autre système algorithmique pertinent, leurs systèmes de modération des contenus, les conditions générales applicables et leur mise en application, ainsi que les pratiques en matière de données[406]. Cela devrait comprendre les "*informations qui ne sont pas illicites mais alimentent les risques systémiques recensés dans le présent règlement*", de même que l'amplification algorithmique des

[400] Commission européenne, COMMUNICATION DE LA COMMISSION, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, p. 22, pt. 65, h.

[401] Commission européenne, Lignes directrices article 28 du DSA préc, p. 17, pt. 57, b. xi.

[402] DSA, art. 34.1. Sur les analyses des risques, v. Chapitre 2 pt. 2.1.2.4.

[403] DSA, art. 34.1.b.

[404] DSA, cons. 81.

[405] DSA, art. 34.1.d.

[406] DSA, art. 34.2.

informations[407]. Les fournisseurs doivent ensuite mettre en place des "*mesures d'atténuation raisonnables, proportionnées et efficaces, adaptées* […]*, en tenant compte en particulier de l'incidence de ces mesures sur les droits fondamentaux*", ce qui inclut l'adaptation des caractéristiques et fonctionnement de leurs services, y compris leurs systèmes de recommandation[408]. Ils devraient alors "*tenir compte de l'intérêt supérieur des mineurs"* dans le choix de ces mesures, et veiller à les protéger *"contre les contenus susceptibles de nuire à leur épanouissement physique, mental ou moral et fournir des outils permettant un accès conditionnel à ces informations*"[409].

Il convient de mentionner une proposition de loi visant à étendre le champ du délit d'abus de faiblesse aux pratiques des plateformes numériques, déposée le 16 septembre 2025. Son titre et son contenu semblent néanmoins révéler une confusion, dès lors qu'il s'agit en réalité d'étendre le délit de manipulation mentale préjudiciable[410], et non celui d'abus de faiblesse qui en est désormais dissocié[411]. L'article 223-15-3 actuel du Code pénal prohibe en effet « le fait de placer ou de maintenir une personne dans un *état de sujétion psychologique* ou physique résultant de l'exercice de pressions graves ou réitérées ou de *techniques propres à altérer son jugement* et ayant *pour effet de causer une altération grave de sa santé physique ou mentale"* ou de conduire cette personne à un acte ou à une abstention qui lui sont gravement préjudiciables (nous soulignons). Initialement pensée pour contrer les dérives sectaires, la disposition se verrait étendue à la sujétion psychologique résultant des pratiques d'une plateforme, "*notamment lorsque les mécanismes algorithmiques de recommandation […] ont pour effet de maintenir un mineur ou une personne vulnérable dans un état de dépendance psychique ou émotionnelle manifeste, ou de favoriser la diffusion de contenus portant atteinte à son intégrité*"[412]. Au-delà de l'opportunité discutable d'une réponse pénale, il n'est pas certain que l'ajout projeté soit conforme au droit de l'Union. Le principe du pays d'origine prohibe en particulier d'imposer des mesures générales et abstraites aux services numériques provenant d'autres États membres pour ce qui relève du domaine coordonné[413], ce qui ne paraît pas exclure par principe le droit pénal[414]. La contrariété au droit de l'Union est très probable également pour l'article 2 de la proposition de loi[415].

---

[407] DSA, cons. 84 ; cette incise paraît toutefois se référer principalement à la désinformation.

[408] DSA, art. 35.1.

[409] DSA, cons. 89.

[410] C. pén., art. 223-15-3 ; v. G.-X. Bourin, *Contribution à l'étude du délit de manipulation mentale préjudiciable*, préf. C. Lazerges, PUAM, 2005.

[411] C. pén., art. 223-15-2.

[412] Proposition de loi visant à étendre le champ du délit d'abus de faiblesse aux pratiques des plateformes numériques, 16 sept. 2025, art. 1.

[413] Dir. 2000/31, art. 3.

[414] V. en ce sens Conclusions de l'Avocat général Szpunar, aff. jointes C-188/24 et C-190/24, *WebGroup Czech Republic* et *Coyote System*, 18 sept. 2025, n° 95.

[415] Celui-ci impose aux plateformes « accessibles aux mineurs ou aux personnes vulnérables », au sein du Code pénal, une transparence des algorithmes de recommandation, la modération des messageries privées, la restriction de la géolocalisation des mineurs, une protection contre les mécanismes addictifs et des pauses d'utilisation, la traçabilité des contenus attentatoires à l'intégrité et la vérification de l'âge.

9.2.2. Angleterre et Pays de Galles

L'Online Safety Act adopté au Royaume-Uni en 2023 impose aux services d'utilisateur à utilisateur auxquels les mineurs sont susceptibles d'accéder de mener une "*analyse des risques envers les enfants*", en estimant le niveau de risque que les utilisateurs mineurs du service soient confrontés à : chaque type de contenu de première priorité préjudiciable aux enfants (chacun étant évalué séparément), chaque type de contenu de simple priorité préjudiciable aux enfants (chacun étant évalué séparément), et enfin des contenus non recensés qui seraient préjudiciables aux enfants, en distinguant les groupes d'âge et en prenant en compte les algorithmes utilisés par le service[416].

Or, le texte qualifie de "*contenu de première priorité préjudiciable aux enfants*" les contenus qui encouragent, promeuvent ou fournissent des instructions pour : le suicide[417], un acte d'automutilation délibérée[418], un trouble du comportement alimentaire ou des comportements associés[419]. Il semblerait cependant que cela ne concerne que les contenus qui comportent au moins un texte, à l'exclusion des seules images ou contenus audio ou vidéo[420]. Les contenus encourageant au suicide, à l'automutilation volontaire et à un trouble du comportement alimentaire par une image ou un contenu audio ou vidéo dépourvus de texte seraient alors saisis parmi les contenus non recensés qui seraient préjudiciables aux enfants. Les fournisseurs de services doivent ensuite adopter des mesures d'atténuation[421], notamment afin d'empêcher les enfants de tout âge d'être confrontés aux contenus de première priorité et de protéger les enfants par groupe d'âge contre les autres contenus[422]. Il consacre en outre une nouvelle incrimination, relative à l'encouragement ou à l'assistance à l'automutilation. Celle-ci est constituée lorsque l'auteur commet un acte susceptible d'encourager ou d'assister l'automutilation d'autrui, dans cette intention[423] ; l'acte en question peut être constitué même s'il vise un public indéterminé[424]. L'automutilation envisagée consiste en une blessure sérieuse ("*grievous bodily harm*", et non le seuil inférieur de "*actual bodily harm*"), y compris les actes successifs d'automutilation qui atteignent cumulativement ce seuil[425] ; le délit est cependant constitué même s'il n'est pas suivi d'effet, c'est-à-dire indépendamment de l'automutilation avérée d'autrui[426]. Dans la mesure où un contenu encourageant ou assistant l'automutilation d'autrui constitue une infraction, il est alors compris

[416] Online Safety Act, s.11(6)(b).
[417] Online Safety Act, s.61(3).
[418] Online Safety Act, s.61(4).
[419] Online Safety Act, s.61(5).
[420] Online Safety Act, s.61(6).
[421] Online Safety Act, s.12.
[422] Online Safety Act, s.12(3).
[423] Online Safety Act, s.184(1).
[424] Online Safety Act, s.184(4) ; v. aussi s.184(2), (6) à (9), (11) et (13) pour l'acception extensive de l'acte incriminé.
[425] Online Safety Act, s.184(3).
[426] Online Safety Act, s.184(5).

dans l'obligation d'effectuer une analyse de risques des contenus illicites, à la charge de toutes les plateformes d'utilisateur à utilisateur[427].

Enfin, afin d'autonomiser les utilisateurs adultes ("*adult user empowerment"),* certains services (ceux dits de "Catégorie 1") doivent inclure dans le service, de manière proportionnée, des fonctionnalités permettant aux utilisateurs adultes d'accroître leur contrôle sur certains types de contenus[428] . Ces fonctionnalités consistent à réduire la probabilité que l'utilisateur soit confronté à ces contenus ou à l'alerter quant à la présence de ces contenus sur le service[429], ou à filtrer les contenus provenant d'utilisateurs non vérifiés[430]. Parmi ces contenus figurent ceux qui encouragent, promeuvent ou fournissent des instructions pour un suicide, une automutilation délibérée, un trouble du comportement alimentaire ou des comportements associés[431].

9.2.3. États-Unis

Le projet de Kids Online Safety Act, dans sa version déposée au Sénat des États-Unis le 13 décembre 2023, impose un devoir de diligence (duty of care) : une plateforme concernée doit prendre des mesures raisonnables dans la conception et le fonctionnement d'un produit, service ou fonctionnalité qu'elle sait être utilisé par des mineurs pour prévenir et atténuer certains préjudices aux mineurs y compris, "*de manière cohérente avec des informations médicales empiriques, les troubles de la santé mentale suivants : anxiété, dépression, troubles du comportement alimentaire, troubles dans la consommation de substances, comportements suicidaires"*[432].

9.3. PRÉCONISATIONS

Préconisation 25 - Renforcer la sensibilisation aux troubles de la santé mentale à tous les niveaux de la société.
L'exposition des mineurs à de tels contenus ou à ces troubles, même de manière indirecte, paraissant inévitable, il paraît pertinent de les sensibiliser en amont à ces enjeux selon une terminologie adaptée à l'âge afin de favoriser leur compréhension et réflexion, promouvoir la sécurité, briser le tabou entourant ces enjeux et leur fournir des outils ainsi que des interlocuteurs pour s'exprimer sur leurs éventuelles difficultés en termes de santé mentale.
L'enjeu spécifique des troubles du comportement alimentaire pourrait être intégré à l'information et éducation des élèves à l'alimentation et à la lutte contre le gaspillage alimentaire déjà prévue par le Code de l'éducation.

---

[427] Online Safety Act, s.9.
[428] Online Safety Act, s.15.2.
[429] Online Safety Act, s.15.3.
[430] Online Safety Act, s.15.9 et 10.
[431] Online Safety Act, s.16.3.
[432] S.1748 - Kids Online Safety Act,, s. 3(a)(1).

Préconisation 26 - Étendre la mention obligatoire « image retouchée » à toute modification de l'apparence physique et à toute publication pour usage commercial.
Cette mention aurait vocation à s'appliquer également pour les modifications de la silhouette, du visage, de la peau ou de tout autre élément corporel ; elle ne s'imposerait pas seulement aux influenceurs ou aux mannequins mais à tout usage commercial.

Préconisation 27 - Obtenir l'accès aux données pertinentes, après consultation de chercheurs pour identifier précisément quelles seraient les données requises, pour étudier l'impact sanitaire de certains filtres et des métriques de réputation apparentes sur les réseaux sociaux. Sur cette base, s'interroger sur l'opportunité d'interdire certaines de ces pratiques.

Préconisation 28 - Dans le cadre de la faculté de paramétrage proposée, permettre aux utilisateurs d'exercer un contrôle sur la présentation, le choix et l'ordonnancement des contenus auxquels ils sont exposés, par exemple : pouvoir exprimer son désintérêt pour un type du contenu afin qu'il ne soit plus recommandé, réinitialiser les recommandations effectuées, exclure les contenus comprenant certains mots-clés ou publiés par certains autres utilisateurs, etc.
Sanctionner toute fonctionnalité donnant une illusion de choix (les boutons plus/moins de contenus non suivis d'effet quant à leur exposition) au titre des interfaces trompeuses et manipulatrices (article 25 DSA).
Source : Panoptykon - People v. Big Tech, *Safe by default*

Préconisation 29 - Analyser l'opportunité d'incriminer l'incitation à l'anorexie et l'automutilation. Au regard de l'ambiguïté des propos, de la vulnérabilité particulière de certains de leurs auteurs, des réserves exprimées par le législateur en 2008 et d'une étude globale de l'effectivité des autres incriminations (celles, par exemple, recensées dans le cadre de l'incitation à des conduites à risque), reprendre la réflexion quant aux mesures juridiques appropriées de lutte contre les contenus incitant à l'anorexie et l'automutilation.

Préconisation 30 - Analyser l'opportunité d'instaurer un nombre maximal quotidien de recommandations personnalisées ainsi qu'une liste régulièrement mise à jour de termes liés à du contenu potentiellement problématique en matière de santé mentale, termes considérés comme acceptables en tant que mots-clés de recherche mais pas à des fins d'amplification dans le fil d'actualité afin de prévenir l'amplification de tels contenus.
Source : Amnesty International, Poussé.e. vers les ténèbres

CHAPITRE 10 : MINEURS APPARTENANT À DES GROUPES PROTÉGÉS

10.1. CARACTÉRISTIQUES

Toutes les pratiques précédemment considérées ayant cours sur les réseaux sociaux, ainsi que leurs impacts et mécanismes transversaux, peuvent produire un effet différent selon le profil du mineur. À cet égard, une réglementation optimale des réseaux sociaux nécessite de prendre en compte les potentielles caractéristiques des utilisateurs, y compris au prisme de l'intersectionnalité – c'est-à-dire en envisageant l'impact combiné de l'appartenance à plusieurs groupes ou communautés. Ce constat vaut également pour les utilisateurs majeurs.

Ainsi, si l'utilisation des réseaux sociaux produit des effets communs pour tous, les mineurs présentant certaines caractéristiques sont susceptibles d'être affectés de manière disproportionnée. Plusieurs effets ou risques sont ensuite spécifiques à certaines caractéristiques.

10.1.1. Genre

Il a pu être démontré que les femmes sont plus susceptibles, à un degré disproportionné, d'être victimes d'abus en ligne, en particulier concernant leurs images ; 70% des victimes d'abus d'images intimes aidées par l'eSafety Commissioner sont ainsi des femmes, en exceptant les cas de sextorsion[433]. Une attention particulière est à porter au développement des techniques d'hypertrucage (deepfake), spécifiquement à caractère sexuel[434]. En outre, si les hommes et les femmes sont victimes de haine en ligne à des niveaux comparables, ces dernières sont plus souvent ciblées en raison de leur genre ou apparence physique[435]. Certaines études font état de taux alarmant de cyberharcèlement[436].
Il semble également plus fréquent que les filles soient exposées à des contenus relatifs aux troubles du comportement alimentaires que les garçons[437].

[433] eSafety Commissioner, Protecting voices at risk online, 2020, p. 9.
[434] Sur les risques spécifiques soulevés par l'intelligence artificielle générative, v. UNESCO, « Ton avis ne compte pas, de toute façon ». Dénoncer la violence de genre facilitée par la technologie à l'ère de l'intelligence artificielle générative, 2023 - Sur la technologie deepfake, v. également la présente étude, Chapitre 6.
[435] Ibid.
[436] Plan International, Libres d'être en ligne ? Les expériences des filles et des jeunes femmes en matière de harcèlement en ligne, 2020, pp. 11-12 et 17.
[437] PA Consulting, Video-Sharing Platform Services: Online Harms Evidence Review, provided to inform Coimisiún na Meán's approach to VSPS regulation, September 2023, p. 29.

Il apparaît à l'inverse que les garçons sont plus susceptibles d'être victimes de coercition sexuelle à des fins financières (dont sextorsion)[438]. Les garçons et les filles semblent donc présenter des vulnérabilités différentes, et sont affectés de manière disproportionnée par des pratiques distinctes. Ce constat est également partagé par le rapport "*Technology on her terms*" de l'UNESCO[439]. En particulier, certaines études révèlent que ces premiers ont moins connaissance des risques en ligne, et que les stéréotypes de genre associés à la masculinité peuvent faire obstacle au fait de se confier ou de chercher de l'aide[440].

L'Online Safety Act 2023 au Royaume-Uni impose à l'OFCOM de produire des lignes directrices sur la protection des femmes et des filles sur les services d'utilisateur à utilisateur. Celles-ci concernent plus précisément les contenus et activités entraînant des devoirs pour les fournisseurs de service, et affectant de manière disproportionnée les femmes et les filles[441]. Avant de publier ces lignes directrices, y compris une version révisée ou de remplacement, l'OFCOM doit consulter le Commissaire pour les victimes et témoins, le Commissaire à la violence conjugale et familiale[442].

Une première version, ouverte à consultation, propose les neuf actions suivantes :

"Prendre ses responsabilités
1. S'assurer que les processus de gouvernance et de responsabilisation (accountability) traitent des dommages en ligne fondés sur le genre, par exemple en consultant des experts du sujet et en établissant des politiques qui les interdisent.
2. Mener des analyses de risques centrées sur les dommages aux femmes et aux filles, par exemple en échangeant avec des survivantes et victimes et en dirigeant des sondages auprès des utilisateurs et utilisatrices.
3. Être transparent au sujet de la sécurité en ligne des femmes et des filles, par exemple en partageant des informations sur la fréquence des dommages sur le service et l'effectivité des mesures de sécurité.

Prévenir les dommages
4. Mener des évaluations du potentiel d'abus et des tests produit, par exemple en utilisant le red teaming pour identifier comment des acteurs mal intentionnés pourraient utiliser les fonctionnalités du service pour causer des dommages.
5. Définir des paramètres par défaut plus sûrs, par exemple en regroupant les paramètres par défaut pour faciliter la sécurisation de leur compte par des femmes victimes d'abus multiples (« pile-ons »).

[438] WeProtect Global Alliance, PA Consulting, Évaluation mondiale de la menace 2023 : Évaluer l'ampleur et la portée de l'exploitation et des abus sexuels en ligne envers les enfants, pour transformer la riposte, Recherche menée en partenariat avec Crisp, 2023, p. 5.
[439] UNESCO, Rapport mondial de suivi de l'éducation : Rapport sur l'égalité des genres – La technologie à ses conditions : égalité des genres et inclusion, 2024, spéc. p. 36&s.
[440] Ibid., p. 5.
[441] Online Safety Act, s.54.1.
[442] Online Safety Act, s.54.3.

6. Réduire la circulation des dommages sexistes en ligne, par exemple en utilisant la correspondance de valeurs de hachage (« hash matching ») pour détecter et supprimer les images intimes partagées sans consentement.

Soutenir les femmes et les filles
7. Donner aux utilisatrices un meilleur contrôle sur leurs expériences, par exemple en leur offrant la possibilité de bloquer plusieurs comptes à la fois.
8. Permettre aux utilisatrices qui subissent des dommages sexistes en ligne de les signaler, par exemple en concevant des systèmes de signalement accessibles et au soutien des victimes de violences conjugales.
9. Prendre des mesures appropriées en cas de dommages sexistes en ligne, par exemple en sanctionnant les utilisateurs qui enfreignent à plusieurs reprises les politiques du service"[443].

10.1.2. Communauté LGBTQ+

Il est unanimement souligné que les réseaux sociaux ont des impacts positifs sur la communauté LGBTQ+[444], en leur permettant de découvrir et de vivre pleinement leur orientation sexuelle ou leur identité de genre, et de trouver une forme de communauté parfois inaccessible hors ligne en raison de la stigmatisation qui y est attachée. Il s'agit d'une « source vitale d'information, de soutien et de relation »[445].

La première conclusion clé d'un rapport effectué par l'organisation Thorn est ainsi que les adolescents LGBTQ+ ont rapporté une plus grande dépendance (au sens de "*reliance*", et non addiction) aux communautés et espaces en ligne[446] ; ils se reposent, de manière très distinctive, sur l'anonymat et le secret perçus en ligne afin de se découvrir et nouer des liens avec la communauté[447]. Ces conclusions ont été confirmées par une étude menée par l'eSafety Commissioner auprès d'adolescents LGBTIQ+ australiens, révélant qu'ils étaient plus susceptibles que la moyenne nationale de se sentir plus à l'aise en ligne qu'en personne[448]. Par conséquent, le fait d'être en ligne leur offre la possibilité d'explorer ce à quoi pourraient ressembler des

[443] OFCOM, A safer life online for women and girls. Practical guidance for tech companies, Consultation, 25 fév. 2025, p. 4.
[444] L'acronyme vise les personnes lesbiennes, gay, bisexuelles, transgenres (ou autrement non-cisgenres) et *queer*, de manière non-exhaustive, incluant également les personnes intersexes, asexuelles ou aromantiques.
[445] eSafety Commissioner, Protecting voices at risk online, *op. cit*., p. 25.
[446] Thorn, LGBTQ+ Youth Perspectives: How LGBTQ+ Youth are Navigating Exploration and Risks of Sexual Exploitation Online. Findings from 2022 qualitative and quantitative research among 13-20-year-olds, Research conducted by Thorn in partnership with Benenson Strategy Group, juin 2023, p. 5 précisant que les jeunes LGBTQ+ se situent presque 20 points plus élevés à cet égard que les jeunes n'appartenant pas à ces communautés.
[447] Ibid., p. 52.
[448] eSafety Commissioner, Tipping the balance. LGBTIQ+ teens' experiences negotiating connection, self-expression and harm online, June 2024, p. 11.

interactions et des expressions de soi authentiques. Les adolescents LGBTQ+ peuvent également trouver des interactions plus inclusives et plus bienveillantes en ligne par rapport à leurs expériences hors ligne. Selon de nombreux jeunes dans l'étude de Thorn, "*internet les laisse être eux-mêmes*"[449].

L'utilité unique des réseaux sociaux pour les jeunes LGBTQ+ se reflète alors par leurs pratiques, l'étude Thorn relevant par exemple qu'ils ont plus fréquemment recours que les autres à des seconds comptes, principalement pour le soustraire au regard de certaines personnes de leur cercle social[450]. En outre, les recherches menées par l'*eSafety Commissioner* ont révélé que les adolescents LGBTQ+ passent plus de temps en ligne pendant leur temps libre que la moyenne nationale australienne pour leur tranche d'âge et sont également plus susceptibles de passer entre 7 et 11 heures en ligne par jour[451].

Si les plateformes et la technologie sont utilisées tant comme outils que comme espaces d'exploration sexuelle pour tous les adolescents, elles peuvent s'avérer plus sûres, privées et inclusives pour les jeunes LGBTQ+ que leurs options existant hors ligne[452]. Ainsi, l'étude Thorn affirme que "*l'exploration sexuelle en ligne n'est pas réservée à la jeunesse LGBTQ+, loin de là ; cependant, les adolescents LGBTQ+ rapportent des taux clairement plus élevés de ces expériences. Ils peuvent avoir moins d'opportunités de rencontrer et interagir avec d'autres jeunes LGBTQ+ dans leurs communautés hors ligne ou sentir que leur orientation sexuelle ou identité de genre ne serait pas soutenue*"[453]. Cette étude relève que l'usage d'applications de rencontre est presque deux fois plus élevé chez les adolescents LGBTQ+ que les autres[454], et qu'ils sont plus de deux fois plus susceptibles d'avoir partagé des images ou vidéos intimes[455]. De même, les recherches de l'*eSafety Commissioner* auprès d'adolescents LGBTQ+ australiens ont révélé que cette cohorte était plus susceptible d'envoyer et de recevoir des messages et des images à caractère sexuel en ligne que la moyenne nationale pour leur tranche d'âge[456]. En effet, les relations et les espaces sexuels et amoureux sont depuis longtemps une caractéristique de la construction communautaire pour diverses populations LGBTQ+[457], qui sont plus susceptibles de trouver des relations sexuelles et amoureuses en ligne[458].

---

[449] Thorn, LGBTQ+ Youth Perspectives, *op. cit.*, p. 55.
[450] Ibid., p. 14.
[451] eSafety Commissioner, Tipping the balance, préc., p. 10.
[452] Thorn, LGBTQ+ Youth Perspectives, *op. cit.*, p. 24.
[453] Ibid., p. 53.
[454] Ibid., p. 24 : 24% des adolescents LGBTQ+ ont rapporté avoir utilisé au moins l'une des applications de rencontre incluses dans l'étude, comparé aux autres (13%).
[455] Ibid., p. 5.
[456] eSafety Commissioner, Tipping the balance, préc., p. 12.
[457] P. Byron, K. Albury, T. Pym, "Hooking up with friends: LGBTQ+ young people, dating apps, friendship and safety", *Media, Culture & Society* 2021, 43(3), 497–514.
[458] Á. Castro, J. R. Barrada, P. J. Ramos-Villagrasa, E. Fernández-del-Río, "Profiling dating apps users: Sociodemographic and personality characteristics", *International Journal of Environmental Research and Public Health* 2020, 17(10).

Une disparité est toutefois soulignée parmi les groupes composant cette communauté. Selon l'étude Thorn, les adolescents garçons, cisgenres et non-hétérosexuels rapportent le plus fréquemment avoir déjà utilisé des applications de rencontre (32%)[459], et sont les plus nombreux à avoir déjà partagé leurs propres images intimes (25%, comparé à 16% pour les adolescentes filles, cisgenres et non hétérosexuelles ainsi que 16% pour les personnes non-cisgenres)[460]. Ils sont également deux fois plus susceptibles que les autres d'avoir déjà sollicité des images intimes, et d'avoir partagé les contenus intimes d'autrui[461].

En dépit des effets positifs des réseaux sociaux et sans même considérer les pratiques à caractère sexuel, les personnes LGBTQ+ sont affectées de manière disproportionnée par les risques en ligne. Il paraît acquis que, de manière générale, elles sont plus susceptibles de présenter des troubles mentaux et dépressifs que les autres, et que les jeunes LGBTQ+ présentent un risque significativement plus grand d'effectuer une tentative de suicide, en particulier les jeunes transgenres[462]. Ce phénomène a pu être relié à une forme de "stress minoritaire"[463]. Parallèlement, les réseaux sociaux sont une importante voie d'expression de l'homophobie et de la transphobie : aussi les études françaises se concentrent-elles principalement sur les signalements effectués en ce sens et la haine en ligne[464]. Les membres de cette communauté sont en outre deux fois plus victimes de propos haineux en ligne que la moyenne nationale australienne[465].

Une fois réintégrées les pratiques sexuelles en ligne des jeunes LGBTQ+, au prisme toujours de leur plus grande accessibilité et acceptabilité sur des réseaux perçus comme anonymes et soustraits du regard d'autrui qu'hors ligne, il a été souligné par l'eSafety Commissioner qu'ils subissaient un risque accru d'abus d'images intimes, de harcèlement et d'autres formes d'abus en ligne, potentiellement à caractère homophobe ou transphobe[466]. Ce niveau de risque augmente encore pour les jeunes vivant dans des zones rurales, présentant une diversité culturelle ou linguistique ou une situation de handicap ; ces facteurs peuvent également influencer leur capacité à reconnaître les risques en ligne ou à chercher de l'aide[467]. En outre, l'étude Thorn rapporte que les adolescents LGBTQ+ sont deux fois plus susceptibles que les autres d'avoir reçu une demande d'images intimes d'un inconnu en ligne (19% contre 8%), d'avoir été victimes de chantage ou de menaces (10% contre 5%), trois fois plus susceptibles d'avoir été contactés et manipulés par un adulte en

---

459 Thorn, LGBTQ+ Youth Perspectives, *op. cit.*, p. 25.
460 Ibid., p. 28.
461 Ibid.
462 IREPS et CRIPS Auvergne Rhône-Alpes, *La santé mentale des personnes LGBT*, Repères en prévention & promotion de la santé, mars 2020, p. 3.
463 Ibid., p. 4.
464 V. not. F. Bolter, D. Quinqueton, La haine anti-LGBTI+ en France. Instantanés issus de l'application FLAG! en 2022, 2023 ; SOS Homophobie, Rapport sur les LGBTIphobies 2023, pp. 76-83.
465 eSafety Commissioner, Protecting voices at risk online, *op. cit*., p. 25, faisant état de fréquences respectives de 30% et 14%.
466 eSafety Commissioner, Protecting voices at risk online, *op. cit*., p. 25. Pour un constat similaire, v. UNESCO, Rapport mondial de suivi de l'éducation : Rapport sur l'égalité des genres – La technologie à ses conditions : égalité des genres et inclusion, 2024, spéc. p. 39.
467 Ibid.

ligne (19% contre 6%), et presque autant d'avoir été harcelés (33% contre 12%)[468]. Des recherches plus récentes de l'eSafety Commissioner corroborent ces conclusions, en soulignant le risque accru de publication non consentie d'informations personnelles (doxxing, 19 %, contre 12 %) ou d'images privées (9 %, contre 6 %)[469].

Les personnes les moins comprises sont particulièrement exposées aux abus en ligne, en particulier les personnes transgenres et celles qui sont séropositives, parfois par malveillance mais aussi par simple ignorance ou manque d'exposition à des individus dont l'orientation sexuelle ou l'identité de genre est divers, y compris dans les médias[470]. Les adolescents garçons non-hétérosexuels et cisgenres ont rapporté des fréquences plus élevées de rencontres à risque et de tentatives de gérer seuls les situations à risque comparé aux autres adolescents[471].

Certains risques sont également spécifiques à la communauté LGBTQ+ comme la menace de révéler l'appartenance de la personne à la communauté, par exemple son orientation sexuelle ou son identité de genre (il s'agit de l'outing), en particulier lorsque cela ne correspond pas aux attentes de sa communauté culturelle. Les personnes transgenres, non-binaires ou autrement non-cisgenres pourraient également être affectées par des pratiques consistant à nier volontairement cette identité, notamment en utilisant le mauvais pronom ("mégenrer") ou prénom (deadnaming). Une autre particularité de la communauté LGBTQ+ réside dans le fort potentiel d'"abus latéral" (lateral abuse), c'est-à-dire des abus commis entre membres de la communauté[472]. Les personnes transgenres et bisexuelles seraient ainsi la cible de davantage d'abus intracommunautaires, de même que les individus présentant des caractéristiques déjà marginalisées, telles que l'ethnie, la religion, le genre, ou encore le poids[473], le handicap et la classe sociale[474].

Au-delà de ces enjeux, lesquels peuvent affecter différemment les membres de la communauté selon leur orientation sexuelle ou identité de genre, se profile un risque d'invisibilisation, au nom de la protection des mineurs entre autres, de contenus nécessaires à la formation et à la représentation de la communauté LGBTQ+. Que ce soit par la modération des contenus (réduction de visibilité, restriction d'âge, suppression, parfois provoquées par des signalements abusifs) ou par l'application d'un contrôle parental (sorte de « filtre » des contenus adaptés à l'âge), le risque est de modérer ou invisibiliser de manière injustifiée des propos relatifs à la communauté LGBTQ+ – qui seraient admis s'il s'agissait du même contenu ayant pour objet des sujets hétérosexuels ou cisgenres, par exemple un simple baiser – ou plus largement à la santé sexuelle et reproductive.

---

[468] Thorn, LGBTQ+ Youth Perspectives, *op. cit.*, p. 23.

[469] V. également en ce sens, European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025. pt. 3.4.

[470] eSafety Commissioner, Protecting LGBTIQ+ voices online, *op. cit.*, p. 13.

[471] Thorn, LGBTQ+ Youth Perspectives, *op. cit.*, p. 5.

[472] eSafety Commissioner, Protecting LGBTIQ+ voices online: resource development research – Qualitative report, août 2021, pp. 4 et 6, et surtout pp. 15 à 19.

[473] eSafety Commissioner, Protecting LGBTIQ+ voices online, *op. cit.*, p. 6 ; v. aussi p. 11 et 17 sur la mention "no Asians" fréquente sur les applications de rencontre.

[474] eSafety Commissioner, Protecting LGBTIQ+ voices online, *op. cit.*, p. 15.

10.1.3. Situation de handicap

Les jeunes en situation de handicap – entendu largement comme incluant les incapacités physiques, mentales, intellectuelles ou sensorielles[475] – sont susceptibles d'être à la fois plus dépendants des services numériques que les personnes non handicapées et plus vulnérables à certains risques.

Parmi les impacts positifs, les multiples travaux du eSafety Commissioner consacrés à ce sujet soulignent qu'Internet est un "grand niveleur" (great equaliser) pour les personnes en situation de handicap[476]. L'un des aspects notables réside dans la possibilité de s'abstraire des obstacles structurels rencontrés dans le monde physique et de pouvoir contrôler la représentation de soi ; une personne peut ne pas y être vue au prisme de son handicap, sauf si elle veut l'être[477]. Cela peut conduire à déstigmatiser des groupes habituellement marginalisés[478].

Les services numériques permettent ainsi de communiquer et socialiser avec les pairs, de lutter contre l'isolation ; ils présentent des opportunités de rejoindre des communautés d'intérêts, de jouer à des jeux et d'accéder à des informations et services[479], de prolonger des amitiés développées à l'école et d'en construire d'autres, au-delà du cercle social immédiat, ce qui est particulièrement important pour les jeunes disposant d'opportunités limitées pour socialiser en dehors de leur famille, notamment en raison d'un handicap physique, de difficultés de communication ou de membres de la famille très protecteurs[480].

Sept jeunes en situation de handicap sur dix (69%) disent ainsi qu'ils sont plus facilement eux-mêmes en ligne qu'en face-à-face, comparé à la moyenne nationale australienne de six sur 10 (59%)[481]. De la sorte, il n'est pas surprenant qu'ils passent davantage de leur temps de loisir en ligne que la moyenne nationale australienne[482]. L'une des raisons de l'utilisation étant d'étendre

[475] Convention internationale relative aux droits des personnes handicapées, 13 déc. 2006, art. 1 : « Par personnes handicapées on entend des personnes qui présentent des incapacités physiques, mentales, intellectuelles ou sensorielles durables dont l'interaction avec diverses barrières peut faire obstacle à leur pleine et effective participation à la société sur la base de l'égalité avec les autres ».
[476] eSafety Commissioner, A New Playground: The Digital Lives of Young People with Disability, 2023, p. 6 ; eSafety research, Online safety for young people with intellectual disability, 2020, p. 4.
[477] eSafety Commissioner, A New Playground: The Digital Lives of Young People with Disability, préc., p. 6.
[478] eSafety Commissioner, Online safety for young people with intellectual disability, préc., p. 4.
[479] Ibid.
[480] eSafety Commissioner, Online safety for young people, préc. p. 9.
[481] eSafety Commissioner, A New Playground: The Digital Lives of Young People with Disability, *op. cit.*, p. 9.
[482] eSafety Commissioner, A New Playground, préc., p. 10 : en semaine, 42% des jeunes en situation de handicap passent 3 à 5 heures en ligne par jour (comparé à la moyenne nationale de 36%) ; en

leur sphère sociale et de rencontrer de nouvelles personnes, il n'est pas non plus étonnant que la moitié des jeunes en situation de handicap aient entamé des conversations en ligne avec des inconnus, comparé à un tiers environ des autres[483].

Pour autant, les jeunes en situation de handicap sont exposés à un risque plus élevé de harcèlement en ligne, d'abus d'images intimes, de contact non sollicité et de *grooming* par des prédateurs sexuels[484]. Ce risque est encore accru au regard du caractère non inclusif des mesures de protection qui ne prennent pas en compte les besoins spécifiques de nombreux jeunes en situation de handicap[485]. Plus particulièrement, les jeunes en situation de handicap intellectuel ou cognitif peuvent avoir une compréhension différente des frontières sociales en ligne, une confiance excessive envers les inconnus rencontrés sur les réseaux[486], ou encore des difficultés de communication et d'appréhension des codes sociaux, qui justifient un soutien plus prononcé en termes de sensibilisation et formation pour leur sécurité et résilience en ligne[487]. Certains éducateurs interrogés par l'eSafety Commissioner ont également souligné qu'ils étaient plus vulnérables à plusieurs préjudices en ligne, dont le harcèlement tant en qualité de victimes que d'auteurs, une compréhension parfois partielle des conventions sociales pouvant les pousser à être blessants ou inappropriés en ligne[488], ou à mal appréhender ce qu'il est opportun de partager (par exemple des images intimes[489]). L'eSafety Commissioner affirme alors que, si les jeunes en situation de déficience intellectuelle ou cognitive sont confrontés à des risques similaires aux autres, leurs réactions sont considérablement différentes : plutôt que de rechercher du soutien extérieur, ils avaient tendance à se refermer et à éviter l'utilisation du service ayant causé une expérience négative (par exemple les réseaux sociaux, les achats en ligne ou, de manière plus extrême, les services numériques en général)[490]. La même étude australienne observe en outre que, bien que des éducateurs spécialisés pour les jeunes en situation de handicap intellectuel aient été prêts à informer ou soutenir leurs collègues en établissements généraux, aucun pont n'avait été pensé pour permettre ces formations[491].

---

weekend, 42% des jeunes en situation de handicap passent 6 heures ou plus en ligne par jour (comparé à la moyenne nationale de 32%).

[483] eSafety Commissioner, Protecting voices at risk online, préc., p. 14.

[484] eSafety Commissioner, Protecting voices at risk online, préc., p. 13 ; v. aussi eSafety Commissioner, A New Playground: The Digital Lives of Young People with Disability, *op. cit*., p. 12, affirmant que les jeunes en situation de handicap étaient plus susceptibles d'avoir été sollicités pour des informations sexuelles (26%, comparé à la moyenne nationale de 18%) ou images sexuelles d'eux-mêmes (15% contre 11%).

[485] WeProtect Global Alliance, PA Consulting, *Évaluation mondiale de la menace 2023*, *op. cit*., p. 14.

[486] eSafety Commissioner, A New Playground: The Digital Lives of Young People with Disability, *op. cit*., p. 7.

[487] eSafety Commissioner, Online safety for young people with intellectual disability, *op. cit*., p. 4.

[488] eSafety Commissioner, Online safety for young people, préc., p. 12 ; v. p. 18 pour un propos similaire de la part de certains parents de l'échantillon.

[489] eSafety Commissioner, Online safety for young people, préc., p. 17.

[490] eSafety Commissioner, Online safety for young people, préc., p. 6.

[491] eSafety Commissioner, Online safety for young people, préc., p. 21.

Un risque spécifique résulte en outre d'un potentielle fracture numérique due au handicap, avec un niveau moindre d'inclusion numérique ; parmi les obstacles figurent par exemple les niveaux variables d'audiodescription et de sous-titrage des contenus vidéos, les possibilités de lecture à voix haute de contenus textuels, la disponibilité de contenus et conseils clés en langage facile à lire et à comprendre (FALC), etc.[492]. Ainsi, parmi les initiatives ciblées du eSafety Commissioner figurent l'accessibilité de ses sites et ressources, la conformité aux lignes directrices relatives à l'accessibilité des contenus en ligne – avec une emphase sur les sous-titrages et l'audiodescription pour les contenus vidéo clés – ainsi que la multiplication des ressources FALC sur la sécurité en ligne[493]. Lors d'une étude menée spécifiquement sur les femmes en situation de handicap intellectuel ou cognitif, il réitère la nécessité d'instructions en formats accessibles, y compris des tutoriels et guides visuels montrant quelles mesures de sécurité mettre en œuvre. Il affirme enfin que les réponses habituelles, comme celles de se détourner des technologies en question, étaient problématiques dès lors que ces femmes se reposaient souvent sur la technologie pour communiquer avec leur famille, des réseaux de soutien et des prestataires de services[494].

10.1.4. Diversité ethnique, religieuse, linguistique ou culturelle

Les mineurs appartenant à une communauté ethnique, religieuse ou culturelle minoritaire sont susceptibles d'être davantage visés par les pratiques précitées, en particulier le harcèlement et la haine en ligne ainsi que – surtout si cette communauté stigmatise certains comportements notamment sexuels – les menaces ou le chantage, y compris la sextorsion. L'eSafety Commissioner souligne en outre que pour certaines communautés, telles que la communauté islamique, le partage de l'image d'autrui sans tenue présentant une importance religieuse ou culturelle est une forme d'abus en ligne[495].

Une fois l'atteinte commise, ces mineurs peuvent être "*confrontés à des obstacles particuliers en matière de signalement et de soutien en raison de la discrimination institutionnelle et systémique, des normes culturelles et des tabous, notamment la minimisation des abus en général et les discussions limitées sur le sexe et les relations intimes*"[496].

Indifféremment de ces premières caractéristiques ou en plus de celles-ci, la diversité linguistique implique ensuite que le français ne soit pas la langue maternelle du mineur, ou encore parfois qu'il bénéficie d'un faible degré d'alphabétisation en français. Cela soulève principalement des enjeux en termes de signalement et d'accès aux ressources permettant un accompagnement ou un soutien psychologique.

---

[492] eSafety Commissioner, Protecting voices at risk online, préc. p. 13.
[493] eSafety Commissioner, Protecting voices at risk online, préc. p. 15.
[494] eSafety Commissioner, 'For my safety'. Experiences of technology-facilitated abuse among women with intellectual disability or cognitive disability, Recherche qualitative menée par Queensland University of Technology, August 2021, p. 6.
[495] eSafety Commissioner, Protecting voices at risk online, préc., p. 23.
[496] WeProtect Global Alliance, PA Consulting, Évaluation mondiale de la menace 2023, préc. p. 13.

L'eSafety Commissioner observe ainsi, dans le cadre d'une étude consacrée aux femmes provenant d'un milieu culturellement ou linguistiquement divers, que la barrière de la langue peut contribuer à ce qu'elles n'aient pas connaissance des services à leur disposition, et peut compliquer le récit de leurs expériences[497]. L'étude conclut ainsi que si les impacts des abus facilités par la technologie ne sont pas substantiellement différents pour ces femmes que pour les autres, "*l'isolation sociale peut être amplifiée pour ces femmes lorsque la peur de l'humiliation est particulièrement forte*"[498].

10.1.5. Mineurs en situation de violence familiale ou conjugale

En 2020, l'eSafety Commissioner a commandé une étude afin d'examiner la dynamique, l'impact et l'implication des enfants dans les abus facilités par la technologie, dans le contexte des violences domestiques et familiales. L'étude a impliqué quatre jeunes (âgés de 16 à 18 ans) ayant été exposés à des abus facilités par la technologie dans un contexte de violence domestique, ainsi que 11 mères d'enfants dans ce contexte et 11 hommes ayant suivi un programme de changement de comportement destiné à sensibiliser et à intervenir en matière de violence domestique. L'étude comprenait également une enquête auprès de 515 professionnels spécialisés dans la violence domestique, ainsi que des groupes de discussion réunissant 13 praticiens. L'étude a relevé deux manières principales par lesquelles les jeunes étaient affectés dans ce contexte : soit en étant la cible directe d'abus ("abus direct"), soit en étant impliqués dans des abus facilités par la technologie et dirigés contre leur parent victime ("abus indirect")[499].

L'eSafety Commissioner a constaté qu'au cours de l'année précédant l'étude, les formes les plus communes d'abus facilités par la technologie à l'encontre des enfants telles que signalées par les professionnels de la violence domestique et familiale étaient la surveillance et le harcèlement (stalking), les menaces et intimidations, et le blocage des communications[500]. Les auteurs cherchaient souvent des informations sur les activités ou la localisation de l'enfant ou du parent non abusif, y compris en se faisant passer pour quelqu'un d'autre (par exemple, par un faux compte sur les réseaux sociaux)[501]. À cet égard, la séparation du couple peut ne pas freiner voire augmenter les abus facilités par la technologie, surtout lorsque les arrangements relatifs à la garde ou à l'autorité parentale obligent à maintenir un contact entre l'enfant et l'auteur des violences[502]. L'étude évoque les graves préjudices subis par les enfants dans ce contexte : troubles de la santé mentale, sentiment de peur et de culpabilité lié à la divulgation d'informations, difficultés relationnelles (y compris avec le parent non abusif), perturbation des activités et routines, isolement vis-à-vis de leur famille et de leurs amis, et sentiment de surveillance constante. Pour

[497] eSafety Commissioner, eSafety for Women from Culturally and Linguistically Diverse Backgrounds. Summary Report, February 2019, p. 4.
[498] eSafety Commissioner, eSafety for Woman, préc., p. 5.
[499] eSafety Commissioner, Children and technology facilitated abuse in domestic and family violence situations, Summary report, December 2020, p. 5.
[500] eSafety Commissioner, préc., p. 5.
[501] eSafety Commissioner, préc., pp. 4-5.
[502] eSafety Commissioner, préc., p. 6.

de tels jeunes, l'eSafety Commissioner souligne que le fait de simplement se couper des technologies n'est pas une réponse viable et ne servira qu'à davantage isoler l'enfant[503], l'exposant à un risque accru de préjudice.

10.1.6. Autres caractéristiques

Il serait également possible d'envisager comme des caractéristiques particulières tout élément relatif à la personne, notamment son état de santé, comme cela a été fait au Royaume-Uni pour les personnes épileptiques. Il pourrait alors paraître opportun d'inclure par ailleurs les troubles du comportement alimentaire ainsi que les troubles dépressifs ou suicidaires déjà envisagés[504] ; en dehors des caractéristiques de santé, il importe de prêter attention par exemple aux enfants placés en foyer[505].

Personnes épileptiques

En mai 2020, la page Twitter (désormais X) de l'*Epilepsy Society* au Royaume-Uni a subi une série soutenue d'attaques consistant à poster des centaines d'images et GIFs clignotants dans la section commentaire de ses publications, et en contactant directement certains abonnés de cette page, dans le but de provoquer des crises d'épilepsie (epilepsy trolling)[506]. En réponse, l'Online Safety Act 2023 crée une nouvelle infraction pour l'envoi ou la communication d'images qui clignotent électroniquement (sending or showing flashing images electronically). Celle-ci est constituée à plusieurs conditions, y compris la connaissance ou suspicion de l'auteur que l'un des utilisateurs exposés à ce contenu est épileptique ainsi que sa volonté de causer un dommage du fait de l'exposition à ces images clignotantes[507].

10.2. CADRE JURIDIQUE

Mesures répressives. Les mineurs appartenant à une communauté ou à groupe historiquement protégé, à raison de leur origine ou de leur appartenance ou non-appartenance à une ethnie, nation, « race » ou religion déterminée, ou en raison de leur sexe, orientation sexuelle, identité de genre ou handicap, bénéficient de certaines protections transversales. Il convient de souligner en premier lieu que le motif discriminatoire d'un crime ou d'un délit, en raison de l'appartenance à l'un des groupes précités à l'exception du handicap, constitue une circonstance aggravante de portée

[503] eSafety Commissioner, préc., p. 4.
[504] V. supra, Chapitre 9 "Modification de l'image de soi".
[505] eSafety voices at risk, p. 5, affirmant qu'il s'agit de l'une des « priorités stratégiques ».
[506] OFCOM, Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm, Consultation, 9 nov. 2023, p. 272, pt. 6R.13.
[507] Pour le détail des éléments constitutifs de l'infraction, v. Online Safety Act, s.184.

générale en droit pénal[508]. En second lieu, un certain nombre d'infractions spécifiques visent à combattre les discours de haine publiquement adressés à ces groupes protégés. Celles-ci incluent la provocation directe ou apologie publique d'actes de terrorisme[509], l'apologie ou négation de certains crimes contre l'humanité[510] ; la provocation à la discrimination, à la haine ou à la violence[511] ; les diffamations ou injures discriminatoires[512]. Sont également considérées comme des contraventions de 5e classe les provocations, diffamations et injures non publiques visant une personne (ou un groupe) appartenant à un groupe précité[513].

S'agissant des abus fondés sur le genre, l'infraction d'outrage sexiste et sexuel incrimine le fait d'imposer à une personne tout propos ou tout comportement à connotation sexuelle ou sexiste qui soit porte atteinte à sa dignité en raison de son caractère dégradant ou humiliant, soit crée à son encontre une situation intimidante, hostile ou offensante, lorsque ce fait est commis, entre autres, sur un mineur[514] et à la condition que ces faits ne soient pas déjà constitutifs de certaines autres infractions[515].

S'agissant des dispositions spécifiques aux personnes présentant une appartenance réelle ou supposée à la communauté LGBTQ+, une innovation récente consiste à réprimer les pratiques, comportements ou propos répétés visant à modifier ou à réprimer l'orientation sexuelle ou l'identité de genre, vraie ou supposée, d'une personne et ayant pour effet une altération de sa santé physique ou mentale[516]. L'infraction d'outrage sexiste et sexuel est également constituée lorsque les faits sont commis en raison de l'orientation sexuelle ou de l'identité de genre, vraie ou supposée, de la victime[517].

Obligations imposées aux fournisseurs de réseau social. Le fournisseur du réseau social est tenu, au titre de l'article 6 DSA, de supprimer promptement les contenus précités lorsqu'ils lui sont notifiés dans les conditions prévues par le texte. La plupart d'entre eux doivent également

---

[508] Code pénal, art. 132-76 instaurant une circonstance aggravante de portée générale en droit pénal lorsqu'un crime ou un délit est précédé, accompagné ou suivi de propos, écrits, images, objets ou actes de toute nature qui soit portent atteinte à l'honneur ou à la considération de la victime ou d'un groupe de personnes dont fait partie la victime à raison de son appartenance ou de sa non-appartenance, vraie ou supposée, à une prétendue race, une ethnie, une nation ou une religion déterminée, soit établissent que les faits ont été commis contre la victime pour l'une de ces raisons, sauf exceptions ; art. 132-77 à raison de son sexe, son orientation sexuelle ou identité de genre vraie ou supposée, sauf exceptions.

[509] Code pénal, art. 421-2-5, la provocation n'ayant toutefois pas besoin d'être publique pour que l'infraction soit constituée.

[510] Loi du 29 juillet 1881 sur la liberté de la presse, art. 24 al. 5 ; art. 24 bis al. 1 ; art. 24 bis al. 2.

[511] Loi du 29 juillet 1881 préc., art. 24 al. 7 et 8.

[512] Loi du 29 juillet 1881 préc., art. 32 al. 1 et 2 ; art. 33 al. 3 et 4.

[513] Code pénal, art. R. 625-7 pour la provocation, R. 625-8 pour la diffamation, R. 625-8-1 pour l'injure.

[514] Code pénal, art. 222-33-1-1, I, 2°.

[515] Code pénal, art. 222-33-1-1, I renvoyant aux art. 222-13, 222-32, 222-33, 222-33-2-2 et 222-33-2-3.

[516] Code pénal, art. 225-4-13.

[517] Code pénal, art. 222-33-1-1, I, 7°.

être signalés par le fournisseur de réseau social auprès des autorités compétentes en vertu de l'article 6, IV, 4 LCEN, et peuvent être punis d'une peine de bannissement au sens de l'article 131-35-1, II, 2° 8° et 11° du Code pénal.

En outre, les très grandes plateformes sont tenues d'évaluer et d'atténuer les risques systémiques présentés par leurs services et fonctionnalités en vertu des articles 34 et 35 du DSA. La quatrième catégorie de ces risques paraît ici particulièrement pertinente : "*tout effet négatif réel ou prévisible lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes*"[518]. Le considérant 40 du DSA précise en outre qu'il a vocation à "*garantir différents objectifs de politique publique, comme celui d'assurer la sécurité et la confiance des destinataires du service, y compris les consommateurs, les mineurs et les utilisateurs qui sont particulièrement exposés au risque de faire l'objet de discours haineux, de harcèlement sexuel ou d'autres actions discriminatoires » et de « donner les moyens d'agir aux destinataires et autres parties affectées*"[519].

L'Online Safety Act adopté au Royaume-Uni en 2023[520] accorde une place plus importante aux caractéristiques de l'utilisateur. Dès son article introductif, il affirme en effet vouloir rendre les services numériques concernés par le texte plus sûrs pour les individus ; pour ce faire, il leur impose des devoirs d'identification, atténuation et gestion des risques de préjudice issus de contenus et activités qui sont soit illégaux, soit préjudiciables aux enfants, "*y compris les risques qui affectent particulièrement les individus présentant une certaine caractéristique*"[521].

Il intègre ensuite expressément, au sein des "*devoirs d'analyse des risques envers les enfants*" applicables aux services d'utilisateur à utilisateur auxquels les mineurs sont susceptibles d'accéder, le devoir d'évaluer "*le niveau de risque de dommage envers les enfants présenté par du contenu préjudiciable aux enfants qui affecte particulièrement les individus avec une certaine caractéristique ou les membres d'un certain groupe*"[522]. En outre, parmi les "*contenus de simple priorité préjudiciables aux enfant*s" et devant être envisagés dans l'analyse de risque figurent les contenus qui sont abusifs et ciblent la race, la religion, le sexe, l'orientation sexuelle, le handicap ou la réattribution sexuelle (*gender reassignment*)[523], ou qui incitent à la haine en raison de ces caractéristiques[524]

Enfin, afin d'autonomiser les utilisateurs adultes (*adult user empowerment*), les services de catégorie 1 sont soumis à des obligations paraissant refléter le droit au paramétrage proposé par ailleurs au sein de notre étude. Ils doivent ainsi inclure dans le service, de manière proportionnée, des fonctionnalités permettant aux utilisateurs adultes d'accroître leur contrôle

[518] DSA, art. 34.1.d.
[519] DSA, cons. 40.
[520] Online Safety Act 2023.
[521] Online Safety Act, s.1.2.a.
[522] Online Safety Act, s.11.6.d.
[523] Online Safety Act, s.62.2.
[524] Online Safety Act, s.62.3.

sur certains types de contenus[525] ; ces fonctionnalités consistent à réduire la probabilité que l'utilisateur soit confronté à ces contenus ou à l'alerter quant à la présence de ce contenu sur le service[526], ou à filtrer les contenus provenant d'utilisateurs non vérifiés[527].

La proportionnalité de l'introduction de telles mesures s'apprécie au regard d'une évaluation, laquelle comprend notamment "*la probabilité que des utilisateurs adultes avec une certaine caractéristique ou qui sont membres d'un certain groupe soient confrontés à du contenu pertinent qui les affecte particulièrement*"[528], ainsi que la taille et les capacités de l'opérateur[529].

Les types de contenus concernés sont ceux qui encouragent, promeuvent ou fournissent des instructions pour un suicide, une automutilation délibérée, un trouble du comportement alimentaire ou des comportements associés[530] ; ceux qui sont abusifs et ciblent la race, la religion, le sexe, l'orientation sexuelle, le handicap ou la réattribution sexuelle (*gender reassignment*)[531], ou qui incitent à la haine en raison de ces caractéristiques[532].

Il convient enfin de relever que, s'agissant des personnes en situation de handicap, le droit français énonce des exigences d'accessibilité des services de communication au public en ligne de certains organismes, notamment les entreprises dont le chiffre d'affaires annuel réalisé en France excède 250 millions d'euros[533]. Ces obligations sont néanmoins soumises à plusieurs exceptions importantes. Tout d'abord, l'exigence d'accessibilité ne s'applique pas aux contenus de tiers qui ne sont ni financés ni développés par l'organisme concerné et qui ne sont pas sous son contrôle[534] ; ni aux contenus audio et vidéo diffusés en direct, y compris ceux comprenant des composants interactifs[535] ; ni aux contenus audio et vidéo préenregistrés, y compris ceux comprenant des composants interactifs, publiés avant le 23 septembre 2020[536]. Ensuite, l'exigence est inapplicable si l'organisme concerné prouve que cela constitue une charge disproportionnée[537], et le non-

[525] Online Safety Act, s.15.2.
[526] Online Safety Act, s.15.3.
[527] Online Safety Act, s.15.9 et 10.
[528] Online Safety Act, s.14.5.d.
[529] Online Safety Act, s.16.1.
[530] Online Safety Act, s.16.3.
[531] Online Safety Act, s.16.4.
[532] Online Safety Act, s.16.5.
[533] Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées, art. 47, I, 4° renvoyant au décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne, art. 2. Sur l'accessibilité numérique par les personnes souffrant de handicap en général, v. not H. Rihal, « Responsabilité et accessibilité numérique », *RDSS* 2023 p.34 ; T. Giraud, « Communication – Numérique – La question de l'accessibilité sur le Web », *Juris associations* 2021, n°641, p. 43.
[534] Décret du 24 juillet 2019 préc., art. 3, 5°.
[535] Décret du 24 juillet 2019 préc., art. 3, 3°.
[536] Décret du 24 juillet 2019 préc., art. 3, 2°.
[537] Loi du 11 février 2005 préc., art. 47, II. La charge disproportionnée est précisée par le décret du 24 juillet 2019 préc., art. 4.

respect par ces entreprises de l'obligation d'accessibilité en soi ne peut être sanctionnée - l'Arcom pouvant toutefois sanctionner le défaut des mentions obligatoires relatives à l'accessibilité[538]. D'autres exigences d'accessibilité, énoncées en droit de la consommation, sont applicables notamment aux services fournissant un accès à des services de médias audiovisuels et aux services de commerce électronique fournis après le 28 juin 2025[539]. Les réseaux sociaux semblent donc concernés, quant au fonctionnement de leur service uniquement ; car sont ici aussi exemptés les contenus de tiers qui ne sont ni financés ni développés par l'opérateur économique concerné et qui ne sont pas sous son contrôle[540], ce qui exclut les contenus postés par les utilisateurs.

10.3. PRÉCONISATIONS

Il convient de préciser au préalable que la mise en œuvre des préconisations suivantes ne doit pas impliquer, pour l'opérateur de réseaux sociaux ou pour quiconque d'autre, de tentative d'identification des caractéristiques présentées par un utilisateur particulier.

Préconisation 31 - S'assurer de l'accessibilité des dispositifs de signalement en ligne, de recours et de plainte pour les personnes en situation de handicap et les personnes dont le français n'est pas la langue maternelle, y compris en multipliant les ressources FALC et les traductions, et en proposant une pluralité de canaux sensoriels. Il convient de veiller à ce que tout mineur puisse recourir seul, si besoin, à ces dispositifs.

Préconisation 32 - Prendre en compte, lors de toute analyse de risque effectuée par les opérateurs ainsi que pour toute mesure étatique, les effets produits sur les personnes présentant une ou plusieurs caractéristiques particulières ; adopter des mesures efficaces pour supprimer – ou, à défaut, atténuer – ces effets lorsqu'ils sont négatifs, y compris l'abandon de la fonctionnalité ou mesure envisagée.

Préconisation 33 - Élaborer des ressources gouvernementales et/ou associatives à destination des mineurs présentant des caractéristiques particulières, de leur famille, du personnel enseignant et de santé, ainsi que des adultes présentant ces caractéristiques, y compris des ressources FALC.
Le travail de l'eSafety Commissioner australien peut servir de modèle : son site internet[541] dispose ainsi de sections spécifiques pour les éducateurs, les parents, les jeunes, les enfants, les femmes,

[538] Loi du 11 février 2005 préc., art. 47-1.
[539] Code de la consommation, art. L. 412-13 et D. 412-49 et s. ; pour le détail des exigences d'accessibilité, v. l'arrêté du 9 octobre 2023 fixant les exigences en matière d'accessibilité applicables aux produits et services. Les textes précisent en outre que ces exigences d'accessibilité ne s'appliquent que dans la mesure où elles n'entraînent pas une modification fondamentale de la nature du service, ou une charge disproportionnée pour l'opérateur : Code de la consommation, art. L. 412-13, II.
[540] Code de la consommation, art. D. 412-50, III, 4°.
[541] V. eSafety Commissioner.

les personnes âgées, les Premières Nations, les communautés et les professionnels, avec une multitude d'informations pour les principales situations rencontrées en ligne. Les ressources sont élaborées en partie selon une stratégie d'implication des jeunes (youth engagement strategy) consistant à recueillir leurs expériences et besoins, afin d'aboutir à une éducation systématique plutôt qu'à un apprentissage par tâtonnements.
Les nombreuses études réalisées par l'eSafety Commissioner proposent également des initiatives et mesures à mettre en œuvre, telles que :

- La fourniture de conseils et voies de signalement sur mesure, ainsi que des guides pour certains risques spécifiques en ligne selon les caractéristiques.
- La formation des professionnels aux enjeux spécifiques de sécurité en ligne auxquels sont confrontées les personnes présentant une caractéristique particulière.
- La fourniture de ressources permettant de comprendre quels sont les abus en ligne (y compris, pour la communauté LGBTQ+, les abus latéraux) ; d'exemples spécifiques de comportements inappropriés et appropriés en ligne, du lexique adéquat, d'exemples encourageant les utilisateurs à prendre conscience de leur propre ignorance, malveillance ou biais inconscient ; l'emphase sur la nécessité de soutenir activement les personnes présentant des caractéristiques particulières, en particulier pour les utilisateurs témoins d'abus en ligne.
- La conception de ressources encourageant les interactions sûres et positives en ligne, les réactions conseillées face aux abus en ligne – y compris celles des témoins – par exemple des guides et outils interactifs.
- La communication et synthèse claire du droit et des politiques relatives aux abus en ligne.
- L'adaptation de ces ressources à l'âge (en distinguant les enfants de 5 à 12 ans, et les jeunes de 13 à 25 ans) et aux capacités de la personne (FALC) ; la fourniture de ressources pouvant être exploitées en classe par les éducateurs, dont une « boîte à outils de la sécurité en ligne pour les écoles ».
- La traduction des ressources cruciales en plusieurs langues afin de garantir leur accessibilité aux personnes provenant d'un milieu culturellement et linguistiquement divers.
- La diversification des ressources, par exemple des programmes éducatifs ou des jeux en ligne promouvant la sécurité et le respect des différentes cultures et identités.

Préconisation 34 - Documenter les effets positifs et négatifs des réseaux sociaux sur les personnes présentant des caractéristiques particulières, ainsi que la spécificité de leurs usages en ligne et des risques auxquels ils sont exposés ; plus largement, documenter le bien-être physique et mental de ces personnes.

Mener des études quantitatives et qualitatives afin de disposer de données fiables sur la population française, en portant une attention particulière aux enjeux découlant de la présentation simultanée de plusieurs caractéristiques (intersectionnalité).
Envisager les pratiques en ligne de manière globale, y compris dans leur aspect positif : en creux, les prises de contact et le partage d'information, la représentation et la bienveillance parfois permises par les réseaux sociaux permettraient de révéler des mesures envisageables hors ligne.
En ce qui concerne le bien-être physique et mental des mineurs présentant des caractéristiques particulières, est ici reprise et élargie la recommandation de la CNDCH relative aux personnes LGBTQI suggérant une étude nationale quantitative et qualitative sur les violences LGBTIphobes en milieu scolaire et une enquête sur les taux de suicide parmi les personnes LGBTI, en particulier les jeunes.

Préconisation 35 - S'assurer de l'accessibilité des réseaux sociaux aux mineurs en situation de handicap ; encourager l'accessibilité des contenus générés par les utilisateurs.

Préconisation 36 - Veiller à ce que les outils de modération ou de protection des mineurs (par exemple les filtres adaptés à l'âge) n'aboutissent pas à l'invisibilisation de certains contenus relatifs notamment à la santé sexuelle, à la contraception et à la communauté LGBTQ+ ; quantifier la modération illégitime de contenus relatifs à cette communauté et implémenter des mesures d'atténuation.

Préconisation 37 - Désactiver par défaut la lecture automatique de contenus vidéos ou, à tout le moins, permettre de la désactiver.
Cette mesure vise principalement la protection des personnes épileptiques et celles présentant une hypersensibilité aux lumières et sons ; elle rejoint en outre certaines préconisations formulées en matière de conception et fonctionnalités des interfaces.

Préconisation 38 - Favoriser la représentation des minorités dans les contenus auxquels les mineurs sont exposés : supports scolaires, médias, jeux vidéo, publicités, etc.

Préconisation 39 - Penser de nouvelles mesures de sensibilisation et garantir le soutien de l'État et des plateformes de réseaux sociaux, y compris aux initiatives existantes.
Promouvoir les mesures et ressources de sensibilisation tant au sein des institutions scolaires (affiches dans l'établissement, formation des enseignants, interventions extérieures par des associations spécialisées) qu'au-delà, en garantissant le soutien y compris financier de l'État et des plateformes concernées.
Une source d'inspiration à cet égard peut être trouvée dans la pratique de certains pays anglo-saxons de désigner un jour, une semaine ou un mois de l'année comme étant privilégié pour la sensibilisation à certains enjeux historiques et sociétaux, de même que pour des évènements, commémorations ou fêtes en ce sens : il existe par exemple un Mois de l'histoire noire (Black History Month), un Mois de l'histoire LGBT (LGBT History Month), un Mois de la santé mentale (Mental Health Awareness Month), etc.

IV. CONCEPTION ET ACCÈS AUX SERVICES

Alors que la conception de certains réseaux sociaux expose les mineurs à différents risques, une conception adaptée à l'âge peut constituer dans le même temps un élément déterminant de leur protection. A ce titre, la réglementation existante interdisant aux fournisseurs de réseaux sociaux d'exposer leurs utilisateurs à des interfaces trompeuses et manipulatrices doit être prolongée par une appréhension juridique des conceptions addictives et par différentes mesures de *Safety by design* visant à garantir aux mineurs d'accéder à un environnement sûr tout en garantissant leur autonomie et le respect de leurs libertés et droits fondamentaux lors de leurs interactions sur les réseaux sociaux (**Chapitre 11**).

Quant aux conditions d'accès au service tenant à l'âge de l'utilisateur, cette mesure est généralement présentée comme un enjeu majeur en ce qui concerne la protection des mineurs en ligne. Il convient à cet égard de relever les évolutions récentes du cadre légal afin d'imposer de nouvelles obligations aux plateformes en ce sens tout en en soulignant les limites au regard des risques d'atteintes aux droits fondamentaux des utilisateurs pouvant résulter de telles mesures ou encore de la disparité des procédés mis en œuvre en l'absence d'harmonisation au niveau européen, auxquels s'ajoute le possible contournement de ces mesures par les mineurs (**Chapitre 12**).

Il convient en outre d'envisager les enjeux relatifs au contrôle parental, lequel vise à restreindre l'accès des jeunes à des contenus inappropriés, qui supposent d'en analyser les modalités et les limites (**Chapitre 13**).

CHAPITRE 11 : CONCEPTION DES SERVICES

11.1. ENJEUX

Différents types de risques ont pu être identifiés pour les mineurs au regard de leurs usages des réseaux sociaux, qui sont désormais présentés selon une typologie dite "5C[542]" : les risques liés aux contenus (1), à la conduite (2), au contact (3), à la consommation (4) et ainsi que les risques transversaux (5).

Plusieurs exemples de risques sont cités dans cette typologie des risques en ligne "5C" en ce qui concerne les enfants[543] :

> (1) risques liés aux contenus (*Content risks*) : est ici visée l'exposition des mineurs, de manière inattendue et involontaire, à des contenus susceptibles de leur porter préjudice, tels que des contenus haineux, préjudiciables ou illicites, ainsi qu'à la désinformation, comme les contenus promouvant l'automutilation, le suicide, les troubles alimentaires ou la violence extrême[544]. Plus précisément et à titre d'exemple, il s'agit des informations et communications violentes, sanglantes, graphiques, racistes, haineuses ou extrémistes qui font partie des formes de contenus haineux et agressifs que les enfants ont rencontrés en ligne et qui peuvent nuire au développement physique, émotionnel, cognitif ou social des enfants[545].
>
> (2) risques liés à la conduite (*Conduct risks*) : sont ici visés des comportements que les mineurs peuvent adopter activement en ligne et qui peuvent présenter des risques tant pour eux-mêmes que pour d'autres, tels que les comportements haineux, préjudiciables ou illicites (par ex. publication/envoi de contenus violents ou pornographiques), ainsi que les

[542] En particulier, v. OECD, How's life for children in the digital age?, June 2025, p. 54 &s ; également, Commission européenne, Commission européenne, Communication de la Commission, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, Annexe Typologie des risques en ligne dite «5C» en ce qui concerne les enfants - Et déjà OECD, Children in the Digital environment. Revised typology of risks, OECD Digital Economy paper, n°3x02, 2021 et S. Livingstone, S., M. Stoilova, The 4Cs: Classifying Online Risk to Children, (CO:RE Short Report Series on Key Topics), Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence, 2021.

[543] Lignes directrices article 28 DSA, Annexe Typologie des risques en ligne dite « 5C » en ce qui concerne les enfants, préc.

[544] Ibid.

[545] B. O'Neill, Research for CULT Committee – The influence of social media on the development of children and young people, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels, 2023, p.20.

comportements problématiques créé par un utilisateur (à l'image de la participation à des défis dangereux)[546]. Le cyberharcèlement en est l'illustration la plus emblématique[547].

(3) risques liés aux contacts (*Contact risks*) : sont visées ici les situations dans lesquelles les mineurs ne sont pas acteurs, mais victimes d'interactions comme les rencontres haineuses, préjudiciables ou illicites et les autres rencontres problématiques (notamment le cyberharcèlement et les sollicitations à caractère sexuel tels que le grooming et la sextorsion[548].

(4) risques pour les consommateurs (*Consumer et contract risks*) : il s'agit ici des risques auxquels les mineurs sont confrontés à des risques en tant que consommateurs, comme les risques de profilage commercial et les risques liés à la sécurité (achat et consommation de produits illicites et dangereux (comme l'alcool et la drogue) ainsi que ceux liés aux contrats (accès aux données à caractère personnel et conditions générales inéquitables)

(5) risques transversaux *(Cross-cutting risks*) : sont notamment visés les risques liés à l'utilisation des technologies et de l'intelligence artificielle, par exemple via les agents conversationnels anthropomorphisés, ou les deepfakes pouvant faciliter le grooming ou la fraude, les risques pour la santé et le bien-être (pouvant par exemple augmentation les troubles du comportement alimentaire et les problèmes de santé mentale, et les risques relatifs à la protection de la vie privée et des données (dont la géolocalisation pouvant être exploitée par les pédocriminels pour localiser et aborder des mineurs)

Plusieurs de ces risques résultent en tout ou partie de la conception des services (1), qu'il s'agisse de leurs interfaces de choix, de leurs fonctionnalités ou encore de leurs algorithmes de recommandation et de modération. Il convient de le préciser au regard des pratiques décrites dans la 3e partie en étudiant en outre les risques propres à la conception - indépendamment des contenus auxquels sont exposés les mineurs -, alors que d'autres sont amplifiés par la conception. Dans le même temps, la conception peut être un outil de prévention des risques (2).

11.1.1. La conception comme source de risques

Différents risques sont directement ou indirectement liés à la conception de ces services, étant entendu que celle-ci est sous-tendue par leur modèle d'affaires, qu'il s'agisse de leurs interfaces de choix, de leurs fonctionnalités ou encore de leurs algorithmes de recommandation et de

[546] Lignes directrices article 28 DSA, préc.
[547] Arcom, Étude qualitative, Mineurs en ligne : Quels risques ? Quelle protection ?, septembre 2025, p.39.
[548] Lignes directrices article 28 DSA, préc. - V. également, Arcom, Etude préc., p.43 ou encore B. O'Neill, Etude préc., qui relevait à ce titre les risques de contacts avec des inconnus ainsi que les rencontres préjudiciables et illégales (sexuelles) ou encore la persuasion idéologique et les risques de manipulation.

modération[549]. Nombreux sont désormais les rapports dénonçant leurs possibles effets délétères résultant de choix directement réalisé par des fournisseurs de service dont le modèle repose sur l'économie de l'attention, en particulier concernant les jeunes utilisateurs de ces services et appellent à agir directement sur leur conception[550]. Il convient de le préciser s'agissant des différentes pratiques décrites dans la 3e partie (a), d'étudier spécifiquement les risques propres à la conception - indépendamment des contenus auxquels sont exposés les mineurs - (b), ainsi que les risques qui se trouvent amplifiés par la conception (c).

(a) Parmi les pratiques identifiées dans la troisième partie de l'étude[551], il est possible de relever l'impact de la conception sur différents risques - comme cela a pu être identifié par la Commission européenne dans ses lignes directrices sur l'article 28 du 14 juillet 2025 -, parmi lesquels on trouve les risques :

- d'exposition à des contenus inadaptés (contenus haineux, préjudiciables et illicites comme les contenus encourageant au suicide, à l'automutilation et les troubles alimentaires et le contenus de violence extrême)[552] ;
- liés au comportement (publication de contenus violents, pornographiques, participation à des comportements illégaux comme le chantage et la sextorsion)[553] ;
- de contact (grooming, sextorsion, abus sexuels, cyberharcèlement)[554] ;
- liés aux évolutions technologiques (deepfakes à caractère sexuel)[555] ;
- pour la santé et le bien-être (augmentation de l'obésité/anorexie et problèmes de santé mentale lié à l'utilisation excessive des plateformes en ligne pouvant dans certains cas

[549] European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025, p. 27. En 2024, l'OCDE a pu constater à quel point les techniques de manipulation, de coercition, de tromperie ou de conception addictive, connues sous le nom de « dark commercial patterns » ou interfaces commerciales truquées, sont répandues dès lors que, si les techniques d'exploitation des biais cognitifs ne sont pas nouvelles, leur prévalence et leur efficacité vont en s'accroissant (OCDE, Déclaration sur la protection et l'autonomisation des consommateurs dans le cadre des transitions numérique et verte, 2024).

[550] V. notamment Mission Enfants et Ecrans, A la recherche du temps perdu, 2024 - Commission d'enquête sur les effets psychologiques de TikTok, Avant propos, 2025. Adde, F. Forestier, M. Kamasi, S. Broadbent, C. Zolynski, *Pour une nouvelle culture de l'attention*, Odile Jacob, 2024.

[551] Sur ce point, v. la 3ème partie de l'étude consacrée aux pratiques en ligne.

[552] Sur ce point, v. Chapitre 7, Exposition à des contenus violents et à caractère pornographique, pt. 7.1.

[553] Ibid.

[554] Sur ce point, v. Chapitre 4, Diffusion non consentie d'images intimes, pt. 4.1 et Chapitre 5 sur le chantage et l'exploitation de mineurs en ligne (sextorsion), pt. 5.1.

[555] Sur ce point, v. Chapitre 6, Deepfakes, pt. 6.1.

avoir des effets négatifs sur la santé physique et mentale tels que la dépendance, la dépression, les troubles anxieux et du sommeil, l'isolement social)[556] ;

- pour la confidentialité des données (accès aux informations du mineur, notamment la géolocalisation, exploitées potentiellement par les prédateurs sexuels pour localiser les mineurs).

(b) Certains de ces risques sont propres à la conception. Ainsi, par exemple, des travaux ont démontré que la conception du service peut jouer un rôle important dans la génération de risques "de contact". En effet, lorsque les comptes utilisateur sont paramétrés en public par défaut et qu'ils sont recommandés à des personnes se trouvant hors de leur sphère de contacts, ceci accroît les risques que des personnes mal intentionnées puissent cibler ou contacter les mineurs à des fins de chantage sexuel[557]. Cela ressort également de l'action engagée en 2023 par le procureur général du Nouveau-Mexique pour manquements graves à la protection des enfants s'agissant des risques d'abus sexuels, de racolage en ligne et de traite des êtres humains contre Meta[558] concernant les services Instagram et Facebook. L'enquête, menée à l'aide de faux profils d'enfants de moins de 14 ans, a révélé que ces services orientaient activement les mineurs vers des contenus à caractère sexuel explicites et facilitaient le contact avec des prédateurs sexuels. Le procureur a alors dénoncé l'incapacité de Meta à prévenir ces dérives malgré la connaissance des risques encourus, soulignant que la société privilégiait la maximisation de l'engagement et des revenus publicitaires au détriment de la sécurité des jeunes utilisateurs.

(c) D'autres risques peuvent être amplifiés par la conception dès lors que l'inexpérience des mineurs peut conduire à des risques accrus de tromperie et de manipulation par le recours à des interfaces de choix trompeuses ou manipulatrices (*dark patterns*) et que différents fournisseurs de services en ligne conçoivent leurs interfaces et leurs algorithmes de manière à maximiser l'engagement de leurs utilisateurs et leur temps passé en ligne. Sur ce dernier point, plusieurs études ont été consacrées à l'impact de certaines fonctionnalités, telles que les likes, les notifications ou les confirmations de lecture ou encore des algorithmes de recommandation, qui exposent les jeunes utilisateurs à des incitations constantes à l'interaction[559]. Certains de ces mécanismes de conception peuvent être considérés comme addictifs et emporter d'importants effets préjudiciables sur la santé physique et mentale ainsi que le bien-être des utilisateurs, en

---

[556] Sur ce point, v. Chapitre 9, Modification de la perception de soi, pt. 9.1.

[557] Knight-Georgetown Institute & Panoptykon Foundation, European Board for Digital Services and European Commission Report on Systemic Risks and Mitigations under the Digital Services Act, 7 April 2025, p. 3.

[558] New Mexico Department of Justice, Attorney General Raúl Torrez Files Lawsuit Against Meta Platforms and Mark Zuckerberg to Protect Children from Sexual Abuse and Human Trafficking, 6 Decembre 2023.

[559] En ce sens, v. Parlement européen, Draft report on Protection of minors online (2025/2060(INI)), May 2025, p. 6 et Résolution du 12 décembre 2023 sur la conception addictive des services en ligne et la protection des consommateurs sur le marché unique de l'UE (2023/2043(INI)), (C/2024/4164) et European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025, pt. 3.4.

particulier des mineurs qui sont particulièrement exposés à de tels effets[560]. A cet égard, deux sujets particuliers sont à envisager compte tenu de leurs enjeux d'actualité : la surexposition à des contenus toxiques du fait de la conception, d'une part ; les interactions avec des systèmes d'IA et spécifiquement avec des IA Compagnons, d'autre part.

Recommandation ultra personnalisée et sur-exposition à des contenus préjudiciables (effet spirale / *rabbit hole*). Les risques tenant à l'exposition à des contenus préjudiciables sont étudiés dans les parties précédentes[561]. Il s'agit ici d'envisager l'accroissement de ces risques tenant à la conception du service, en particulier en ce qui concerne le système de recommandation organisant l'exposition de l'utilisateur aux contenus lors de ses interactions sur/avec le service dès lors qu'ils reposent sur un mécanisme visant à stimuler l'engagement des utilisateurs[562]. Sur ce point, et comme cela a pu être relevé, le fonctionnement des algorithmes de recommandation repose sur des modèles de comportements pouvant révéler les vulnérabilités individuelles des utilisateurs du service, comme des troubles du comportement alimentaire ou des troubles dépressifs[563]. Ces vulnérabilités peuvent s'en trouver exploitées dès lors que les algorithmes de recommandation, s'inscrivant dans une logique de maximisation de l'engagement des utilisateurs du service, peuvent les exposer à une sélection de contenus ciblés. Cela peut conduire à générer un effet spiral (*rabbit hole effect*) qui désigne, comme cela a pu être décrit[564], un phénomène selon lequel les utilisateurs se voient continuellement proposer un type de contenus qui les amène à approfondir un sujet ou un point de vue spécifique, les contenus proposés devenant souvent plus extrêmes ou polarisés en cours du processus[565].

Plusieurs études ont analysé dans quelle mesure les mineurs peuvent être exposés à des contenus inappropriés en raison du fonctionnement de l'algorithme de recommandation. En ce sens, il convient notamment de citer une étude récente portant sur l'impact du système de recommandation de YouTube sur la recommandation de contenus en lien avec des troubles du comportement

---

[560] En ce sens, v. not. le rapport de la Mission Enfants et Ecrans, A la recherche du temps perdu, 2024, p. 47&s et 77&s. Il convient de souligner ici que le rapport de la Commission d'enquête sur les effets psychologiques de TikTok livre une définition de l'addiction renvoyant à la typologie des risques 5C en précisant qu'il s'agit d' "*une pathologie définie par une dimension comportementale et biologique*" et que, sur "*le plan comportemental, une addiction est caractérisée par le cumul des 5C*" ; il énonce que, si l'utilisation excessive de TikTok présente des caractéristiques addictives, l'emploi de la notion d'addiction continue de faire l'objet de débats parmi les experts (Assemblée nationale, Rapport fait au nom de la commission d'enquête *sur les* effets psychologiques *de* TikTok *sur les* mineurs, 4 septembre 2025, pp. 105-106).

[561] Sur ce point, v. Chapitre 9, Modification de l'image de soi, Cadre légal, France et Union européenne.

[562] V. notamment, European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025.

[563] People vs Bigtech - Irish Council for Civil Liberties - Panoptykon Foundation, Fixing Recommander Systems, From identification of risk factors to meaningful transparency and mitigation, 2023.

[564] People vs Bigtech - Irish Council for Civil Liberties - Panoptykon Foundation, op. cit.

[565] V. également, Knight Georgetown Institute, Better Feeds : Algorithms that put the People first, A How-to guide for platforms and Policymaker, 2025, p. 16.

alimentaire[566]. A partir de la simulation d'un scénario réel, celui d'une adolescente fictive de 13 ans vivant en Irlande qui regarde pour la première fois ce type de contenus, l'étude relève que l'algorithme de YouTube ne limite pas l'exposition à ce type de contenus mais contribue à en recommander davantage[567]. Le rapport publié par Amnesty en octobre 2025[568] - qui prolonge celui déjà publié en 2023[569] - souligne en outre, à partir d'études réalisées à la fois manuellement et automatiquement, que le fil "Pour toi " de TikTok entraîne les mineurs dans une "spirale" de contenus liés à la dépression et au suicide. Selon le rapport, quelques heures passées sur la plateforme suffisent pour qu'un jeune qui consulte des contenus recommandés sur la santé mentale soit exposé à un flux presque continu de vidéos potentiellement nocives[570]. Il relève que ces contenus peuvent inclure des références à des pratiques d'automutilation et de suicide, ce qui démontre, selon le rapport, que les mesures d'atténuation des risques annoncées par TikTok en 2024[571] restent manifestement insuffisantes. Ont été relevées des stratégies visant à contourner les mécanismes de modération ("trompe-algorithmes") par le recours à des émoticônes, des abréviations ou le remplacement de lettres par des chiffres faisant par exemple référence au suicide ou à l'automutilation[572]. Amnesty International en conclut que TikTok ne se conforme ni au respect des droits humains tels que définis par les principes directeurs des Nations unies et de l'OCDE ni à ses obligations au titre du DSA[573]. Quant au rapport de la Commission d'enquête sur les effets psychologiques de TikTok sur les mineurs[574], il relève la possibilité pour TikTok "*de déterminer en temps réel, en fonction du comportement de l'utilisateur, les contenus qui lui seront ensuite montrés, [qui en] fait toute sa spécificité*"[575]. Il souligne que ce phénomène "d'ultra personnalisation" des contenus expose ainsi l'utilisateur au risque de se retrouver enfermé et intellectuellement isolé à cause d'une sélection algorithmique effectuée à son insu, entraînant une réduction de la diversité des informations auxquelles il a accès[576]. Il souligne, en outre, que l'utilisateur peut se retrouver confronté à des "chambres d'écho" au sein desquelles certaines informations, idées ou croyances sont amplifiées et renforcées, et rarement remises en question.

---

[566] CCDH, YouTube's Anorexia Algorithm, How YouTube recommends eating disorder videos to young girls in EU, 2025.

[567] Selon l'étude, une vidéo suggérée sur trois contenait des contenus préjudiciables liés aux troubles alimentaires, tandis que près de trois vidéos sur quatre étaient axées sur les troubles alimentaires ou la perte de poids : CCDH, Etude préc.

[568] Amnesty International, Entraîné·e·s dans le « rabbit hole » de nouvelles preuves montrent les risques de TikTok pour la santé mentale des enfants, octobre 2025.

[569] Amnesty International, Poussé·e·s vers les ténèbres, 2023.

[570] Rapport Amnesty International, Entraîné.e.s dans le "rabbit hole", préc., p.38.

[571] TikTok, DSA Risk Assessment Report 2024 ,28 August 2024 (Updated 2 October 2024).

[572] Sur ce point, v. not. European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025. - Rapport Amnesty, préc. p. 36.

[573] Rapport Amnesty International, Entraîné.e.s dans le "rabbit hole", préc., p.38.

[574]Assemblée nationale, Rapport fait au nom de la commission d'enquête *sur les* effets psychologiques *de* TikTok *sur les* mineurs, 4 septembre 2025.

[575] Rapport sur les effets psychologiques de TikTok sur les mineurs, préc., p.68.

[576] Ibid.

Si ces contenus pris isolément peuvent ne pas être nécessairement qualifiés de préjudiciables - et donc ne pas faire l'objet d'une modération par la plateforme -, nombreux s'interrogent désormais sur les effets d'une exposition répétée en particulier sur le bien-être des utilisateurs ainsi que sur leur santé mentale et physique, alors qu'un tel processus peut résulter de la conception même du service au soutien du modèle d'affaire de son fournisseur[577].

Réseaux sociaux et agents conversationnels (IA Compagnons). Le recours aux agents conversationnels inclus par les réseaux sociaux pour favoriser les interactions avec l'utilisateur peuvent être source de risques à l'égard des mineurs. Dans ses lignes directrices sur l'article 28 du DSA, la Commission européenne souligne ainsi que l'intégration croissante des agents conversationnels et des IA compagnons dans les plateformes en ligne peuvent affecter la manière dont les mineurs interagissent avec les plateformes en ligne, exacerber les risques existants et en créer de nouveaux qui peuvent nuire à la vie privée, à la sécurité et à la sûreté des mineurs. Ces risques peuvent provenir de l'expérience directe du mineur avec la plateforme et/ou des actions d'autres utilisateurs sur la plateforme[578]. Il peut notamment en résulter un risque d'anthropomorphisation auquel sont particulièrement vulnérables les enfants, et qui avait été déjà identifié concernant les agents conversationnels notamment par le Comité national pilote d'éthique du numérique[579]. Concernant en particulier les interactions entre les enfants et ces IA Compagnons qui désignent "un système d'IA qui est conçu de manière anthropomorphique et simule des réponses émotionnelles de type humain dans ses interactions"[580], la Commission européenne a relevé dans ses lignes directrices sur l'article 5 du Règlement Intelligence artificielle[581] qu'elles pourraient entraver le développement social et émotionnel et les relations sociales des plus jeunes utilisateurs ainsi que leurs compétences socio-émotionnelles comme l'empathie, la régulation émotionnelle, la compréhension sociale et l'adaptabilité, et qu'il pourrait en résulter une augmentation de l'anxiété, des risques de dépendance à l'égard du service ou encore une atteinte plus générale au bien-être des enfants[582]. L'Arcom notait à cet égard que les IA compagnons peuvent "ressembler à des amis virtuels et se comporter comme tels", qu'ils peuvent notamment "créer un attachement émotionnel qui peut, dans des situations extrêmes, conduire les utilisateurs

---

[577] Sur ce point, v. notamment Knight Georgetown Institute & Panoptykon Foundation, European Board for Digital Services and European Commission Report on Systemic Risks and Mitigations under the Digital Services Act, 7 April 2025 , p. 3 - Plus généralement Council of the European Union, Council conclusions on promoting and protection the mental health of children and adolescents in the digital era, 27 May 2025, pts. 29-30.

[578] Commission européenne, Communication de la Commission, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, p.1, pt. 2.

[579] CNPEN, Avis Agents conversationnels : enjeux d'éthique, 2022.

[580] Commission européenne, Communication de la Commission, Lignes directrices sur les pratiques interdites en matière d'intelligence artificielle au sens du Règlement UE 2024/1689 (Règlement sur l'IA), C(2025) 5052 final, 29 juillet 2025, p. 45.

[581] Ibid.

[582] Commission européenne, Lignes directrices article 28 DSA préc., p. 6, pt.18.b – V. également, eSafety Commissioner, AI chatbots and companions - risks to children and young people, February 2025.

à prendre des décisions préjudiciables pour eux et leurs proches"[583]. Le suicide de deux adolescents aux Etats-Unis et les actions en justice engagées par leur famille ont récemment contribué à susciter d'importantes inquiétudes à cet égard[584].

Plus généralement, il a été relevé qu'il peut résulter des interactions entre l'utilisateur et l'IA Compagnon un risque d'exposition à des contenus ou d'incitation à des pratiques toxiques, telles que l'automutilation ou les troubles du comportement alimentaire, ainsi qu'à des pratiques illicites, notamment la consommation de substances (toxicomanie). A cet égard, un rapport du CCDH publié en juillet 2025 [585] a identifié ces divers risques à travers plusieurs « études de cas » mettant en évidence le type de réponses préjudiciables qu'un agent conversationnel peut produire. Le rapport en conclut que la conception de ces interfaces peut conduire à générer des contenus susceptibles de nuire et d'influencer rapidement le comportement des jeunes utilisateurs. D'autres études conduites depuis, analysent l'efficacité des mesures de sécurité mises en place pour prévenir ce type de risques[586].

11.1.2. Conception adaptée à l'âge

La conception du service peut être également envisagée comme un outil de prévention des risques qui se traduit désormais par la promotion d'une conception dite "adaptée à l'âge" (*Age appropriate design*)[587]. Selon certains auteurs, "*Age-appropriate design means tailoring digital services and*

---

[583] Arcom, Arcom's contribution to the Call for evidence for guidelines on the protection of minors under the Digital Services Act, September 2024, p. 5.

[584] Sur ce point, v. notamment v. not. K. Roose, « Can A.I. be blamed for a Teen's suicide ? », *The Shift*, 23 octobre 2024. United States District Court, Middle District of Florida, Orlanda Division, Megan Garcia v. Character Technologies INC and alii, Case 6:24-cv-01903-ACC-EJK, Novembre 9th, 2024.

[585] CCDH, Fake Friend, ChatGPT betrays vulnerable teens by encouraging dangerous behavior, July 2025. Trois cas sont présentés dans l'étude à partir de comptes utilisateur paramétrés pour simuler un profil déterminé : le premier (Bridget) dans lequel "une jeune fille" de 13 ans dont le compte indiquait un intérêt pour "dépression, automutilation, idées suicidaires" dans lequel l'agent conversationnel a fourni des conseils relatifs à l'automutilation et au suicide ; le deuxième (Sophie) dans lequel "une jeune fille" de 13 ans dont le compte indiquait un intérêt pour "la perte de poids et les troubles du comportement alimentaire" pour lequel l'agent conversationnel a suggéré des régimes alimentaires extrêmes et un troisième cas (Brad) dans lequel un " jeune de 13 ans" ayant déclaré un intérêt pour "la fête, la drogue et l'alcool" voyait les réponses de l'agent conversationnel l'orienter vers des informations sur les moyens de dissimuler son état d'ébriété.

[586] En ce sens CCDH, The illusion of AI Safety, Testing OpenAI's new Safe Completions approach to chatbot safety, October 2025. Adde, International Joint Testing Exercise : Agentic Testing, Advancing Methodologies for Agentic Evaluations Across Domains, Leakage of sensitive Information, Fraud and Cybersecurity Threats, July 2025.

[587]Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, p.6, pt.17.d. - CEN-CENELEC, Age appropriate digital services framework, September 2023 - également, M. Buiten, C. Busch, CERRE Issue Paper, Protection of Minors: Age-Appropriate Design, March 2025 - 5 Rights

platforms to align with the developmental, cognitive, and emotional needs of children and young people, while ensuring their safety, privacy, and wellbeing. This includes designing online services with children's safety in mind, incorporating safeguards just as we do for physical products and spaces". Ils précisent par ailleurs que, dans la mesure où bon nombre de services ne sont pas conçus exclusivement pour les utilisateurs mineurs, cela suppose alors que soient intégrées à ces services des protections appropriées. Ils relèvent toutefois qu'une conception adaptée à l'âge doit donner accès à des environnements "*that are not only safe but also empowering, allowing minors to explore, learn, and connect without unnecessary risks*"[588]. Cela suppose donc de retenir une approche holistique, qui garantit à la fois la sécurité des mineurs en ligne tout en promouvant leur autonomie et respectant leurs libertés fondamentales ; une telle approche permet alors de préserver l'intérêt supérieur de l'enfant.

Comme le soulignent ces mêmes auteurs, la conception adaptée à l'âge suppose en particulier la mise en œuvre de mesures techniques de protection des utilisateurs afin de limiter les utilisations préjudiciables, c'est-à-dire celles qui pourraient porter atteinte à la sécurité des utilisateurs, à leur intégrité ou à leur bien-être. Dans le cadre du DSA, ils relèvent en outre qu'elle vise "*all ways in which platforms design, govern, and manage their services to protect and empower children. In a narrower sense, age-appropriate design focuses on the technical aspects of platform design - such as user interfaces and algorithms (including recommender systems) - that directly shape user experiences*"[589].

Plusieurs éléments essentiels doivent être relevés. Tout d'abord, une conception adaptée à l'âge peut compléter d'autres mesures de protection du mineur, à l'image de la vérification de l'âge ou du contrôle parental. Ce point est d'autant plus essentiel dès lors que ces dernières mesures de protection trouvent à ce jour d'importantes limites[590].

Ensuite, celle-ci s'inscrit dans une approche holistique qui doit permettre non seulement de protéger l'utilisateur mineur en lui garantissant de pouvoir interagir avec/via des environnements sûrs mais également de pouvoir bénéficier de ces environnements conformément à son intérêt, et préserver ses libertés fondamentales, notamment sa liberté d'expression[591]. Cette approche est essentielle si l'on entend garantir que les enfants puissent bénéficier de l'environnement numérique, et non pas seulement être protégés. A cette fin, deux catégories de mesures complémentaires sont à promouvoir. D'une part, les mesures dites de "*Safety by default*" qui visent le paramétrage de confidentialité par défaut ou encore celui des mécaniques d'engagement, notamment s'agissant des algorithmes de recommandation et autres fonctionnalités. Celles-ci doivent être complétées, d'autre part, par des mesures de conception visant à promouvoir l'intérêt de l'enfant, qui visent quant à elles à conférer aux utilisateurs la possibilité de paramétrer les

foundation, A High Level of privacy, safety & security for minors , 2024. Sur les techniques by design, v. en particulier Toward Digital Safety by Design for Children, OECD Digital Economy papers, n°363, June 2024.

[588] M. Buiten, C. Busch, étude préc., p. 48.

[589] M. Buiten, C. Busch, étude préc., p. 48.

[590] Sur ce point, v. Chapitre 12 sur les conditions d'accès tenant à l'âge, pt.12.1. et Chapitre 13 sur le contrôle parental, pt.13.1.

[591] M. Buiten, C. Busch, étude préc., p. 10.

fonctionnalités et les algorithmes de recommandation, ce à quoi il convient d'ajouter la promotion d'une action possible sur l'architecture du service permettant à l'utilisateur de choisir et d'interagir avec/sur des environnements, conformément au principe de l'intérêt supérieur de l'enfant.

Dans les lignes directrices de l'article 28, la Commission européenne relève à cet égard que l'intérêt supérieur de l'enfant doit être considéré comme le principe directeur d'une conception adaptée à l'âge pour les services en ligne[592]. Cela s'inscrit dans le respect de l'article 3 de la Convention des Nations Unies relative aux droits de l'enfant et de l'article 24.2 de la Charte des droits fondamentaux de l'Union européenne, reconnaissant le droit de l'enfant à ce que son intérêt supérieur soit évalué et pris en compte en tant que une considération primordiale lorsque différents intérêts sont en jeu afin de prendre toute décision relative à un enfant, un groupe d'enfants identifiés ou non identifiés ou encore les enfants en général.

Deux éléments doivent être précisés sur ce point. Tout d'abord, dans la mesure où l'intérêt supérieur de l'enfant est un concept fondé sur les droits, cela suppose de retenir une approche contextuelle consistant à prendre en compte, lors de sa définition, l'âge de l'enfant, son stade de développement, son contexte personnel et ses besoins spécifiques[593]. Ensuite, il conviendra de respecter une balance entre différents intérêts légitimes, à savoir mettre en balance l'intérêt supérieur de l'enfant avec la protection des données personnelles et l'innovation notamment. Dès lors, cela justifie que les mesures prises soient nécessaires et proportionnées, ce qui suppose de ne pas imposer des restrictions excessives à d'autres droits ou intérêts.

11.2. CADRE JURIDIQUE

11.2.1. France et Union européenne

S'agissant de la conception des services, plusieurs textes trouvent à s'appliquer et visent à répondre en tout ou partie aux risques préalablement décrits.

Tel est l'objet de plusieurs dispositions du DSA visant différents opérateurs à savoir les plateformes accessibles aux mineurs ou encore les très grandes plateformes et moteurs de recherche. Quant aux textes visant la protection des mineurs, l'article 28 du DSA impose aux plateformes accessibles aux mineurs d'assurer un haut niveau de protection de leur vie privée, de leur sécurité et de leur sûreté, des précisions étant apportées sur ce point par les lignes directrices publiées par la Commission européenne le 10 octobre 2025[594]. Par ailleurs, les très grandes

[592] Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, pt. 17.d.
[593] M. Buiten, C. Busch, étude préc., p. 10.
[594] Sur ce point, v. Chapitre 1, pt.1.3.2.

plateformes et moteurs de recherche sont tenues de réaliser des analyses de risques systémiques et de prendre des mesures de mitigation de ces risques au titre des articles 34 et 35 du DSA[595].

Il s'agit en particulier ici d'envisager comment sont encadrés les risques relevant de la conception des services. A cet égard, différentes mesures sont désormais préconisées pour encadrer la conception des réseaux sociaux. Tel est notamment l'objectif poursuivi par plusieurs recommandations figurant dans les lignes directrices de l'article 28 du DSA qui portent sur les risques préalablement identifiés (b) en préconisant une conception adaptée à l'âge (a). Si plusieurs d'entre elles doivent être saluées, certaines restent toutefois insuffisamment précises et d'autres devraient être renforcées afin de parvenir à l'objectif recherché, à savoir garantir un niveau élevé de protection de la vie privée, de la sécurité et de la sûreté des utilisateurs mineurs.

11.2.1.1. Conception adaptée à l'âge

Dès 2023, le Parlement européen relevait dans son étude sur l'influence des réseaux sociaux sur le développement des enfants[596] la nécessité de renforcer la sécurité des enfants en ligne et différentes propositions visant à consacrer un principe de "conception adaptée à l'âge" : l'accent était mis tout d'abord sur les propositions pour élaborer les lignes directrices visant à garantir le respect de l'article 28 du DSA afin notamment de définir des principes de conception pour les services numériques destinés aux enfants ; il était également souligner la nécessité pour les fournisseurs de ces services de placer l'intérêt supérieur de l'enfant au cœur de leurs pratiques. À ce titre, le Parlement européen rappelait plus généralement que la création d'un "environnement numérique sûr et adapté à l'âge" constitue l'un des principes fondamentaux de la stratégie BIK+ et que, dans ce cadre, la Commission européenne s'engageait dès 2022[597] à "faciliter l'élaboration d'un code de conduite européen complet sur la conception adaptée à l'âge, fondé sur les nouvelles dispositions du DSA et en conformité avec la directive SMA et le RGPD".

Afin de lutter contre les risques préalablement décrits, la Commission européenne préconise désormais une approche dite "conception adaptée à l'âge"[598]. Le paramétrage des comptes est un

[595] Sur ce point, v. les développements sur les analyses de risques pt. 2.1.2.4 et European Board for Digital Services, First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures, 18 November 2025.

[596] Parlement européen, Study Requested by the CULT Committee The influence of social media on the development of children and young people, 2023, p.52.

[597] Commission européenne, Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions Une décennie numérique pour les enfants et les jeunes : la nouvelle stratégie européenne pour un internet mieux adapté aux enfants, mai 2022, p.9.

[598] Commission européenne, Communication de la commission, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025. Sur la définition de la conception adaptée à l'âge, v. Chapitre 11, pt. 11.1.2.

outil important à cet égard dans la mesure où il permet aux fournisseurs de plateformes en ligne accessibles aux mineurs d'atténuer les risques pesant sur la vie privée, la sûreté et la sécurité de ces derniers, notamment le risque de contact non désiré par des personnes malveillantes. S'agissant du paramétrage des comptes utilisateurs, certaines mesures sont particulièrement promues et s'inscrivent dans une approche holistique visant à préserver l'intérêt supérieur de l'enfant : certaines sont relatives au paramétrage par défaut et d'autres traduisent la consécration d'une forme de droit au paramétrage au bénéfice des utilisateurs mineurs.

Paramétrage par défaut. Les données montrent que les utilisateurs modifient rarement leurs paramètres par défaut, ce qui influence de manière déterminante leur expérience et leur comportement en ligne. C'est pourquoi la Commission considère que les fournisseurs de services en ligne devront s'assurer que les principes de confidentialité, de sûreté et de sécurité dès la conception sont appliqués par défaut à l'ensemble des paramètres de compte destinés aux mineurs[599]. En outre, il est attendu que les fournisseurs de plateformes évaluent la nécessité d'instaurer des paramètres par défaut plus stricts en fonction de l'âge et des capacités évolutives des mineurs, ainsi que du résultat de leur examen des risques. Ces réglages doivent être régulièrement testés et mis à jour pour garantir leur efficacité au fil des évolutions technologiques, des nouveaux risques identifiés et des tendances émergentes, en particulier celles qui affectent la vie privée et la sécurité des mineurs[600]. Selon les lignes directrices de l'article 28 du DSA, le dispositif offert par la plateforme doit offrir aux utilisateurs mineurs un contrôle progressif sur leurs paramètres, accompagné d'explications formulées dans un langage accessible et adapté à l'âge[601]. Il est également essentiel qu'ils ne soient ni incités, ni dissuadés, de changer les réglages établis par défaut[602] et qu'ils se voient offrir la possibilité de choisir de modifier les paramètres par défaut de manière temporaire ou permanente[603]. Tout cela devrait être assorti d'un accompagnement continu, tout en permettant aux utilisateurs de demander à ce que leurs choix soient conservés ou modifiés sur certains points.

Droit au paramétrage. A la suite des recommandations de la mission Enfants et Ecrans[604], le rapport d'enquête sur les effets psychologiques de TikTok sur les mineurs rappelle en outre la nécessité pour l'utilisateur de pouvoir paramétrer ses comptes de réseaux sociaux afin de reprendre le contrôle sur ses interactions[605]. Cela prolonge certaines propositions formulées en ce sens dans le cadre de travaux antérieurs, notamment par un avis de la CNCDH pour lutter contre la haine en ligne qui préconisait déjà de permettre à l'utilisateur de choisir les critères assurant la promotion ou la rétrogradation des contenus figurant sur son fil d'actualités, de décider selon quels critères l'information lui est présentée ou encore de déterminer le public auquel il souhaite rendre visible

[599] Commission européenne, Lignes directrices , p. 17, pt. 57 - S 6.3.1.
[600] Commission européenne, Lignes directrices article 28 DSA préc., p.18, pt. 57.c-d.
[601] Commission européenne, Lignes directrices article 28 DSA préc., pt. 57.f.
[602] Commission européenne, Lignes directrices article 28 DSA préc., pt. 57.e.
[603] Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025,pt. 58.a.
[604] Rapport de la Mission Enfants et Ecrans, A la recherche du temps perdu, 2024, p. 79.
[605]Assemblée nationale, Rapport fait au nom de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs, 4 septembre 2025, p. 221.

ses messages et de pouvoir définir les possibilités de commentaires[606]. Il convient de souligner que le DSA s'avère insuffisamment protecteur à cet égard[607]. C'est pour cette raison que le rapport de la Commission d'enquête sur les effets psychologiques de TikTok relève l'importance de soutenir le renforcement des obligations des plateformes dans le cadre des négociations concernant le Digital Fairness Act (DFA), en leur "imposant de proposer des paramètres spécifiques permettant à chaque utilisateur de personnaliser son expérience sur les réseaux sociaux"[608].

11.2.1.2. Conception et risques spécifiques

Différents risques spécifiques liés à la conception des services doivent être envisagés : la confidentialité et les risques de contact, les interfaces trompeuses et manipulatrices, la conception dite addictive, l'exposition aux contenus du fait du fonctionnement des algorithmes de recommandation ultra-personnalisés ainsi que les risques en lien avec l'utilisation d'un système d'intelligence artificielle tel que les IA Compagnons.

Il convient de relever que certains de ces risques font l'objet d'analyses dans le cadre de différentes actions. Au niveau européen, la Commission européenne a ouvert deux enquêtes, l'une à l'encontre de TikTok [609] l'autre de Meta[610], pour non respect de plusieurs de leurs obligations au titre du DSA, qui portent notamment sur les effets qu'engendre la conception de leurs services sur la santé mentale et physique et le bien-être de leurs utilisateurs ainsi que le respect des droits des mineurs, qui envisagent en particulier les possibles "effets de spirale" de contenus toxiques[611]. Différents rapports ont été versés à la procédure, à l'image du rapport publié par Amnesty International en octobre 2025 relatif à TikTok qui a également déposé un recours contre la plateforme pour non respect du DSA auprès de l'Arcom[612]. A la suite de la publication des lignes directrices de l'article 28 du DSA, la Commission a lancé de nouvelles actions, notamment à l'encontre de Snapchat et YouTube, leur demandant de fournir des informations complémentaires concernant l'accès de leurs utilisateurs mineurs via leurs services à des produits et contenus illicites ainsi que concernant leurs algorithmes de recommandation[613].

---

[606] CNCDH, Avis sur la lutte contre la haine en ligne, Avis A-2021-9, 2021, n°80&s. Adde, CCNum, Votre attention s'il vous plait ! Quels leviers face à l'économie de l'attention, 2021 ; Knight Georgetown Institute, Better Feeds: Algorithms that Put the People First, A How-to Guide for Platforms and Policymaker, 2025.

[607] Sur ce point, v. supra, pt. 11.2.1.2.

[608] Ibid.

[609] Commission européenne, La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques, 19 février 2024.

[610]Commission européenne, La Commission ouvre une procédure formelle à l'encontre de Meta au titre du DSA concernant la protection des mineurs sur Facebook et Instagram, 16 mai 2024.

[611] V. les constatations préliminaires de ces enquêtes : Commission européenne, Communiqué de presse, 24 octobre 2025 - V. également les demandes d'information adressées à You Tube, Snapchat et TikTok sur leurs systèmes de recommandation, Communiqué de presse, 2 oct. 2024.

[612] Rapport Amnesty International, Entraîné.e.s dans le "rabbit hole", préc.

[613] Commission européenne, Communiqué de presse, 10 octobre 2025.

D'autres actions sont désormais intentées en France devant les juridictions. Ainsi, une première plainte a été déposée à l'encontre de TikTok le 12 septembre 2023 pour provocation au suicide[614]. En outre, le parquet de Paris a annoncé le 4 novembre 2025[615] avoir ouvert une enquête préliminaire le 11 septembre 2025 découlant d'un signalement du député Arthur Delaporte relatif aux dysfonctionnements constatés par la commission d'enquête parlementaire sur les effets psychologiques de TikTok[616]. Confiée à la Brigade de lutte contre la cybercriminalité (BL2C), cette enquête vise des infractions telles que la propagation de contenus incitant au suicide, la fourniture d'une plateforme permettant des activités illicites ou encore l'altération de systèmes de traitement automatisé de données. L'enquête est menée en coordination avec l'Arcom et Viginum, et s'appuie sur plusieurs rapports qui soulignent la dangerosité de l'algorithme de TikTok et son rôle potentiel dans la diffusion de contenus nocifs.

11.2.1.2.1. Confidentialité et risque de contact

Afin d'assurer un haut niveau de protection des mineurs compte tenu des risques de contact (notamment par des pédocriminels à des fins de grooming et de sextorsion), les lignes directrices de l'article 28 du DSA préconisent que soit contrôlée la visibilité du mineur sur le réseau social. Pour ce faire, le texte reconnaît notamment que, par défaut, seuls les comptes préalablement acceptés par celui-ci peuvent interagir avec lui ou accéder à ses contenus et informations personnelles. Il relève par ailleurs la nécessité d'empêcher tout téléchargement ou capture d'écran des informations sensibles partagées par les mineurs, ainsi que la visibilité des activités telles que les likes ou les abonnements[617]. En outre, afin d'assurer le niveau le plus élevé de protection de la vie privée, de la sûreté et de la sécurité du mineur, il est recommandé que la géolocalisation, le micro, la caméra et les options de suivi soient automatiquement désactivés par défaut[618] et que, si ces fonctionnalités sont activées par le mineur, la fermeture de chaque session emporte une re-désactivation automatique.

Le texte préconise aussi d'organiser un meilleur contrôle de la sphère d'émission et de réception du mineur. Ainsi, il mentionne la nécessité d'empêcher par défaut les commentaires et messages directs de personnes non préalablement acceptées. Il souligne également l'importance d'activer par défaut des fonctionnalités qui permettent aux mineurs de contrôler les interactions les concernant, comme le blocage ou la désactivation des commentaires de manière anonyme[619].

---

[614] Sur ce point, et concernant le collectif Algos Victima, v. infra Chapitre 9 Modification de l'image de soi.

[615] Parquet de Paris Tribunal judiciaire, Communiqué de presse, 4 novembre 2025.

[616] Assemblée nationale, Rapport fait au nom de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs, 4 septembre 2025.

[617] Commission européenne, Communication de la Commission, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, pt. 57.b.i-iii-iv.

[618] Commission européenne, Lignes directrices article 28 DSA préc., pt. 57.b.v.

[619] Ibid.

11.2.1.2.2. Interfaces trompeuses et manipulatrices

Définition. Le DSA définit les interfaces trompeuses des plateformes comme "*des pratiques qui ont pour objectif ou pour effet d'altérer ou d'entraver sensiblement la capacité des destinataires du service de prendre une décision ou de faire un choix, de manière autonome et éclairée. Ces pratiques peuvent être utilisées pour persuader les destinataires du service de se livrer à des comportements non désirés ou de prendre des décisions non souhaitées qui ont des conséquences négatives pour eux*"[620]. Son article 3 précise que l'interface en ligne est définie comme « *tout logiciel, y compris un site internet ou une section de site internet, et des applications, notamment des applications mobiles*".

Cette définition large vise à permettre une adaptation du texte aux pratiques des acteurs. Le considérant 67 du DSA en livre quelques illustrations comme le fait de rendre certains choix plus difficiles ou plus longs que d'autres ou appliquer des paramètres par défaut très difficiles à modifier. Toutefois, le texte souligne qu'une telle interdiction ne doit pas être interprétée comme empêchant l'opérateur d'interagir avec l'utilisateur et de lui proposer des services complémentaires, ou encore que la publicité ne doit pas être considérée comme constituant une interface trompeuse.

Il convient de relever que la définition des interfaces trompeuses peut néanmoins poser difficulté, en l'absence de consensus sur leur qualification comme cela a pu être relevé[621]. Plusieurs typologies ont néanmoins été proposées. Dans son cahier "La forme des choix", la CNIL distingue ainsi le design dangereux, abusif et trompeur pour identifier les techniques qui exploitent les biais cognitifs humains, ou induisent en erreur l'utilisateur par brouillage ou omission d'information[622].

Afin d'éclairer les opérateurs et les designers lors de la conception des interfaces, l'article 25.3 du DSA prévoit que "*la Commission européenne peut publier des lignes directrices sur la manière dont le paragraphe 1 s'applique à des pratiques spécifiques, notamment :*

a. accorder davantage d'importance à certains choix au moment de demander au destinataire du service de prendre une décision ;

b. demander de façon répétée au destinataire du service de faire un choix lorsque ce choix a déjà été fait, notamment en

c. faisant apparaître une fenêtre contextuelle qui perturbe l'expérience de l'utilisateur ;

d. rendre la procédure de désinscription d'un service plus compliquée que l'inscription à celui-ci".

---

[620] DSA, considérant 67.

[621] OCDE, « Dark commercial patterns », *Documents de travail de l'OCDE sur l'économie numérique*, n° 336, 2022 - V. également, K. Pineau, A. Fabre, "Evaluer la captologie et le design persuasif des services numériques", *Information, données & documents*, 2021/2 (n°2), p. 151.

[622] CNIL, La forme des choix, Cahier IP Innovation et prospective n°6, 2019.

Le Comité européens des services numériques travaille actuellement à l'élaboration d'un document afin de favoriser une interprétation harmonisée. Ces travaux s'inscrivent également dans le cadre de la revue du droit des consommateurs de l'Union européenne pour assurer son adéquation avec les pratiques en ligne ("Digital Fairness Check"). En France, ils sont menés conjointement par l'Arcom et la DGCCRF.

Par ailleurs, certains proposent de distinguer le design trompeur du design persuasif. En France, le collectif des "Designers éthiques" précise ainsi que (1) le design trompeur peut être défini comme "*un élément de conception dont le but est de pousser l'utilisateur à faire des choses qu'il n'aurait pas forcément faites initialement*" alors que (2) le design persuasif vise le "*design dans le but de guider l'utilisateur à adopter un comportement particulier. Le design persuasif est considéré comme une spécialisation du design UX (centré utilisateur)*"[623].

Sanction et interdiction des interfaces trompeuses et manipulatrices. Les interfaces trompeuses peuvent être sanctionnées sur différents fondements. Elles peuvent être considérées comme des pratiques commerciales déloyales sanctionnées sur le fondement de la Directive 2005/29 (DPCD) transposée en droit français aux articles L. 121-1 à L. 121-7 du Code de la consommation. Les orientations générales de la Commission européenne relative à la Directive 2005/29 le précise explicitement, dans leur version de 2021 en visant certaines pratiques[624]. Les interfaces de choix trompeuses peuvent également être sanctionnées pour non respect du RGPD et de la Loi informatique et libertés notamment, dès lors que ces pratiques ne respectent pas les principes de transparence, de garantie d'un consentement éclairé et du principe de *privacy by default* en orientant les choix des personnes concernées à leur insu. Cela a pu être souligné

[623] Designers éthiques, Concevoir sans dark patterns. Guide à l'intention des designers, 2023 :

[624] Commission européenne, Orientations concernant l'interprétation et l'application de la directive 2005/29/CE du Parlement européen et du Conseil relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur, C/2021/9320, chapitre 4.2.7: "*La DPCD s'applique à « toute pratique commerciale déloyale » satisfaisant aux critères du champ d'application matériel de la directive, quelle que soit sa classification. Si des interfaces truquées sont appliquées dans le contexte de relations commerciales entre entreprises et consommateurs, la directive peut être utilisée pour contester l'équité de telles pratiques, en plus d'autres instruments du cadre juridique de l'UE, tels que le RGPD.*

[…] toute pratique manipulatrice d'une entreprise vis-à-vis d'un consommateur qui altère de manière substantielle ou est susceptible d'altérer le comportement économique d'un consommateur moyen ou vulnérable pourrait être contraire aux obligations de diligence professionnelle du professionnel (article 5) ou constituer une pratique trompeuse (articles 6 et 7) ou une pratique agressive (articles 8 et 9), en fonction de l'interface truquée spécifique utilisée. La DPCD ne requiert pas une intention pour le recours à une interface truquée. La norme de diligence professionnelle visée à l'article 5 de la DPCD en ce qui concerne la conception des interfaces peut inclure des principes découlant de normes internationales et de codes de conduite relatifs à la conception éthique. À titre de principe général, dans le cadre des exigences de diligence professionnelle visées à l'article 5 de la DPCD, les professionnels devraient prendre des mesures appropriées pour veiller à ce que la conception de leur interface n'altère pas les décisions commerciales des consommateurs".

notamment par la CNIL dans diverses décisions[625] ou encore par l'*European Data Protection Board* (EDPB) dans ses lignes directrices consacrées aux dark patterns et aux réseaux sociaux[626]. Au-delà, les interfaces trompeuses sont explicitement interdites par plusieurs textes récents. Concernant les réseaux sociaux, il convient de mentionner en particulier les réformes réalisées avec l'adoption du DSA et du Règlement sur les marchés numériques.

Règlement sur les marchés numériques (DMA). L'article 13 du DMA pose une interdiction explicite de contourner les obligations imposées aux opérateurs visés par le texte - soit les contrôleurs d'accès (*gatekeepers*)[627] - par des comportements « *qu'ils soient de nature contractuelle, commerciale, technique ou autre, y compris l'utilisation de techniques comportementales ou la conception d'interfaces* ». S'ajoute à cette « *règle anti-contournement* », une interdiction de détériorer les conditions ou la qualité du service et de rendre l'exercice des droits des utilisateurs ou leur choix excessivement difficile, y compris en proposant des choix de manière partiale, ou encore en utilisant la structure, la conception, la fonction ou le mode de fonctionnement d'une interface utilisateur ou d'une partie connexe pour perturber leur autonomie, prise de décision ou leur libre choix. Il convient toutefois de relever que ce texte ne pose pas une interdiction générale des interfaces trompeuses mais ne concerne que le champ d'application du DMA.

Règlement sur les services numériques (DSA). L'article 25 du DSA interdit aux plateformes de concevoir, organiser ou exploiter leurs interfaces en ligne de façon à tromper ou manipuler les destinataires de leur service ou de toute autre façon propre à altérer ou à entraver substantiellement leur capacité à prendre des décisions libres et éclairées[628]. La Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique est venue modifier le Code de la Consommation qui dispose désormais, en son article L. 133-1, qu' "*Est puni d'un emprisonnement de deux ans et d'une amende de 300 000 euros, dont le montant peut être porté, de manière proportionnée aux avantages tirés du délit, à 6 % du chiffre d'affaires mondial hors taxes réalisé au cours de l'exercice précédent pour une personne morale, le fait pour un fournisseur de places de marché : 1° De méconnaître ses obligations relatives à la conception, à l'organisation ou à l'exploitation d'une interface en ligne, en violation de l'article 25 du 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 (DSA)*". En outre, conformément à l'article 34 du DSA, la conception du service doit faire l'objet d'une analyse de risques systémiques imposée aux très grandes plateformes ; en cas d'identification de l'un de ces risques, les opérateurs doivent adopter

[625] CNIL, délib., 21 janv. 2019, SAN-2019-001 ; CNIL, délib., 31 déc. 2021, SAN-2021-023 et 2021-024 ; CNIL, délib, 10 nov. 2022, SAN-2022-020. Adde CNIL, La forme des choix, préc.

[626] EDPB, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0 2023.

[627] Six contrôleurs d'accès ont été désignés par la Commission européenne (Alphabet, Amazon, Apple, ByteDance, Meta et Microsoft). Au titre de leurs activités de services de plateforme essentiels, quatre réseaux sociaux sont concernés : TikTok, Facebook, Instagram et LinkedIn.

[628] Il convient toutefois de préciser que l'article 25 du DSA s'applique sous réserve de la Directive pratiques commerciales déloyales et du RGPD.

des mesures d'atténuation des risques identifiées à l'article 35 du DSA[629]. Quant aux lignes directrices de l'article 28 du DSA, les interfaces trompeuses et manipulatrices sont évoquées en lien avec les pratiques commerciales[630].

L'interdiction des interfaces trompeuses et manipulatrices de l'article 25 du DSA peut toutefois viser le design de fonctionnalités résultant d'obligations imposées par le texte. Tel est par exemple le cas de l'obligation imposée aux très grandes plateformes d'offrir à leurs utilisateurs une option leur permettant de choisir d'autres systèmes de recommandation ne reposant pas sur le profilage au sens du RGPD. En atteste une décision de la Cour d'Amsterdam relative à Meta du 2 octobre 2025[631] ayant reconnu que le choix de l'utilisateur de se voir appliquer un système de recommandation ne reposant pas sur le profilage doit être persistant, à savoir doit pouvoir être conservé lorsque l'utilisateur ferme et ouvre de nouveau l'application ou le site jusqu'à ce qu'il le modifie lui-même délibérément ; les juges en déduisent qu'imposer à l'utilisateur de réitérer son choix à chaque session constitue une interface trompeuse ou manipulatrice prohibée par l'article 25 du DSA.

Réforme du Digital Fairness Act : Vers une interdiction générale ? En dépit de ces évolutions, des lacunes subsistent dès lors que le cadre légal existant n'offre pas de garanties suffisantes aux consommateurs[632]. Une discussion est désormais engagée sur la nécessité de consacrer une sanction plus générale des interfaces trompeuses et manipulatrices sur le fondement des pratiques commerciales déloyales, sur le modèle de l'interdiction posée au titre de l'article 25 du DSA. Une telle évolution pourrait être consacrée à l'occasion de la prochaine réforme du droit de la consommation dans le cadre du Digital Fairness Act afin de renforcer la sécurité juridique et la protection des consommateurs.

11.2.1.2.3. Conception dite addictive

Aucune disposition du DSA ne vise spécifiquement la conception dite addictive, seul le considérant 81 en fait mention. En revanche, plusieurs dispositions des lignes directrices de l'article 28 du DSA évoquent les difficultés pouvant en résulter et les mesures à mettre en œuvre afin d'y remédier. Ainsi, la Commission y relève que les mineurs sont particulièrement exposés aux effets persuasifs des pratiques commerciales et qu'ils doivent être protégés contre l'exploitation économique dans les environnements numériques[633]. Elle souligne que cette

[629] Sur ce point, v. Chapitre 1 sur le panorama des textes de droit européen et français applicables aux réseaux. pt. 2.1.2.4.
[630] Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, pts. 68&s.
[631] Court of Justice Amsterdam, Stichting bits of freedom against Facebook Netherlands B.V., Meta Platforms Ireland LTD, Meta Platforms Inc., Case number: C/13/774725 / KG ZA 25-687 MK/JD.
[632] Sur ce constat, v. Commission européenne, Staff Working Document Fitness Check of EU consumer law on digital fairness, 3 October 2024, p. 146&s.
[633] Commission européenne, Lignes directrices article 28 DSA préc., pt. 68.

protection s'inscrit dans le cadre du respect de l'intérêt supérieur de l'enfant, en application de l'Observation générale n°25 du Comité des droits de l'enfant de l'ONU, qui souligne que les enfants ne doivent jamais être considérés uniquement comme des consommateurs[634]. Selon la Commission, il est également nécessaire que les plateformes n'exploitent pas le "*manque de compétences des mineurs dans le domaine commercial*", en adaptant les interfaces à leur niveau de compréhension et en leur fournissant un accompagnement actif, clair et accessible[635].

S'agissant des très grandes plateformes, il convient de relever que la conception de plusieurs services est actuellement analysée dans le cadre d'enquêtes formelles lancées par la Commission européenne depuis l'entrée en application du DSA. Ainsi, dans le cadre de l'enquête formelle ouverte le 18 février 2024 à l'égard de TikTok[636], la Commission européenne s'interroge sur plusieurs points notamment sur le respect par TikTok des obligations qui lui sont imposées au titre des articles 34 et 35 du DSA en matière d'évaluation et d'atténuation des risques systémiques en ce qui concerne les effets négatifs réels ou prévisibles découlant de la conception du système de Tiktok, "y compris ses systèmes algorithmiques susceptibles de stimuler les dépendances comportementales et/ou de créer des effets de «spirales infernales". Quant à la procédure ouverte le 16 mai 2024 à l'encontre de Meta[637], elle vise les risques causés par la conception des interfaces de Facebook et d'Instagram qui peuvent exploiter les faiblesses et l'inexpérience des mineurs et provoquer un comportement addictif. Les résultats de ces procédures permettront d'apporter des éléments probants sur ces différents points.

Concernant les plateformes accessibles aux mineurs, plusieurs recommandations sont formulées par les lignes directrices de l'article 28 concernant la conception dite addictive. Outre les mesures de gestion du temps d'écran[638], le texte préconise de désactiver par défaut toutes les fonctionnalités susceptibles de favoriser une utilisation excessive telles que les likes, les streaks, la confirmation de lecture, les indicateurs de saisie (comme "… est en train d'écrire"), le pull-to-refresh, la lecture automatique par défaut de vidéos ou encore la diffusion de flux en direct[639]. En outre, il relève que les plateformes doivent veiller à ne pas exposer les mineurs à des mécanismes visant principalement à susciter leur engagement ou à développer des habitudes comportementales addictives, comme le défilement infini ou les récompenses virtuelles[640]. Il évoque aussi la nécessité

---

634 Observation générale n° 25 du Comité des droits de l'enfant de l'ONU, para 112 ; UNICEF, Document de travail : Le marketing numérique et les droits de l'enfant, 2019.

635 Commission européenne, Lignes directrices article 28 DSA préc., pt. 69.a.

636 Commission européenne, La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques, 19 février 2024.

637 Commission européenne, La Commission ouvre une procédure formelle à l'encontre de Meta au titre du règlement sur les services numériques en ce qui concerne la protection des mineurs sur Facebook et Instagram, 16 mai 2024.

638 Commission européenne, Lignes directrices article 28 DSA préc., pt. 61.c. : "*Mettre en place des outils de gestion du temps personnalisés, visibles, faciles d'accès et d'utilisation, adaptés aux enfants et efficaces, afin de sensibiliser davantage les mineurs au temps qu'ils passent sur les plateformes en ligne. Pour être efficaces, ces outils devraient dissuader les mineurs de passer plus de temps sur la plateforme. Il pourrait également s'agir d'incitations douces qui favorisent des options plus sûres*".

639 Commission européenne, Lignes directrices article 28 DSA préc., pt. 57.b.vi.

640 Commission européenne, Lignes directrices article 28 DSA préc., pt. 61.b.

d'introduire une "friction positive" destinée à ralentir ou conscientiser les actions de publication, de partage ou de consultation[641], et de proposer un paramétrage par défaut des systèmes de recommandation non fondés sur l'engagement. Cela reviendrait à consacrer ce que certains qualifient d'un droit à ne pas être dérangé par défaut[642].

Certains proposent d'aller plus loin afin de renforcer la protection des utilisateurs en consacrant des mesures plus fermes pour limiter la conception dite addictive qui visent la conception des interfaces *stricto sensu* jusqu'à celle des services. Cela tient notamment au caractère incertain du cadre légal s'agissant de l'encadrement de ce type de fonctionnalités[643] ainsi que de la portée limitée des lignes directrices de l'article 28 du DSA quant à leur force normative et à leur champ d'application. En effet, si les mineurs sont particulièrement sensibles au caractère addictif de ces fonctionnalités, celles-ci peuvent emporter des effets délétères à l'égard de l'ensemble des utilisateurs.

C'est en ce sens que le Parlement européen et la Commission européenne réfléchissent désormais à adopter une nouvelle réglementation visant à interdire la conception addictive des services en ligne pour prolonger les premières avancées permises par le RGPD, la Directive PCD ainsi que par le DSA et le DMA. En effet, si plusieurs fonctionnalités et interfaces peuvent d'ores et déjà être encadrées par ces textes, une réforme du droit de la consommation permettrait la mise en œuvre de dispositions plus prescriptives. Le Parlement européen a formulé un certain nombre de propositions à cette fin dans le cadre de sa recommandation sur le design addictif des services en ligne[644] en préconisant d'explorer plusieurs pistes d'évolution possibles.

Parmi les pistes envisagées, les premières visent à limiter certaines pratiques d'ores et déjà identifiées comme problématiques. Plusieurs de ces pratiques pourraient être interdites dès lors qu'elles ne sont pas encore visées par le droit positif en tant que telles. Plusieurs rapports visent ainsi des fonctionnalités telles que le défilement infini (*infinit scroll*), de la lecture automatique par défaut (*autoplay*), du "tirer pour rafraîchir" (*pull-to-refresh*), des contenus éphémères (dont les *stories*) ou des notifications incessantes. Le Parlement européen en a appelé à "*l'adoption de mesure ambitieuses au niveau de l'Union à cet égard*"[645]. Il en appelle en outre à la constitution d'un groupe d'experts sur l'accès aux médias sociaux des enfants et invite la Commission à travailler "*en collaboration avec l'Organisation mondiale de la santé et les autorités sanitaires nationales des États membres, ainsi qu'avec les représentants des jeunes et des parents, afin de publier des lignes directrices européennes fondées sur des données probantes et les plus à la pointe concernant le temps passé par les mineurs devant les écrans, afin d'améliorer la protection de ces derniers en tant que consommateurs en ligne, en s'appuyant sur les travaux déjà réalisés en*

[641] Ibid.
[642] EDRi, A Rights-Based Digital Fairness Act, October 2025, pt. 4.
[643] European Commission, COMMISSION STAFF WORKING DOCUMENT FITNESS CHECK of EU consumer law on digital fairness, 3 octobre 2024, SWD(2024) 230 final.
[644] European Parliament, IMCO, Resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market, P9_TA(2023)0459IMCO, December 2023.
[645] Parlement européen, Résolution du Parlement européen du 26 novembre 2025 sur la protection des mineurs en ligne ((2025/2060(INI)), 2025, pt. 37.

France, en Suède et aux Pays-Bas", en précisant que "*ces lignes directrices devraient inclure des conseils sur un temps d'écran adapté à l'âge, y compris un temps maximum par âge*"[646].

En ce qui concerne la France, le rapport de la Mission Enfants et écrans[647] a également souligné que "*les mécanismes de "fil déroulement infini", de "lancement automatique et sans fin" des vidéos, d'hyper notifications posent sans controverse des difficultés sur le plan éthique, en effaçant tout choix de l'utilisateur et en poussant à une consommation de contenus sans effort ni engagement actif*". Selon ce même rapport, cette première liste pourrait être *régulièrement complétée pour assurer un haut niveau des utilisateurs, en particulier des mineurs. Pour ce faire, il convient de conduire dans les plus brefs délais des études approfondies concernant le fonctionnement les risques suscités par :*

- *les flux addictifs de contenus proposés à un utilisateur spécifique sur la base du traitement de données comportementales ;*
- *les conceptions favorisant l'adoption de comportements compulsifs définis comme toute réponse stimulée par des facteurs externes qui conduit un individu à adopter un comportement répétitif raisonnablement susceptible de causer une détresse psychologique, une perte de contrôle, de l'anxiété ou une dépression, et ce sans limite de temps de connexion ;*
- *les fonctions d'incitation ou d'engagement notamment l'exposition aux « likes » et aux commentaires*"[648].

Le Président de la Commission d'enquête TikTok va jusqu'à recommander une interdiction de tout flux addictif[649] et de la fonction défilement infini de vidéo pour les comptes mineurs, ce qui rejoint des réflexions actuellement menées aux États-Unis[650].

Une attention particulière doit en outre être portée aux systèmes de recommandation reposant sur les critères de l'engagement, qui caractérisent l'économie de l'attention, dès lors qu'ils conduisent à privilégier l'exposition à des contenus émotionnels, extrêmes, inappropriés ou (hyper)personnalisés afin de maximiser l'interaction des utilisateurs[651].

Au-delà, il pourrait être pertinent de consacrer un renversement de la charge de la preuve afin de tenir compte de l'asymétrie d'information existante entre les fournisseurs de service et leurs

---

[646] Parlement européen, Résolution du 26 novembre 2025, pt. 40.

[647] Rapport de la Mission Enfants et Ecrans, A la recherche du temps perdu, 2024, p. 77.

[648] Ibid.

[649] Assemblée nationale, Rapport fait au nom de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs, 4 septembre 2025, recommandations du Président n°1 et 2.

[650] Sur ce point, v. Chapitre 11 sur la conception des services, pt.11.2.3.

[651] Résolution du Parlement européen du 26 novembre 2025 sur la protection des mineurs en ligne, ((2025/2060(INI)), pt. 36. - sur ce point, v. les développements supra, pt. 11.2.1.2.5.

utilisateurs, ces derniers étant dans l'incapacité de démontrer le caractère addictif de la conception du service. Il s'agirait ainsi d'imposer aux fournisseurs de service - dont les réseaux sociaux - de rapporter la preuve de l'absence de caractère addictif de leurs fonctionnalités, notamment en partageant les tableaux de bord d'expérimentation et l'évaluation de leurs effets avec les autorités de contrôle et les utilisateurs, ce qu'a recommandé le Parlement européen dans sa recommandation sur la conception addictive[652]. Il préconise encore d'évaluer les effets de dépendance et d'impact sur la santé mentale de la conception des services, en particulier en ce qui concerne les systèmes de recommandation hyper-personnalisés, et s'agissant des enfants et adolescents. A ce titre, le Parlement souligne la nécessité pour la Commission européenne de coordonner, faciliter et financer des recherches en ce domaine.

Convergence avec la conception durable des services numériques. Il convient également de souligner un alignement important entre la remise en cause des conceptions addictives de certains services numériques et les travaux menés sur leur conception durable afin d'en réduire l'empreinte environnementale, ces derniers préconisant aussi des mesures visant à contrer la captation de l'attention des utilisateurs.

L'Arcep et l'Arcom ont en effet défini en 2024 un référentiel général de l'écoconception des services numériques, non contraignant, à destination des fournisseurs de services numériques[653]. Celui-ci "*vise à définir des critères de conception durable des services numériques afin d'en réduire l'empreinte environnementale"*, notamment "*l'affichage et la lecture des contenus multimédias pour permettre de limiter le recours aux stratégies de captation de l'attention des utilisateurs des services numériques*"[654]. Le deuxième objectif affiché de ce référentiel est d'ailleurs de "*promouvoir une démarche de sobriété environnementale face aux stratégies de captation de l'attention de l'utilisateur pour des usages alignés avec les objectifs environnementaux*"[655].

En soulignant que l'économie de l'attention "*peut entrer en dissonance avec l'objectif de sobriété environnementale*", l'Arcep et l'Arcom ambitionnent d'en limiter les effets négatifs, notamment : "*restreindre les fonctionnalités "nudge" poussant à l'usage incontrôlé du service : "mur de contenu" infini, déclenchement automatique des contenus vidéo, notifications intempestives, etc*.", "*redonner à l'utilisateur le contrôle de ses usages grâce à des informations claires, l'absence de procédés manipulatoires dans son interface ("dark patterns") et des fonctionnalités adaptées allant d'un bouton "stop" à un mode "sobriété énergétique" ou "économie des données", ou encore à la mise en place d'un indicateur de suivi de consommation*" et "*limiter la captation de données et métadonnées à des fins de profilage publicitaire*"[656]. Le référentiel comporte en outre

[652] Parlement européen, IMCO, Résolution du 12 décembre 2023 préc.

[653] Arcep, Arcom, Référentiel général de l'écoconception des services numériques, mai 2024.

[654] Loi n°2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France, art. 25 introduisant l'art. L. 38-5 du c. des postes et des communications électroniques.

[655] Arcep, Arcom, préc., p. 3.

[656] Ibid.

des précisions opérationnelles sur la lecture automatique des contenus[657], le défilement infini[658] et les notifications par défaut[659].

11.2.1.2.4. Algorithmes de recommandation et exposition aux contenus

S'agissant des algorithmes de recommandation qui organisent l'exposition des utilisateurs aux contenus accessibles sur les réseaux sociaux, leur conception n'est pas directement visée par les dispositions du DSA. Certaines dispositions imposent des obligations de transparence aux plateformes. Ainsi, selon l'article 27, les utilisateurs doivent être informés des principaux paramètres utilisés dans leurs systèmes de recommandation et de l'existence d'une option permettant aux utilisateurs de les modifier ou les influencer ; quant à l'article 38, il impose aux très grandes plateformes et moteurs de recherche de proposer au moins une option de paramétrage ne reposant pas sur le profilage de l'utilisateur au sens du RGPD. Ces obligations paraissent toutefois limitées à plusieurs égards. Tout d'abord, l'existence d'une simple option ne paraît pas suffisante, y compris concernant l'obligation imposée aux très grandes plateformes dès lors que le profilage peut être maintenu comme valeur de paramétrage par défaut. De plus, puisque sa nature n'est pas précisée, les opérateurs sont autorisés à proposer une alternative peu attractive pour leurs utilisateurs en guise d'option. Les très grandes plateformes sont en outre tenues de conduire des analyses de risques et de prendre des mesures de remédiation de ces risques au titre des articles 34 et 35 du DSA[660].

En revanche, la conception des algorithmes de recommandation tombe sous le coup de l'article 28 imposant aux plateformes accessibles aux mineurs de concevoir leur service pour imposer un haut niveau de protection de leur vie privée, sécurité et sûreté. A cet égard, les lignes directrices de l'article 28 du DSA recommandent tout d'abord que les plateformes prennent en compte les besoins, les caractéristiques des mineurs, les situations de handicaps et autres besoins d'accessibilité lors de la définition des objectifs, paramètres et les stratégies d'évaluation des systèmes de recommandation. Elles relèvent à cet égard qu'il s'agira, en particulier, de ne pas seulement optimiser, et de façon prédominante, la maximisation du temps passé sur le service ainsi que l'engagement et l'interaction avec la plateforme mais de prendre aussi en compte des paramètres et métriques en lien avec l'exactitude, la diversité, l'inclusivité et la loyauté. En outre, les lignes directrices énoncent que les plateformes concernées doivent veiller à ce que les systèmes de recommandation promeuvent l'accès pour les mineurs à des informations pertinentes et adéquates pour eux, en tenant en compte les différentes catégories d'âge.

Par ailleurs, la Commission préconise que le système de recommandation repose sur les intérêts de l'utilisateur mineur ce qui suppose de respecter un certain nombre d'exigences cumulatives. Pour ce faire, il est souligné la nécessité de concevoir un système de recommandation ne reposant

[657] Arcep, Arcom, préc., p. 61.
[658] Arcep, Arcom, préc., p. 63.
[659] Arcep, Arcom, préc., p. 75.
[660] Sur ce point, v. infra 2.1.2.4.

pas sur la collecte permanente des données comportementales[661]. Il y est aussi souligné l'importance que le système priorise les signaux fournis par l'utilisateur sur les signaux implicites fondés sur l'engagement[662]. De plus, les lignes directrices mentionnent la nécessité de fournir à l'utilisateur une explication délivrée de telle sorte qu'il puisse comprendre, de façon effective, pourquoi chaque contenu spécifique lui est recommandé, ce qui devrait inclure les informations relatives aux paramètres utilisés et signaux collectés pour cette recommandation spécifique.

Par ailleurs, le texte préconise plusieurs mesures afin de renforcer le contrôle et le pouvoir d'agir de l'utilisateur. A cette fin, les utilisateurs mineurs doivent se voir proposer une option afin de pouvoir choisir un paramétrage du système de recommandation ne reposant pas sur le profilage au sens de l'article 4 du RGPD[663]. Cette mesure, déjà imposée aux très grandes plateformes et moteurs de recherche au titre de l'article 38 du DSA, est ainsi étendue à l'ensemble des plateformes dès lors que celles-ci sont accessibles aux mineurs. L'utilisateur doit en outre se voir offrir la possibilité de modifier ou influencer les paramètres à tout moment, notamment en lui permettant de sélectionner les catégories de contenus et les activités qui l'intéressent le plus ou le moins, et ce lors de la création du compte et tout au long de l'utilisation du service[664] ; il ne doit pas en être dissuadé par des choix complexes ou des sollicitations récurrentes[665]. Ceci viendra alors s'ajouter aux obligations imposées aux très grandes plateformes au titre de l'article 27 du DSA. Enfin, pour rendre effectif ce paramétrage par l'utilisateur, les plateformes doivent veiller à ce que les paramètres et les informations qui sont fournies aux mineurs concernant les systèmes de recommandation soient présentés de manière accessible et adaptée aux enfants.

Si l'on entend assurer un haut niveau de protection de la vie privée, de la sécurité et de la sûreté des utilisateurs mineurs, certaines de ces recommandations figurant dans les lignes directrices devraient être précisées et les exigences renforcées pour mieux prendre en compte l'intérêt des utilisateurs.

---

[661] Commission européenne, Communication de la Commission, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, p.21, pt. 65.d.

[662] Commission européenne, Lignes directrices article 28 DSA préc., p.22, pt. 65. Les données comportementales sont définies comme "*les données utilisées pour le classement. Ils résument les aspects du contenu, de l'utilisateur, contexte et de la manière dont tous ces éléments interagissent*" : Knight Georgetown Institute, Better Feeds: Algorithms that Put the People First, A How-to Guide for Platforms and Policymaker, 2025, p.6.

[663] Commission européenne, Communication de la Commission, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, p.23, pts. 66 et ss.

[664] Sur la reconnaissance d'un droit au paramétrage, v. Enfants et Ecrans. A la recherche du temps perdu, 2024 - CNCDH, Avis sur la lutte contre la haine en ligne, 2021 - CNNum, Votre attention s'il vous plait, 2022 et Cultiver la richesse des réseaux, 2024.

[665] Commission européenne, Lignes directrices article 28 DSA préc., pt. 67.a-b-c.

Tout d'abord, il serait préférable d'imposer un paramétrage par défaut du fonctionnement du système de recommandation valorisant les intérêts des utilisateurs et non une simple option ne reposant pas sur le profilage[666]. En effet, il a été démontré que, le plus souvent, le biais de confirmation conduit l'utilisateur à privilégier la fonctionnalité paramétrée par défaut et ne pas opter pour le choix des options proposées. Quant au recours aux algorithmes basés sur le profilage, le rapport publié en octobre 2025 par Amnesty International recommande qu'il ne soit autorisé que si l'utilisateur du service a donné son consentement explicite, libre et éclairé[667]. Il préconise par ailleurs que la collecte et l'exploitation de données à des fins de personnalisation des publicités ou des recommandations de contenus soient interdites[668] et que la plateforme leur offre la possibilité de communiquer volontairement leurs préférences personnelles[669].

S'agissant du fonctionnement du système de recommandation, il conviendrait d'exiger des plateformes que ne soient pris en compte que les signaux fournis par l'utilisateur[670] et non les signaux implicites fondés sur l'engagement[671]. Il conviendrait ainsi de ne se fonder que sur les données fournies activement par l'utilisateur, par exemple les intérêts déclarés lors de la définition de son profil, et ses retours d'information, notamment le signal "voir plus, voir moins" / "intéressé, pas intéressé"[672]. Cela supposerait toutefois de préciser la notion de profilage telle que visée par les lignes directrices de telle sorte à ce que soient pas inclus les systèmes de recommandation basés sur les signaux d'utilisateur (et non les signaux d'engagement)[673].

Quant à la possibilité offerte à l'utilisateur de modifier ou influencer les paramètres pour faire primer ses intérêts, des modalités particulières devraient être exigées afin de rendre ces actions pleinement efficientes. Cela suppose, comme l'évoquent les lignes directrices, que soient réunies plusieurs conditions. Tout d'abord, s'il paraît essentiel que cette possibilité soit offerte à l'utilisateur non seulement lors de la création du compte mais encore tout au long de l'utilisation du service, ces modifications doivent en outre être mises en œuvre de telle sorte à ne pas décourager les utilisateurs de réaliser de tels choix. A cet égard, concernant tout d'abord la liste de choix proposés, il est important que celle-ci ne prenne pas la forme d'une énumération trop longue et qu'elle ne soit pas formalisée de façon trop complexe ou présentée de telle sorte que l'utilisateur ne puisse comprendre l'incidence de ces choix. Ensuite, des modalités de choix devraient être

---

666 V. également en ce sens Amnesty International, Entraîné·e·s dans le « rabbit hole » de nouvelles preuves montrent les risques de TikTok pour la santé mentale des enfants, octobre 2025, p.39. Adde, Knight Georgetown Institute, Better Feeds: Algorithms that Put the People First, A How-to Guide for Platforms and Policymaker, 2025, p.6.

667 Ibid.

668 Amnesty International, Entraîné.e.s dans le "rabbit hole", préc., p.40.

669 Ibid.

670 Sur ce point, v. notamment Knight Georgetown Institute, Better Feeds : Algorithms that put the People first, A How-to guide for platforms and Policymaker, 2025, p. 8&s. Adde, Rapport Amnesty International, Entraîné.e.s dans le "rabbit hole", préc., p. 40.

671 Panoptykon Fondation, People vs BIGTECH, Safe by default, Moving away from engagement-based ranking toward safe, rights-respecting and human centric recommended systems, 2024.

672 Ibid.

673 CDT Europe, CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28, June 2025.

proposées afin de permettre à l'utilisateur de ne pas devoir le réitérer, au risque d'être découragé. En ce sens, l'Arcom suggère que ces paramètres ne soient pas fréquemment réinitialisés par les plateformes en ligne et que les mineurs et leurs tuteurs ne soient pas incités de manière répétitive par les plateformes à exprimer à nouveau un choix précédemment fait concernant les systèmes de recommandation[674] ; à défaut, cela pourrait être considéré comme une interface trompeuse ou manipulatrice au sens de l'article 25 du DSA[675]. Il pourrait être également pertinent que ce choix puisse varier en fonction du contexte d'usage.

Plus généralement, il est déterminant de s'assurer que le recours au choix individuel de l'utilisateur mineur soit mis en œuvre de telle sorte à ce que les plateformes ne présentent pas ces modalités de choix pour orienter la décision de l'utilisateur vers une solution moins protectrice de sa vie privée, de sa sécurité et de sa sûreté.

Il en est par ailleurs essentiel, comme le souligne la Commission dans les lignes directrices, que ces préférences influencent directement les recommandations fournies par le système. En revanche, il conviendrait de préciser comment procéder à l'évaluation concrète de ces effets tant concernant l'utilisateur que le régulateur. En outre, il paraît important que l'utilisateur se voit offrir la possibilité de signaler à la plateforme que ces préférences sont insuffisamment prises en compte. Au-delà, il est possible de relever que ces facultés de choix offertes à l'utilisateur, si elles ne sont pas suivies d'effet, pourraient être qualifiés d'interface trompeuse ou manipulatrice au sens de l'article 25 du DSA qui s'applique à toute plateforme, et pourraient contrevenir au respect de l'article 28 du DSA concernant les plateformes accessibles aux mineurs.

Au-delà, pour rendre effectif ce paramétrage à la main de l'utilisateur, les plateformes devraient, comme le souligne la Commission, veiller à ce que les paramètres et les informations qui sont fournies aux mineurs concernant les systèmes de recommandation soient présentés de manière accessible et adaptée aux enfants, ce qui est une condition essentielle de leur effectivité. A cet égard, il convient de relever l'importance de mettre en place des pratiques d'évaluation pour s'assurer que l'objectif est bien atteint, en organisant de façon indépendante des échanges avec divers panels d'utilisateurs.

Contenus illicites et inappropriés, sur-exposition et "effet de spirale". Des recommandations sont également formulées par les lignes directrices de l'article 28 qui visent tout particulièrement à éviter que ne soient recommandés aux utilisateurs mineurs des contenus inappropriés et que ceux-ci soient exposés à une spirale de contenus préjudiciables. A cette fin, les plateformes accessibles aux mineurs doivent en particulier mettre en œuvre des mesures visant à prévenir l'exposition répétée des mineurs à des contenus générant un risque pour leur sécurité et sûreté, particulièrement lorsqu'ils sont exposés de manière répétée à des contenus tels que ceux promouvant des standards de beauté non réalistes, ceux idolâtrant ou banalisant les troubles de santé mentale tels que l'anxiété ou la dépression, les contenus discriminatoires, les contenus

[674] Arcom, Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques, 12 juin 2025.
[675] En ce sens, v. Court of justice Amsterdam, 2 October 2025, préc.

choquants, voire relatifs à des actes violents ou encore ceux encourageant les mineurs à avoir des pratiques dangereuses.

Si une telle mesure doit être soutenue, elle semble appeler plusieurs précisions. La formulation retenue par la Commission reste très générale ; il serait pertinent de spécifier voire d'illustrer les modalités de mise en œuvre de telles mesures, par exemple en se référant aux bonnes pratiques en ce domaine[676]. En outre, il est important de tenir compte des risques d'atteinte disproportionnée à la liberté d'expression et d'information ; de tels risques peuvent en effet résulter d'une modération excessive des plateformes concernant ce type de contenus, en particulier en cas de modération algorithmique prenant insuffisamment en compte le contexte, dès lors que pourraient s'en trouver ainsi supprimés des contenus publiés dans pour objectif de soutenir les victimes notamment de trouble du comportement alimentaire[677].

Ensuite, les lignes directrices soulignent que les plateformes doivent mettre en place des mesures pour réduire le risque de recommandation de contenus comportant un risque pour la vie privée, la sécurité et la sûreté des mineurs, ou des contenus signalés par les utilisateurs, signaleurs de confiance et autres acteurs ou outils de modération, et dont la légalité ou la conformité aux CGU n'ont pas encore été vérifiées.

Selon les lignes directrices, elles doivent aussi mettre en œuvre des mesures pour garantir que le système de recommandation ne permette pas ou ne facilite pas la diffusion de contenus illégaux ou la commission d'une infraction pénale à l'égard d'un mineur.

Il est également préconisé qu'il revienne aux plateformes de veiller à ce que les fonctions de recherche, notamment la saisie automatique de texte dans la barre de recherche et les termes et phrases clés suggérés, ne recommandent pas de contenu considéré comme préjudiciable à la vie privée, à la sécurité ou à la sûreté des mineurs (ex. bloquer les termes de recherche connus comme donnant accès à un contenu considéré comme préjudiciable à la vie privée, à la sécurité ou à la sûreté des mineurs, tels que des mots particuliers, de l'argot, des hashtags ou des emojis).

D'autres mesures visent quant à elles à conférer à l'utilisateur un meilleur contrôle sur les contenus auxquels il se trouve exposé, outre les mécanismes de signalement et de retour d'information de l'utilisateur et l'importance que leur impact soit rapide et durable comme précédemment évoqués, les plateformes doivent offrir à l'utilisateur la possibilité de réinitialiser le fil de recommandation complètement et de façon permanente[678]. Sur ce point, comme le souligne l'Arcom[679], il est

---

[676] Sur les difficultés pouvant résulter de la définition des contenus visés, v. les développements relatifs à la définition des contenus préjudiciables, Sous-Chapitre 3, Modification de la perception de soi - Cadre légal, France et Union européenne, notamment la nécessité pour les plateformes de définir clairement ce qui relève de ce type de contenus dans leurs CGU.

[677] CDT Europe, CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28, June 2025.

[678] Commission européenne, Lignes directrices article 28 DSA préc., p.23, pt. 66.a-b.

[679] Arcom, Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques, 12 juin 2025.

essentiel que "*Cette fonctionnalité [soit] directement et aisément accessible dans la rubrique spécifique de l'interface de la plateforme en ligne où les informations sont hiérarchisées*".

Afin d'éviter des effets d'enfermement délétères, les lignes directrices énoncent que les plateformes doivent inviter le mineur à rechercher de nouveaux contenus après un certain nombre d'interactions, étant entendu que ces contenus ne doivent pas être présentés de façon déceptive à l'utilisateur. Afin de redonner du contrôle à l'utilisateur, la Commission relève encore que les plateformes doivent aussi mettre à disposition des utilisateurs des mécanismes de signalement et de retour d'information accessibles et compréhensibles pour les mineurs (par ex. "Show me less/more", "I don't want to see/I am not interested in", "I don't want to see content from this account," "This makes me feel uncomfortable," "Hide this," "I don't like this," or "This is not for me"). Elles doivent en outre s'assurer que leur utilisation influence le fonctionnement de l'algorithme de recommandation, à savoir que ces mécanismes de signalement et de retour d'information aient un impact rapide et durable sur les paramètres, l'édition et les résultats des systèmes de recommandation, ce qui devrait inclure la suppression définitive des recommandations des contenus signalés et la réduction de leur visibilité. Les plateformes sont par ailleurs tenues de veiller à ce que les mécanismes de signalement aient un effet immédiat, c'est-à-dire que les contenus et contacts signalés doivent être retirés du fil de recommandations, et la visibilité des contenus similaires réduite[680]. Étant donné que ces mesures sont particulièrement importantes pour assurer un haut niveau de protection de l'utilisateur - notamment - du mineur, il est déterminant de mettre en œuvre les moyens permettant de s'assurer qu'elles font l'objet d'une évaluation efficace de cet impact, comme précédemment évoqué.

Au-delà, conférer à l'utilisateur un meilleur contrôle sur les contenus devrait conduire à consacrer un principe de pluralisme des algorithmes afin de lui permettre de choisir différents algorithmes au sein de la plateforme. Cette idée est désormais portée par plusieurs auteurs et institutions, notamment par le rapport d'enquête sur les effets psychologiques de TikTok sur les mineurs[681]. En ce sens, ce rapport relève l'importance de recourir à des protocoles interopérables sur le modèle de Bluesky, permettant à ses utilisateurs de choisir leur propre algorithme et à des tiers de proposer des algorithmes tiers intégrés à cette application[682]. A cette fin, il est recommandé d'introduire dans le droit européen une obligation de pluralisme algorithmique, s'inspirant du principe de pluralisme des médias inscrit à l'article 34 de la Constitution française[683]. Les utilisateurs des plateformes se verraient ainsi conférer un pouvoir de décision sur leur expérience numérique. Ce contrôle pourrait également s'étendre aux parents, qui pourraient ainsi mieux accompagner l'expérience en ligne de leurs enfants. Une telle réforme pourrait ainsi renforcer la protection des mineurs en ligne en permettant l'apparition d'algorithmes alternatifs proposant des environnements numériques adaptés aux enfants.

[680] Commission européenne, Lignes directrices article 28 DSA préc., pt. 66.e.

[681] Assemblée nationale, Rapport fait au nom de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs, 4 septembre 2025, p.222.

[682] Rapport sur les effets psychologiques de TikTok sur les mineurs, préc., p.222.

[683] Rapport sur les effets psychologiques de TikTok sur les mineurs, préc., p.225.

11.2.1.2.5. Risques en lien avec l'utilisation d'un système d'IA in app

Compte tenu du recours croissant à l'IA dans le cadre des services de réseaux sociaux au-delà des algorithmes de recommandation et de modération, une attention particulière est désormais portée à ce sujet. Un traitement distinct doit leur être réservé, ce qui explique que les lignes directrices sur l'article 28 énoncent plusieurs mesures que doivent respecter les plateformes dès lors qu'elles intègrent de telles fonctionnalités. A cet égard, et compte tenu des risques précédemment exposés, les IA Compagnons supposent de conduire des analyses approfondies concernant l'impact potentiel des interactions entre ces dispositifs techniques et leurs utilisateurs, en particulier lorsqu'ils sont mineurs.

Tout d'abord, il s'agit d'encadrer l'accessibilité et l'utilisation de ces services par les mineurs[684]. Les lignes directrices préconisent ainsi que les utilisateurs mineurs ne soient encouragés ou incités à les utiliser. La Commission précise en outre que ces systèmes doivent être conformes aux capacités évolutives des mineurs et conçus de manière sûre. Il est aussi souligné la nécessité que ces fonctionnalités ne soient accessibles qu'après avoir réalisé une analyse de risques concernant la protection de la vie privée, la sûreté et la sécurité des mineurs.

Au-delà, la Commission mentionne la nécessité pour les plateformes de permettre aux mineurs et leurs représentants de refuser d'utiliser l'agent conversationnel et de ne pas être incités à l'utiliser par le recours à des techniques de *nudge*[685]. Afin de renforcer la protection des utilisateurs mineurs, il devrait être imposé que ce type de fonctionnalité ne soit pas installée par défaut et que l'utilisateur se voit offrir la possibilité de la désinstaller aisément.

S'ajoutent à cela des exigences d'information de l'utilisateur quant à la nature et le fonctionnement des agents conversationnels. A cet égard, l'article 50.1 du Règlement Intelligence artificielle impose une obligation d'information au fournisseur d'un système d'IA ayant vocation à interagir directement avec une personne physique - dont les agents conversationnels -, qui est tenu de s'assurer que celui-ci est conçu et développé de telle sorte que l'utilisateur soit informé qu'il interagit avec un système d'IA. Les lignes directrices de l'article 28 du DSA précisent quant à elles que les plateformes doivent informer leurs utilisateurs mineurs des mesures qu'elles mettent en place pour garantir un haut niveau de protection de leur vie privée, sûreté et sécurité en ce qui concerne en particulier les systèmes d'IA intégrés à leur service, leurs limites et les potentielles conséquences de leur utilisation[686]. En outre, le texte indique que les plateformes doivent veiller à ce que des mesures techniques soient mises en œuvre pour avertir les mineurs que les interactions avec ce système sont différentes des interactions humaines et que ces systèmes peuvent fournir des informations factuellement inexactes et trompeuses[687]. Le document cite plusieurs exemples, comme la nécessité de ne pas mettre ces agents conversationnels en évidence, qu'ils ne fassent pas

[684] Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065, C/2025/5519, *JOUE* 10 oct. 2025, p.20, pt. 61, e.

[685] Commission européenne, Lignes directrices article 28 DSA préc., p.20, pt. 61, f.

[686] Commission européenne, Lignes directrices article 28 DSA préc., pt. 91, a, vi.

[687] Commission européenne, Lignes directrices article 28 DSA préc., pt. 61, f.

partie des contacts suggérés ou encore qu'ils ne soient pas regroupés avec les utilisateurs auxquels le mineur est connecté[688]. Il souligne en outre que cet avertissement doit être facilement visible et directement accessible à partir de l'interface et ce, tout au long de l'interaction du mineur avec la fonctionnalité d'interaction avec une IA/agent conversationnel/ système d'IA (*AI features*), étant entendu qu'il paraît nécessaire ici que ces rappels soient réguliers[689].

D'autres mesures visent en outre à limiter les risques d'influence pouvant résulter de l'utilisation de ces fonctionnalités. En ce sens, les lignes directrices de l'article 28 relèvent en particulier que les systèmes d'IA intégrés à la plateforme ne doivent pas conduire à influencer les mineurs à des fins commerciales, notamment en cas d'utilisation d'un agent conversationnel[690]. Il convient d'ajouter les risques d'exploitation des vulnérabilités des mineurs, au sens du Règlement Intelligence artificielle. En effet, son article 5, 1, b., vise, au titre des usages prohibés, les systèmes d'IA exploitant les éventuelles vulnérabilités dues notamment à l'âge, par exemple celles des enfants, ayant pour objectif ou pour effet d'altérer substantiellement le comportement de cette personne d'une manière qui cause ou est susceptible de causer un préjudice important à cette personne ou à un tiers. Parmi les exemples cités par les lignes directrices de la Commission sur les usages prohibés concernant ce texte, est mentionné le cas du système d'IA conçu de manière anthropomorphique et simulant des réactions émotionnelles de type humain dans ses interactions avec les enfants pouvant exploiter leurs vulnérabilités d'une manière qui favorise un attachement émotionnel malsain, manipule le temps d'engagement et déforme la compréhension qu'ont les enfants des relations humaines authentiques[691]. Certains envisagent ainsi la nécessité d'étudier une

---

[688] Commission européenne, Lignes directrices article 28 DSA préc. pt. 61, f.

[689] Arcom, Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques, 12 juin 2025.

[690] Commission européenne, Commission européenne, Lignes directrices article 28 DSA préc., p.25, pt. 69, e.

[691] Commission européenne, Communication de la Commission, Lignes directrices sur les pratiques interdites en matière d'intelligence artificielle au sens du Règlement UE 2024/1689 (Règlement sur l'IA), C(2025) 5052 final, 29 juillet 2025, p.45, pt. 116. A cet égard, le texte relève que cela peut entraver le développement social et émotionnel normal des enfants, leurs relations avec d'autres personnes humaines et leurs compétences socio-émotionnelles telles que l'empathie, la régulation émotionnelle, la compréhension sociale et l'adaptabilité. Il peut en résulter des préjudices psychologiques tels que l'augmentation de l'anxiété et de la dépendance des enfants à l'égard du service, ainsi que des préjudices à plus long terme pour le bien-être de l'enfant. Il relève plus généralement que les enfants sont très impressionnables et peuvent ne pas avoir la maturité cognitive nécessaire pour évaluer de manière critique les contenus persuasifs ou pour résister à certaines pratiques d'exploitation visant à les maintenir dans une situation de dépendance vis-à-vis des services utilisant l'IA. Cela pourrait contribuer à façonner leurs valeurs, leurs croyances et leurs comportements de manière potentiellement préjudiciable. La Commission précise que le préjudice important est ici à la fois physique et psychologique, exacerbé par l'incapacité des enfants à discerner et à résister à l'exploitation et par les effets néfastes sur leur développement et leur bien-être, qui peuvent avoir un impact à long terme.

possible interdiction des fonctionnalités anthropomorphiques et de veiller à s'assurer que les mineurs puissent aisément se désengager de ce type d'interactions[692].

Il conviendrait de compléter ou d'illustrer ces recommandations en mentionnant en particulier les mesures de sécurité à mettre en œuvre (*AI Safety*). Il s'agit ici de s'assurer que ces systèmes ne puissent pas favoriser des comportements nuisibles à la santé mentale des mineurs, comme la génération de réponses incitant à l'automutilation ou au suicide, ou banaliser et légitimer des comportements dangereux mettant en péril leur sécurité. A cette fin, il conviendrait de s'assurer de la mise en œuvre de mesures anti-contournement (*guardrails*) efficaces, notamment en conduisant des tests de robustesse auxquels devraient être associés des organismes indépendants dont les chercheurs académiques et les ONG de défense des droits des utilisateurs. Il reviendrait en outre d'enjoindre les fournisseurs de service à mettre à disposition des utilisateurs des mécanismes efficients afin de leur permettre de signaler toutes interactions comportant de tels risques[693].

11.2.2. Angleterre et Pays de Galles

En droits anglais et gallois, l'Online Safety Act[694] impose des obligations d'évaluation des risques envers les enfants, à la charge des services d'utilisateur à utilisateur régulés auxquels des enfants sont susceptibles d'accéder[695]. Dans le cadre d'une telle évaluation, l'opérateur doit notamment envisager les différentes utilisations du service, y compris ses fonctionnalités ou autres caractéristiques qui affectent à quel point les enfants l'utilisent (par exemple la lecture automatique de contenus), et l'impact d'une telle utilisation sur le niveau de risque de préjudice pouvant être souffert par les enfants[696]. Plus largement, il doit indiquer comment la conception et le fonctionnement du service, y compris son modèle d'affaires, peut réduire ou augmenter les risques identifiés[697].

Le Code de conception adaptée à l'âge (Age-Appropriate Design Code) de l'autorité de protection des données du Royaume-Uni (ICO) évoquait déjà en 2020, en matière de droit des données à caractère personnel, les stratégies visant à étendre l'engagement de l'utilisateur au titre des « *usages préjudiciables des données* ». À défaut de recherches scientifiques solides, il recommandait alors aux opérateurs concernés de ne développer qu'avec précaution de telles fonctionnalités et de « *retirer les capabilités addictives* », en visant notamment les pratiques de récompense, de défilement infini, les notifications et la lecture de contenus qui encouragent les utilisateurs à continuer de jouer à un jeu, de regarder des contenus vidéo ou de rester en ligne d'une

[692] Parlement européen, Résolution du Parlement européen du 26 novembre 2025 sur la protection des mineurs en ligne (2025/2060(INI)), pt. 77.
[693] Sur ces différentes préconisations, v. not. CCDH, The illusion of AI Safety. Testing OpenAI's new Safe Completions approach to chatbot safety, October 2025, p. 23.
[694] Online Safety Act 2023, 2023 c. 50.
[695] Online Safety Act, s.11.
[696] Online Safety Act, s.11(6)(f).
[697] Online Safety Act, s.11(6)(h).

quelconque autre manière[698]. Le code préconisait en outre d'éviter de traiter des données personnelles d'une manière incitant les enfants à rester engagés (exemple : offrir des avantages personnalisés dans un jeu en échange d'un temps de jeu prolongé) ; de présenter les options pour continuer de jouer ou d'interagir avec un service de manière neutre ; d'éviter les fonctionnalités qui utilisent des données personnelles pour étendre automatiquement le temps d'utilisation au lieu de requérir des enfants un choix actif de passer leur temps de cette sorte (lecture automatique fondée sur les données) ; et d'introduire des mécanismes tels que des boutons « pause » qui permettent aux enfants de faire une pause n'importe quand sans perdre leur progrès dans le jeu, ou fournir des ressources adaptées à l'âge pour soutenir des choix conscients relatifs aux pauses.

11.2.3. États-Unis

Au niveau fédéral, trois propositions de loi peuvent être envisagées : le Kids Online Safety Act de 2023 (1)[699], le Protecting Kids on Social Media Act de 2023 (2)[700], et le Kids Internet Design and Safety Act (KIDS Act) de 2021 (3)[701]. Parmi les initiatives étatiques, l'État de Californie a adopté en 2022 son Age-Appropriate Design Code Act[702] auquel s'ajoute proposition particulièrement volontaire de Social Media Youth Addiction Law de 2024[703] (4). Il convient enfin de mentionner la loi de l'État de New York Stop Addictive Feeds Exploitation (SAFE) For Kids Act (5.)

(1) Le **Kids Online Safety Act** (ci-après « KOSA ») en sa version du 13 décembre 2023 serait applicable largement aux plateformes connectées à Internet, utilisées par des mineurs ou raisonnablement susceptibles de l'être (dont jeux vidéo en ligne, partage de vidéos et réalité virtuelle)[704]. Il consacre une définition de l'usage compulsif (*compulsive usage*) comme "*toute réponse stimulée par des facteurs externes qui conduit un individu à adopter un comportement répétitif raisonnablement susceptible de causer une détresse psychologique, une perte de contrôle, de l'anxiété ou une dépression*"[705].

Les dispositions les plus intéressantes de ce texte consistent à énoncer des mesures protectrices des mineurs ainsi que des outils parentaux, en portant une attention particulière au paramétrage

[698] Information Commissioner's Office, *Age appropriate design: a code of practice for online services*, 2 sept. 2020, p. 45.
[699] Proposition de Kids Online Safety Act, S.1409 — 118th Congress (2023-2024), en sa version déposée au Sénat le 2 mai 2023 et réécrite par un amendement du 13 décembre 2023.
[700] Proposition de Protecting Kids on Social Media Act, S. 1291 – 118th Congress (2023-2024), en sa version introduite au Sénat le 26 avril 2023.
[701] Proposition de Kids Internet Design and Safety Act, H.R.5439 - 117th Congress (2021-2022), en sa version introduite à la Chambre des Représentants le 30 septembre 2021.
[702] California Age-Appropriate Design Code Act, Assembly Bill No. 2273, 15 September 2022.
[703] Proposition de Social Media Youth Addiction Law, CA SB976 – 2023-2024 – Regular Session, en sa version introduite au Sénat de Californie le 29 janvier 2024.
[704] Proposition de Kids Online Safety Act, s.2(3), certaines de ces plateformes étant plus précisément définies à s.2(9) et s.2(10).
[705] Proposition de Kids Online Safety Act, s.2(2).

par défaut. Ainsi, une plateforme concernée doit fournir à un individu dont elle connaît l'état de minorité des protections (« *safeguards* ») directement accessibles et facilement utilisables pour, notamment : limiter les fonctionnalités qui augmentent, maintiennent ou étendent l'utilisation de la plateforme concernée par le mineur, telles que la lecture automatique de contenu, les récompenses pour le temps passé sur la plateforme, les notifications et autres fonctionnalités qui résultent en un usage compulsif de la plateforme concernée par le mineur[706] ; et contrôler les systèmes de recommandation personnalisés, y compris par au moins l'une de deux possibilités pour le mineur (s'en exclure au profit d'un format chronologique, ou limiter les types et catégories de recommandations de la part de tels systèmes)[707]. La plateforme doit également offrir des options, notamment pour limiter le temps passé par le mineur sur la plateforme concernée[708]. Si l'utilisateur est identifié comme étant mineur, le paramètre par défaut pour les protections précitées doit être celui qui fournit le niveau de contrôle le plus protecteur en termes de vie privée et de sécurité de l'utilisateur[709].

Ces mesures doivent se doubler d'outils parentaux, permettant de gérer les paramètres du compte et de vie privée du mineur, de restreindre les achats et transactions financières effectués par celui-ci, et de visualiser des métriques du temps total passé sur la plateforme, ainsi que de restreindre le temps d'utilisation maximal autorisé[710]. En cas d'usage de ces outils, le mineur doit en être clairement informé[711]. Les outils précités doivent être activés par défaut pour les utilisateurs identifiés comme mineurs[712]. La texte précise en outre que la plateforme doit fournir une information claire, visible et adaptée à l'âge sur ces protections et outils parentaux, et ne doit pas encourager les mineurs ou les parents à les affaiblir ou désactiver[713] ; il porte une interdiction des interfaces truquées (« *dark patterns* ») à cet égard[714].

Au-delà de ces éléments centraux, plusieurs mesures s'avèrent fortement similaires aux dispositions du DSA, telles qu'un devoir de diligence (*duty of care*), une obligation de transparence réservée à de plus grandes plateformes assortie d'un audit par un tiers indépendant et la prévision de lignes directrices de la Federal Trade Commission. Cependant, à la différence du DSA qui ne fait pas mention dans le corps du texte des précisions opérationnelles (ces précisions devraient être apportées par la suite à l'issue des travaux menés par la Commission européenne dans le cadre de la mise en œuvre du DSA - et en particulier de l'article 28 - en lien avec la stratégie BIK), le KOSA détaille les exigences attendues dans le corps du texte.

---

[706] Proposition de Kids Online Safety Act, s.4(a)(1)(C).

[707] Proposition de Kids Online Safety Act, s.4(a)(1)(D). V. cependant s.4(e)(3)(C) : pour autant, les plateformes concernées peuvent utiliser un système de recommandation personnalisé pour présenter du contenu à un mineur si les seules données utilisées sont : la langue du mineur, la ville dans laquelle il se situe, et son âge.

[708] Proposition de Kids Online Safety Act, s.4(a)(2)(B).

[709] Proposition de Kids Online Safety Act, s.4(a)(3).

[710] Proposition de Kids Online Safety Act, s.4(b)(2)(A) à (C) respectivement.

[711] Proposition de Kids Online Safety Act, s.4(b)(3).

[712] Proposition de Kids Online Safety Act, s.4(b)(4).

[713] Proposition de Kids Online Safety Act, s.4(e)(1).

[714] Proposition de Kids Online Safety Act, s.4(e)(2).

Ainsi, le devoir de diligence (*duty of care*) oblige la plateforme à prendre des mesures raisonnables dans la conception et le fonctionnement d'un produit, service ou fonctionnalité qu'elle sait être utilisé par des mineurs pour prévenir et atténuer les préjudices résultant, notamment, des schémas d'utilisation qui indiquent ou encouragent des comportements similaires à l'addiction[715].

Il convient de souligner que le texte fait l'objet de critiques à l'égard de ce devoir de diligence. Les opposants à la loi KOSA estiment que l'obligation de diligence (*duty of care*) entraînerait une censure généralisée des contenus en ligne, notamment des contenus émanant de la communauté LGBTQ+ ou la concernant. Ces critiques affirment que, pour se conformer au KOSA et éviter les poursuites judiciaires des procureurs généraux des États, les plateformes de médias sociaux supprimeront des catégories entières de contenu de leurs plateformes[716]. À titre d'exemple, les critiques affirment qu'un procureur général d'État pourrait soutenir que le contenu LGBTQ+ est associé à l'anxiété ou à la dépression, en violation de l'obligation de diligence, et qu'il devrait donc être entièrement supprimé d'une plateforme couverte[717].

En réponse à ces critiques, les auteurs du KOSA ont suggéré une interprétation disposant que le devoir de diligence "*ne doit être interprété comme exigeant d'une plateforme couverte qu'elle empêche ou exclue* "[718]. À ce titre, les mineurs pourront rechercher délibérément ou indépendamment du contenu.

Le texte impose également à certaines plateformes[719] une obligation de transparence sous la forme d'un rapport public au moins annuel décrivant les risques raisonnablement prévisibles de

---

[715] Proposition de Kids Online Safety Act, s.3(a)(2). Par contraste, l'article 28 du DSA intitulé « Protection des mineurs en ligne » ne détaille pas les risques envisagés ; tout au plus le considérant 71 correspondant mentionne-t-il que les interfaces en ligne devraient être conçues « *avec le plus haut niveau de protection de la vie privée, de sécurité et de sûreté des mineurs par défaut* ». Les considérants relatifs à l'analyse et l'atténuation des risques systémiques (art. 34 et 35) évoquent, au titre des risques pour les droits de l'enfant, « la conception des interfaces en ligne qui exploitent intentionnellement ou non les faiblesses et l'inexpérience des mineurs ou qui peuvent entraîner un comportement de dépendance » (cons. 81 sur la seconde catégorie de risques systémiques), puis la « conception d'interfaces en ligne susceptibles de stimuler les dépendances comportementales des destinataires du service » (cons. 83 sur la quatrième catégorie). Le texte insiste également sur la nécessité de se concentrer sur tous les systèmes algorithmiques concernés et de les adapter, y compris les interfaces (cons. 84 et 87), en tenant compte de l'intérêt supérieur des mineurs (cons. 89).

[716] American Action Forum, KOSA Updates Seek To Address Critics' Concerns, February 22, 2024.

[717]Fairplay, Our legal analysis of the Kids Online Safety Act.
https://fairplayforkids.org/our-legal-analysis-of-the-kids-online-safety-act/

[718] Section 3 du KOSA.

[719] Proposition de Kids Online Safety Act, s.6(b) : sont concernées les plateformes disposant de plus de 10 millions d'utilisateurs mensuels aux États-Unis sur l'année écoulée, et fournissant principalement un forum de communauté pour des contenus et discussions générés par les utilisateurs, y compris en réalité virtuelle.

préjudices substantiels aux mineurs et évaluant les mesures de prévention et d'atténuation prises à leur égard, sur le fondement d'un audit effectué par un tiers indépendant et ayant raisonnablement inspecté la plateforme concernée[720]. Le contenu de ce rapport est très détaillé et comprend en premier lieu le nombre d'utilisateurs raisonnablement envisagés comme mineurs aux États-Unis[721] et le temps médian et moyen passé sur la plateforme par des mineurs aux États-Unis par jour, par semaine et par mois[722]. Il inclut ensuite, entre autres, une évaluation des risques raisonnablement prévisibles de préjudices substantiels aux mineurs ; de la manière dont les systèmes de recommandation personnalisée et de publicité ciblée pour les mineurs peuvent contribuer à ces préjudices ; une description des éventuelles fonctionnalités dans la conception du système qui augmentent, maintiennent ou étendent l'usage d'un produit ou service par un mineur, telles que la lecture automatique de contenu, les récompenses pour le temps passé, et les notifications[723] ; une évaluation de l'efficacité des mesures de protection et des outils parentaux[724]. La plateforme décrit également ses mesures de protection, outils parentaux et interventions ; ses mesures de prévention et atténuation des risques, y compris l'adaptation ou le retrait de certaines fonctionnalités ou des systèmes de recommandation ; les mesures additionnelles à prendre pour éviter le contournement des protections et outils parentaux[725].

Par ailleurs, pour rappel le texte établit un Conseil de la sécurité des enfants en ligne (Kids Online Safety Council)[726] et confère à la Federal Trade Commission, après consultation de ce Conseil, la charge d'émettre des lignes directrices notamment sur les fonctionnalités utilisées pour augmenter, maintenir ou étendre l'utilisation de la plateforme par un mineur[727]. D'autres lignes directrices doivent indiquer les conduites qui n'ont pas pour objet ou effet substantiel de subvertir ou d'altérer l'autonomie, la prise de décision ou le choix de l'utilisateur, ou de causer, d'augmenter ou d'encourager un usage compulsif pour un mineur, telles que les changements de minimis à l'interface utilisateur dérivés de tests quant aux préférences des consommateurs, y compris différents styles, dispositions ou textes, quand de tels changements ne sont pas fait dans le but d'affaiblir ou désactiver des protections ou contrôles parentaux ; ou l'établissement de paramètres par défaut qui fournissent de plus grandes protections pour la vie privée des utilisateurs ou qui améliorent autrement leur autonomie et leur capacité à prendre des décisions[728].

---

[720] Proposition de Kids Online Safety Act, s.6(a). V. aussi s.6(d) détaillant l'audit mené par un tiers indépendant sur les risques systémiques de préjudice aux mineurs, qui doit notamment prendre en considération les systèmes de recommandation personnalisés et consulter les parents, mineurs et experts. Le Règlement sur les services numériques énonce également une obligation de recourir à un audit indépendant (art. 37) et de publier des rapports de transparence (art. 42) pour les très grandes plateformes et très grands moteurs de recherche.

[721] Proposition de Kids Online Safety Act, s.6(c)(1)(C)(i).

[722] Proposition de Kids Online Safety Act, s.6(c)(1)(C)(ii).

[723] Proposition de Kids Online Safety Act, s.6(c)(2)(A) à (C) respectivement.

[724] Proposition de Kids Online Safety Act, s.6(c)(2)(E).

[725] Proposition de Kids Online Safety Act, s.6(c)(3).

[726] Proposition de Kids Online Safety Act, s.12.

[727] Proposition de Kids Online Safety Act, s.10(a)(1)(A).

[728] Proposition de Kids Online Safety Act, s.10(a)(2)(A) et (C) respectivement.

Pour les services de streaming vidéo diffusant des contenus présélectionnés par le fournisseur et non générés par les utilisateurs, requérant une inscription et ne fournissant pas principalement des contenus d'actualité ou des contenus sportifs, la conformité au texte est conditionnée entre autres à la possibilité de limiter la lecture automatique du contenu sur demande sélectionné par un système de recommandation personnalisée pour un individu dont l'état de minorité est connu du service[729].

Enfin, par une disposition applicable au-delà des seuls utilisateurs mineurs, le Kids Online Safety Act consacre une distinction entre les « *algorithmes transparents sur les données d'entrée* » (*input-transparent algorithm*) n'utilisant pas de données spécifiques à un utilisateur pour déterminer l'ordre de présentation de l'information, sauf à ce que ces données soient expressément fournies par l'utilisateur à cette fin[730] – entre autres les termes de recherche, filtres, préférences sauvegardées, géolocalisation, profils de réseaux sociaux ou chaînes de vidéos suivies ou sélectionnées, et excluant toutes les autres données ou inférences spécifiques à l'utilisateur ou à son terminal (historique de recherche et navigation web, activité physique, transactions financières)[731] – et les « algorithmes opaques », qui se fondent sur des données spécifiques aux utilisateurs non expressément fournies par ceux-ci à cette fin, à l'exception des filtres de contenus appropriés à l'âge[732]. Cette distinction fonde un régime contraignant pour tout site internet destiné au public, application internet ou mobile, y compris un réseau social, un service de partage de vidéo, un moteur de recherche ou un service d'agrégation de contenus[733], sous réserves d'importantes exceptions[734]. Le texte interdit les algorithmes opaques, à moins que deux conditions cumulatives ne soient remplies : d'une part, le caractère opaque est dévoilé, et les conditions générales détaillent ses principaux paramètres, les options de l'utilisateur, et les quantités éventuelles – temps d'utilisation, mesures d'engagement ou d'interaction – que l'algorithme serait conçu pour optimiser[735] ; d'autre part, l'opérateur permet à l'utilisateur de choisir facilement une version du site soumise à un algorithme transparent sur les données d'entrée[736]. Il est interdit d'imposer un prix différent pour ces deux versions du service[737].

[729] Proposition de Kids Online Safety Act, s.15(e)(2)(B).
[730] Proposition de Kids Online Safety Act, s.13(a)(6)(A).
[731] Proposition de Kids Online Safety Act, s.13(a)(6)(B).
[732] Proposition de Kids Online Safety Act, s.13(a)(7).
[733] Proposition de Kids Online Safety Act, s.13(a)(5)(A).
[734] Proposition de Kids Online Safety Act, s.13(a)(5)(B) : sont exclus les sites entièrement opérés par une personne qui n'avait pas plus de 500 employés dans les six derniers mois, et moins de $50 millions de chiffre d'affaires annuel en moyenne, et qui traitent annuellement les données spécifiques à un utilisateur de moins d'un million d'utilisateurs ; sont également exclus ceux opérés pour une recherche non commerciale.
[735] Proposition de Kids Online Safety Act, s.13(b)(2)(A)(i).
[736] Proposition de Kids Online Safety Act, s.13(b)(2)(A)(ii).
[737] Proposition de Kids Online Safety Act, s.13(b)(4).

(2) Le **Protecting Kids on Social Media Act** interdirait aux plateformes de réseaux sociaux (ce qui exclut les jeux en ligne[738]) d'utiliser les données à caractère personnel d'un individu pour organiser sa recommandation algorithmique, à moins que la plateforme n'ait la certitude ou la croyance raisonnable que l'individu a plus de 18 ans selon son processus de vérification d'âge[739]. Cette interdiction ne couvre pas la suggestion d'information ou la fourniture de publicité lorsqu'elles sont contextuelles[740].

(3) Le **KIDS Act (Kids Internet Design and Safety Act)** porterait interdiction de plusieurs éléments d'interface délimités, applicable aux plateformes en ligne destinées aux enfants ou à toute plateforme en ligne employant de tels éléments d'interface à l'égard d'un utilisateur dont elle a une connaissance avérée ou imputée qu'il est un mineur de seize ans[741].

Les éléments d'interface visés sont les suivants : lecture automatique du contenu vidéo suivant celui initialement sélectionné par l'utilisateur ; messages ou alertes qui encouragent un utilisateur concerné à interagir avec la plateforme alors qu'il ne l'utilisait pas activement ; affichage de la quantité d'engagement positif ou de retour qu'un utilisateur concerné a reçu des autres ; tout élément d'interface ou paramètre qui encourage déloyalement un utilisateur concerné, en raison de son âge ou inexpérience, à partager des informations personnelles, soumettre du contenu, ou passer plus de temps à interagir avec la plateforme ; tout élément d'interface qui fournit à un utilisateur concerné des badges ou autres symboles de récompense visuels sur le fondement d'un niveau élevé d'interaction avec la plateforme ; tout élément d'interface qui maximise les dépenses d'un utilisateur concerné sur la plateforme, l'encourage déloyalement à dépenser de l'argent sur la plateforme, facilite une transaction financière sans notification parentale, ou facilite une transaction financière qui n'est pas dans ses intérêts[742].

(4) État de Californie

Le ***California Age-Appropriate Design Code Act***, adopté en 2022 et dont l'entrée en vigueur était prévue pour le 1er juillet 2024, adopte une acception large de l'analyse d'impact sur la protection des données (« data protection impact assessment ») à des fins de protection des mineurs. Cette analyse impose à l'opérateur d'analyser notamment si les algorithmes utilisés, ou les systèmes de publicité ciblée, pourraient porter préjudice aux enfants[743], et si et comment la conception du système utilise des fonctionnalités pour augmenter, maintenir ou étendre l'usage du produit, du

[738] Proposition de Protecting Kids on Social Media Act, s. 2(6) pour la définition des plateformes de réseaux sociaux.

[739] Proposition de Protecting Kids on Social Media Act, s.6(a). Le texte définit un système de recommandation algorithmique comme un système automatisé en tout ou partie qui suggère, promeut, ou classe de l'information pour un individu ou lui présente de la publicité : s.2(1).

[740] Proposition de Protecting Kids on Social Media Act, s.6(b).

[741] Proposition de Kids Internet Design and Safety Act, s.4(a)(1)(A). Pour une définition des plateformes concernées, v. s.3(a)(8) ; du caractère « destiné aux enfants », v. s.3(a)(5) ; de la connaissance imputée (« constructive knowledge »), v. s.3(a)(3).

[742] Proposition de Kids Internet Design and Safety Act s.4(a)(1)(B)(i) à (vi) respectivement.

[743] California Age-Appropriate Design Code Act, 1798.99.31(a)(1)(B)(v) et (vi).

service ou de la fonctionnalité par des enfants, y compris la lecture automatique de contenus, des récompenses pour le temps passé, et des notifications[744]. Cette analyse doit être réexaminée deux fois par an et être assortie de mesures d'atténuation ou d'élimination des risques ; si elle doit être fournie sur requête du procureur général de Californie, elle ne peut être communiquée au public[745].

Au-delà, le texte souligne la nécessité de protéger les enfants non seulement à l'égard des produits et services qui leur sont destinés, mais aussi sur ceux auxquels ils sont susceptibles d'accéder (« likely to access »)[746]. Il affirme également que l'intérêt supérieur de l'enfant doit être considéré lors de la conception, du développement et de la fourniture du service, produit ou de la fonctionnalité et qu'en cas de conflit avec les intérêts financiers, la vie privée, la sécurité et le bien-être des enfants doivent primer[747]. En outre, un Groupe de travail sur la protection des données des mineurs (California Children's Data Protection Working Group) est en charge de préciser les bonnes pratiques[748].

Enfin, le texte interdit à toute entreprise qui fournit un service, un produit ou une fonctionnalité en ligne auquel un mineur est susceptible d'accéder d'utiliser les données à caractère personnel d'un mineur d'une manière que l'entreprise sait, ou a des raisons de savoir, être substantiellement préjudiciable à la santé physique ou mentale ou au bien-être d'un enfant[749], ou d'user d'interfaces truquées encourageant le mineur à des actions similairement préjudiciables, entre autres[750]. Il prohibe également le profilage d'un enfant par défaut sauf exceptions[751].

Il fait cependant l'objet d'un recours de la part du lobby de la tech NetChoice pour non conformité au Premier Amendement[752].

Le **Protecting Our Kids from Social Media Addiction Act** adopté en Californie insère au Code de la santé et sécurité californien un nouveau chapitre relatif à l'addiction des mineurs aux médias sociaux. Il consacre une définition du "*fil d'informations addictif*"("*addictive feed*") comme "*un site internet, service en ligne, application en ligne ou mobile, ou une partie de celui-ci, dans lequel plusieurs contenus générés ou partagés par des utilisateurs sont, simultanément ou consécutivement, recommandés, sélectionnés ou priorisés pour être présentés à un utilisateur d'une manière fondée, en tout ou partie, sur des données fournies par l'utilisateur, ou autrement associés à l'utilisateur ou à son terminal"*, celle-ci étant soumises à plusieurs exceptions[753]. La

[744] California Age-Appropriate Design Code Act, 1798.99.31(a)(1)(B)(vii).
[745] California Age-Appropriate Design Code Act, 1798.99.31(a)(3) et (4).
[746] California Age-Appropriate Design Code Act, 1798.99.29.
[747] California Age-Appropriate Design Code Act, 1798.99.29(a) et (b).
[748] California Age-Appropriate Design Code Act, 1798.99.32.
[749] California Age-Appropriate Design Code Act, 1798.99.31(b)(1).
[750] California Age-Appropriate Design Code Act, 1798.99.31(b)(7).
[751] California Age-Appropriate Design Code Act, 1798.99.31(b)(2), notamment si l'entreprise peut démontrer qu'elle a mis en place des mesures appropriées pour protéger les enfants.
[752] NetChoice v. Bonta, Case No. 22-cv-08861-BLF, N.D. Cal.
[753] Protecting Our Kids from Social Media Addiction Act, Senate Bill No. 976, 20 sept. 2024, 27000.5(a). Les exceptions s'appliquent notamment si l'information n'est pas associée à l'utilisateur ou à son

fourniture d'un tel fil d'informations addictifs par un site internet, service en ligne, application en ligne ou mobile, lorsqu'il s'agit d'une part importante du service, conduit alors à la qualification d'*"application ou service en ligne addictif"*[754].

Il est alors illicite pour l'opérateur d'un tel service de fournir un fil d'informations addictif à un utilisateur à moins que l'une des deux conditions suivantes ne soit remplie : soit l'opérateur a raisonnablement déterminé que l'utilisateur n'était pas mineur (condition entrant en vigueur au 1er janvier 2027 ; d'ici là, il suffit qu'il n'ait pas une connaissance avérée de la minorité de l'utilisateur), soit il a obtenu un consentement parental vérifiable pour fournir un fil d'informations addictif à un utilisateur mineur[755].

En outre, le texte rend illicite le fait pour l'opérateur d'un service en ligne addictif d'envoyer des notifications à un utilisateur dont il connaît l'état de minorité (ou, à compter du 1er janvier 2027, dont il n'a pas raisonnablement déterminé la majorité) en l'absence de consentement parental vérifiable entre minuit et six heures du matin inclus, et entre huit heures et quinze heures du lundi au vendredi de septembre à mai[756]. Il impose à l'opérateur d'un tel service d'adopter les paramètres "*par défaut*" suivants : empêcher l'accès de l'enfant à la plateforme et aux notifications entre minuit et six heures du matin, limiter son temps d'utilisation à une heure par jour, restreindre la visibilité du nombre de "*j'aime*" ou d'autres formes de réponses à des contenus dans un fil d'informations addictif, proposer un fil d'informations non addictif, rendre le compte de l'enfant privé de sorte que seuls ses contacts puissent voir et interagir avec son contenu[757]. Il oblige également l'opérateur à fournir un mécanisme par lequel le parent d'un utilisateur mineur puisse modifier ces paramètres, notamment pour fixer les heures entre lesquelles l'enfant ne peut accéder au réseau social ou recevoir des notifications, ou le temps maximal d'utilisation[758], tout en précisant que cela n'a pas vocation à imposer à l'opérateur de donner aux parents un accès ou contrôle plus étendu sur les données ou les comptes de leurs enfants[759].

Enfin, l'opérateur a l'obligation de communiquer annuellement le nombre d'utilisateurs mineurs ainsi que, parmi ceux-ci, le nombre d'utilisateurs bénéficiant du consentement parental vérifiable pour consulter un fil addictif, et le nombre d'utilisateurs pour lesquels les paramètres précités sont

---

terminal de manière invariable et ne concerne pas ses interactions passées avec du contenu (27000.5(a)(1)) ; si l'utilisateur a demandé de manière expresse et univoque ce contenu ou son auteur, ou le blocage, la mise en avant ou en retrait de ce contenu, tant que sa présentation n'est pas fondée sur d'autres données concernant l'utilisateur ou son terminal et que le contenu audio ou vidéo n'est pas lu automatiquement (27000.5(a)(4)) ; s'il s'agit uniquement du prochain contenu dans une séquence préexistante du même auteur ou source et que celui-ci, s'il est en format audio ou vidéo, n'est pas lu automatiquement (27000.5(a)(6)).

[754] Protecting Our Kids from Social Media Addiction Act, 27000.5(b)(1). Pour les exceptions, v. 27000.5(b)(2).

[755] Protecting Our Kids from Social Media Addiction Act, 27001(a).

[756] Protecting Our Kids from Social Media Addiction Act, 27002(a).

[757] Protecting Our Kids from Social Media Addiction Act, 27002(b)(1) à (5).

[758] Protecting Our Kids from Social Media Addiction Act, 27002(b).

[759] Protecting Our Kids from Social Media Addiction Act, 27003(a).

ou non activés[760]. Il convient de noter qu'il lui est interdit d'exercer tout traitement défavorable de l'utilisateur du fait de l'exercice des droits prévus (retrait, dégradation, augmentation des prix du service), même si un opérateur peut choisir de ne pas fournir son service à des mineurs[761].

Un recours a été formé par NetChoice contre ce texte, sur le fondement notamment du Premier Amendement, et la Cour d'appel du Neuvième Circuit devrait se prononcer en avril 2025[762].

(5) État de New York

Un projet de loi de l'État de New York vise à lutter contre les contenus addictifs des médias sociaux et à protéger les enfants en ligne. Ce projet de loi S.7694A/A.8148A signé le 20 juin 2024 par le Gouverneur de l'État de New York, établit le Stop Addictive Feeds Exploitation (SAFE) For Kids Act[763] pour exiger des entreprises de médias sociaux qu'elles limitent les flux addictifs sur leurs plateformes pour les utilisateurs de moins de 18 ans.

Ainsi, le texte interdit aux sites internet de collecter et de traiter les données personnelles de toute personne âgée de moins de 18 ans, à moins qu'ils n'aient reçu un consentement éclairé ou que cela ne soit strictement nécessaire à l'objectif du site web. Il interdit par ailleurs aux entreprises de médias sociaux de fournir aux enfants de moins de 18 ans des flux addictifs sans le consentement de leurs parents, un "flux addictif" (article 45) étant défini généralement comme un flux qui recommande, sélectionne et hiérarchise des médias sur la base d'informations associées à un utilisateur ou à son appareil. Cette loi permettra aux mineurs de consulter des flux non addictifs et tout contenu disponible sur une plateforme, tels que les flux classés par ordre chronologique, afin de s'assurer que les enfants puissent toujours bénéficier de tous les avantages fondamentaux des médias sociaux (Section 1). Le texte prévoit que le procureur général de l'État puisse diffuser des règles d'application. Par ailleurs, une entreprise en infraction aurait 30 jours pour modifier ses pratiques, à défaut de quoi elle s'exposerait à des sanctions pouvant aller jusqu'à 5 000 dollars par utilisateur âgé de moins de 18 ans (§1508).

Focus : Action contre Meta*, People of the State of California v. Meta Platforms, Inc., 4:23-cv-05448, (N.D. Cal.), Oct. 24, 2023*

Depuis octobre 2023, une quarantaine d'États américains poursuivent Meta pour atteinte à la santé mentale des jeunes utilisateurs. Est visée la conception des fonctionnalités des plateformes de médias sociaux Facebook et Instagram concernant le risques de dépendance qu'elle génère auprès des jeunes utilisateurs vulnérables, qui revient à exploiter un « *harmful and psychologically manipulatrice product* » susceptible de leur causer d'importants préjudice afin d'en tirer un

[760] Protecting Our Kids from Social Media Addiction Act, 27005.
[761] Protecting Our Kids from Social Media Addiction Act, 27004(a).
[762] M. Simons, "Ninth Circuit blocks California law protecting kids from social media addiction", *Courthouse News Service*, 28 janv. 2025. Il s'agit de l'affaire *NetChoice v. Bonta*, 2025 BL 879, N.D. Cal., No. 5:24-cv-07885.
[763] Senate Bill S7694A SIGNED BY GOVERNOR

bénéfice financier. Il est également reproché à Meta d'avoir publié des rapports trompeurs faisant état d'une incidence faussement faible des préjudices subis par les utilisateurs. Sont également visés les manquements de Meta à l'égard de ses obligations imposées par le COPPA dès lors qu'auraient été collectées des données de mineurs sans consentement parental. L'enquête fait notamment suite aux révélations de Frances Haugen sur les pratiques de la société Meta.

11.3. PRÉCONISATIONS

Préconisation 40 - S'assurer que tous les principes d'une conception adaptée à l'âge respectueuse de l'intérêt supérieur de l'enfant soient respectés par les réseaux sociaux. Afin de protéger l'utilisateur mineur, s'assurer en particulier de la mise en œuvre efficiente des obligations de paramétrage par défaut afin de protéger l'utilisateur des risques pour sa vie privée, sa sécurité et sa sûreté au regard de la typologie des 5 C (*Contact, Content, Conduct, Consumer, Contract, Cross cutting*) ; dans le même temps, toute modification du paramétrage par défaut doit être pensée dans l'intérêt du mineur et proposée pour atteindre cet objectif ce qui suppose qu'elle soit aisément compréhensible, non excessivement complexe et trop fastidieuse.
Sources :
- Pour le design : Designers éthiques (2023), Concevoir sans dark patterns
- Pour les recommandations algorithmiques : Panoptykon Foundation - People vs BIGTECH, Prototyping User Empowerment et Safe by Default

Préconisation 41 - Imposer au réseau social de démontrer l'absence de caractère trompeur ou addictif de la conception du service pour l'utilisateur final en cas de doute de la part des autorités compétentes (Commission européenne ou autorités nationales).
Source : Parlement européen, Résolution sur la conception addictive des services en ligne et la protection des consommateurs sur le marché unique de l'UE

Préconisation 42 – Promouvoir les travaux de recherche afin d'analyser plus finement les effets produits par l'utilisation de ces services, en particulier pour ce qui concerne le recours aux algorithmes de recommandation hyper-personnalisés afin d'évaluer les effets de dépendance et leur impact sur la santé mentale. A cette fin, promouvoir l'accès aux données aux chercheurs agréées prévue dans le cadre de l'article 40 du DSA.
Sources : Parlement européen, Résolution sur la conception addictive des services en ligne et la protection des consommateurs sur le marché unique de l'UE – Rapport Mission Enfants et Ecrans

Préconisation 43 – Sur la base du résultat de ces études, conduire une réflexion sur l'opportunité d'interdire certaines pratiques visant à capter l'attention de l'utilisateur et à susciter fortement son engagement (information selon laquelle tel autre utilisateur est en ligne / en train d'écrire / a vu le message, notifications artificielles, récompenses pour le temps passé sur la plateforme, défilement infini, lecture automatique de vidéo courtes, flux addictif, etc.). Dès à présent, s'assurer pleinement que les fournisseurs de service de réseaux sociaux respectent leurs obligations d'identifier et de ne pas avoir recours aux schémas d'utilisation qui indiquent ou encouragent des comportements addictifs préjudiciables à la santé mentale et

physique ainsi qu'au bien-être des utilisateurs, dans le respect des articles 34 et 35 et de l'article 28 du DSA.

Préconisation 44 – Imposer dès à présent aux fournisseurs de service de réseaux sociaux de désactiver par défaut pour tous les utilisateurs les fonctionnalités qui augmentent, maintiennent ou étendent artificiellement l'utilisation du service, telles que les récompenses pour le temps passé sur la plateforme, les notifications ou encore, la fonction de défilement infini et la lecture automatique de vidéo courtes (autoplay), ainsi que certains indicateurs d'activité ("en ligne", "en train d'écrire", "vu") ou de réputation ("j'aime").
Remarque : il est proposé d'étendre cette mesure à l'ensemble des utilisateurs en raison des failles des systèmes de vérification de l'âge tout en envisageant d'en permettre toutefois la réactivation
Sources : référentiel Arcep et Arcom sur l'écoconception des services numériques – Parlement européen, Résolution sur la conception addictive des services en ligne et la protection des consommateurs sur le marché unique de l'UE – Rapport Enfants et Ecrans – California Appropriate Code Act – CNCDH, Avis protection de l'intimité des mineurs en ligne

Préconisation 45 – Désactiver par défaut les systèmes de recommandation reposant sur les signaux implicites fondés sur l'engagement pour privilégier les systèmes reposant uniquement sur les signaux explicites fournis par l'utilisateur. Par ailleurs, se fonder sur les données résultant des intérêts déclarés par l'utilisateur lors de la définition de son profil, et ses retours d'information, comme le signal "voir plus, voir moins" / "intéressé, pas intéressé. Pour ce faire, compléter les lignes directrices de l'article 28 qui renvoient dans leur version actuelle à une simple option offerte à l'utilisateur et non un paramétrage par défaut, et étendre cette obligation à l'ensemble des utilisateurs. Garantir que ces préférences influencent directement les recommandations fournies par le système et offrir à l'utilisateur la possibilité de signaler à la plateforme si ses préférences sont insuffisamment prises en compte.
Remarque : il est proposé d'étendre cette mesure à l'ensemble des utilisateurs en raison des failles des systèmes de vérification de l'âge
Sources: Panoptykon Foundation et People vs Big tech, Safe by Default – Knight-Georgestown Institute, Better feeds

Préconisation 46 – Consacrer un droit au paramétrage
a. S'assurer que les services de réseaux sociaux permettent pleinement à leurs utilisateurs de modifier les principaux paramètres en fonction de leurs intérêts afin que leurs interactions ne soient pas orientées par les seuls paramètres prévus par le réseau social ; rendre le design désirable pour rendre ce droit effectif en pratique.
Sources: CNCDH, Avis lutte contre la haine en ligne - CNNum, Votre attention s'il vous plait - Rapport Mission Enfants et Ecrans, proposition 3 - Lignes directrices de l'article 28 DSA
b. Promouvoir l'ouverture d'infrastructure des réseaux sociaux afin qu'ils puissent accéder à des applications tierces ou ajouter des fonctionnalités externes aux interfaces originales et s'éloigner ainsi du modèle sur lequel repose le service.
Sources: CNNum, Cultiver la richesse des réseaux et Assurer notre liberté à l'heure de l'Intelligence artificielle - Rapport Mission Enfants et Ecrans, proposition 2.

Préconisation 47 - Pour éviter les effets délétères d'une sur-exposition à des contenus préjudiciables (effet de spirale), s'assurer de la mise en œuvre pleine et efficace des mesures préconisées par les lignes directrices de l'article 28 et évaluer l'impact de telles mesures en consacrant tout moyen nécessaire à cette fin, y compris le recours à des experts tiers.

Préconisation 48 - Mettre en place, plus généralement, des pratiques d'évaluation pour s'assurer que les paramètres et les informations qui sont fournies aux mineurs concernant les systèmes de recommandation sont présentés de manière accessible et adaptée aux enfants, en organisant de façon indépendante des échanges avec divers panels d'utilisateurs.

Préconisation 49 - Conduire dans les plus brefs délais une réflexion afin d'identifier toute fonctionnalité d'IA in app (intégrée dans un réseau social et reposant sur un système d'intelligence artificielle), dont les agents conversationnels, qu'il conviendrait de prohiber afin de prévenir les risques pour la vie privée, la sûreté et la sécurité, en particulier ceux relatifs à la santé mentale et physique ainsi qu'au bien-être des utilisateurs mineurs.

Préconisation 50 - Prévenir les risques résultant des interactions de l'utilisateur avec un système d'IA in App en garantissant le respect de l'ensemble des dispositifs prévus à cette fin au titre des lignes directrices de l'article 28 du DSA et évaluer de façon périodique leur impact ainsi qu'en imposant des obligations complémentaires à savoir :

a. Imposer aux fournisseurs de ces systèmes de les concevoir en préservant le bien-être et l'autonomie des enfants lors de l'utilisation de ces technologies, en organisant un contrôle rigoureux du respect des obligations

b. S'assurer que, avant leur mise sur le marché, les fournisseurs de ces systèmes procèdent à une évaluation des risques pour la vie privée, la sûreté et la sécurité des utilisateurs mineurs, de façon conforme aux exigences de rigueur au vu des risques encourus

c. Prévoir et évaluer de façon récurrente et rigoureuse l'efficacité des mesures de modération que les fournisseurs de ces systèmes doivent mettre en œuvre afin que ceux-ci ne puissent générés des scénarios ou interactions favorisant des comportements nuisibles à la santé mentale ou physique du mineur, notamment tels que les troubles du comportement alimentaires, la dépression et les idées suicidaires ainsi que la consommation de produits interdits aux mineurs.

d. Permettre aux mineurs et leurs représentants de refuser d'utiliser l'agent conversationnel et de ne pas être incités à l'utiliser, imposer que ce type de fonctionnalité ne soit pas installée par défaut et offrir la possibilité à l'utilisateur de la désinstaller aisément.

CHAPITRE 12 : CONDITIONS D'ACCÈS AU SERVICE TENANT À L'ÂGE

12.1. PRATIQUES

Enjeux et statistiques. L'usage des réseaux sociaux par les mineurs s'avère de plus en plus précoce, massive et ne cesse de croître. Ainsi, si 67% des 8-10 ans étaient déjà inscrits sur les réseaux sociaux en 2024[764], en 2025 l'Arcom relève que 99% des 11 - 17 ans utilisent au moins une plateforme en ligne[765]. L'Ofcom relève, pour le Royaume Uni, qu'"*un tiers des enfants âgés de 8 à 17 ans ayant un profil sur les réseaux sociaux ont indiqué un âge d'utilisateur adulte après s'être inscrits avec une fausse date de naissance*"[766]. Cela inclut "*jusqu'à deux tiers* » des enfants de 8 à 12 ans qui « *ont reçu l'aide d'un parent ou d'un tuteur*"[767]. En France, l'Arcom relève également une utilisation de plus en plus précoce, l'âge moyen lors de la première utilisation d'un réseau social étant de 12,3 ans en 2025[768]. En outre, 62% des mineurs reconnaissent ainsi ne pas avoir déclaré leur vraie date de naissance lors au moins d'une inscription[769].

Définition et distinction. Il convient de distinguer la limitation d'âge, qui conditionne l'accès à une plateforme ou à certaines de ses parties, des procédés techniques d'assurance de l'âge qui permettent de vérifier l'âge effectif des utilisateurs.

"*Age assurance*" (assurance de l'âge) est un terme générique qui désigne "*à la fois les solutions de vérification et d'estimation de l'âge".* Il fait également *"référence aux différents niveaux de certitude que les différentes solutions offrent pour établir un âge ou une fourchette d'âge"*[770]. Cela comprend les technologies permettant à un fournisseur de plateforme en ligne de s'assurer de manière plus ou moins précise, fiable et robuste de l'âge de ses utilisateurs. À ce titre, il convient de distinguer, selon la classification retenue par la Commission européenne[771], les différentes mesures permettant de vérifier l'âge des utilisateurs et qui seront utilisées par les plateformes : l'autodéclaration, l'estimation de l'âge et la vérification de l'âge.

---

[764] Étude online réalisée par l'institut Audirep en mai 2024 pour l'Association e-Enfance/3018 avec le soutien de la Caisse d'Epargne. 1 602 binômes de parents-enfants de 6 à 18 ans scolarisés interrogés (3 204 répondants au total), 2024.

[765] Arcom, Mineurs : Quels risques ? quelle protection ?, Résultats du volet d'étude quantitatif, septembre 2025.

[766] OFCOM, A third of children have false social media age of 18+, 2022.

[767] Ibid.

[768] Arcom, étude préc.

[769] Ibid.

[770] CEN and CENELEC, Workshop agreement, Age appropriate digital services framework, September 2023.

[771] Commission européenne, COMMUNICATION DE LA COMMISSION, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065 (C/2025/5519), 10 octobre 2025, pt 29.

Dans un premier temps, l'autodéclaration est un outil permettant à l'utilisateur de fournir son âge ou de confirmer sa tranche d'âge, soit en fournissant volontairement sa date de naissance ou son âge, soit en cliquant sur un bouton afin de déclarer qu'elle détient l'âge requis pour accéder au contenu[772]. L'estimation de l'âge[773] quant à elle, permet à un fournisseur d'établir qu'un utilisateur est susceptible d'avoir un certain âge, d'appartenir à une certaine tranche d'âge ou d'avoir plus ou moins d'un certain âge[774]. Enfin, la vérification d'âge[775], qui constituera dans la suite du développement notre objet d'étude, repose sur des identifiants physiques ou des sources d'identification vérifiées qui offrent un haut degré de certitude pour déterminer l'âge d'un utilisateur.

Outils mis en place par les plateformes. Depuis quelques années, les réseaux sociaux ont commencé à appliquer des mesures de vérification de l'âge. À titre d'illustration, en 2022, Instagram a commencé à tester un outil de vérification de l'âge pour s'assurer que les utilisateurs ont bien l'âge qu'ils déclarent avoir ; la société a également commencé à utiliser la technologie biométrique pour l'analyse faciale dans certains cas[776]. En parallèle, YouTube a lancé une application dédiée aux enfants et a introduit de nouvelles pratiques en matière de données[777]. Enfin, récemment, Meta a créé Messenger Kids sur Facebook, permettant aux enfants de communiquer uniquement avec des contacts approuvés par leurs parents[778] et a également proposé un nouvel encadrement pour les comptes adolescents sur Instagram selon la classification PG-13[779].

Limites concernant les droits et libertés ainsi que les contournements possibles. Il existe une difficulté à concilier l'impératif de protection des mineurs par le contrôle de l'âge avec le respect des droits et libertés fondamentaux de l'ensemble des utilisateurs de ces services. À ce titre, il est fréquemment soutenu que le contrôle de l'âge serait susceptible d'avoir un impact négatif sur le droit des personnes physiques à l'égard de la protection de leurs données personnelles ainsi que sur d'autres droits et libertés tels que le droit à la non-discrimination, le droit à l'intégrité de la personne, le droit à la liberté et à la sécurité ou encore le droit à la liberté d'expression et d'information[780]. Dans la mesure où ces dispositifs imposent à tout utilisateur de prouver qu'il est majeur, cela revient en effet à renforcer la surveillance en ligne de tous les internautes et à limiter le droit à l'anonymat en ligne[781]. Les méthodes permettant de prouver l'âge des utilisateurs soulèvent également des inquiétudes en matière de cybersécurité ainsi que de risque de violation

---

[772] Commission européenne, Lignes directrices sur l'article 28 du DSA, préc., pt 29.a.
[773] Commission européenne, Lignes directrices sur l'article 28 du DSA, préc., pt 29.b.
[774] A ce titre, v. CEN and CENELEC, Workshop agreement, Age appropriate digital services framework, September 2023.
[775] Commission européenne, Lignes directrices sur l'article 28 du DSA, préc., pt 29.c.
[776] Instagram, Introducing New Ways to Verify Age on Instagram, 2022.
[777] YouTube Kids, YouTube & your child's Google Account.
[778] Messenger Kids.
[779] Sur ce point, v. Chapitre suivant sur le Contrôle parental - Section 1.
[780] En ce sens, v. EDRi, Online age verification and children's rights, octobre 2023.
[781] En ce sens, v. La Quadrature du Net, Projet de loi SREN et accès au porno : identifier les internautes ne résoudra rien, 2023.

de données[782]. En outre, certains relèvent que les solutions de vérification de l'âge ne suffiront pas à elles seules à améliorer la protection des enfants ni à créer un espace en ligne plus sûr et que, sans mesures de sécurité par défaut et dès la conception, les systèmes d'évaluation de l'âge risquent d'exposer les mineurs à des environnements en ligne dangereux, voire d'exclure les majeurs. Au-delà, il convient de relever que les systèmes de vérification de l'âge peuvent être inopérants dès lors que les utilisateurs mineurs peuvent facilement les contourner en utilisant un réseau privé virtuel (VPN). Le Royaume-Uni a récemment ouvert une réflexion sur ce point. Dans un rapport publié le 18 août 2025, la commissaire britannique à l'enfance a souligné que l'entrée en vigueur de l'Online Safety Act s'était immédiatement accompagnée d'une promotion accrue de l'usage des VPN comme moyen de contournement. Pour y remédier, elle propose d'aller plus loin en envisageant une modification du texte afin d'imposer aux fournisseurs de VPN de mettre en place, eux aussi, des dispositifs de vérification de l'âge effectifs.

Par ailleurs, le rapport d'enquête sur les effets psychologiques de TikTok sur les mineurs[783] propose d'interdire l'accès aux réseaux sociaux avant 15 ans et d'après 15 ans, encadrer l'usage plus strictement en établissant à titre d'exemple un couvre-feu numérique pour mieux encadrer l'usage des réseaux sociaux chez les 15-18 ans tout en renforçant le recours aux solutions de contrôle parental et leur efficacité[784]. Si certaines plateformes ont elles-mêmes mis en œuvre certaines restrictions, proposant aux utilisateurs mineurs une expérience limitée sur l'application, cela reste limité et doit être complété par le cadre juridique existant. À titre d'illustration, sur TikTok, certaines fonctionnalités sont obligatoirement limitées en fonction de l'âge de l'utilisateur[785] (pour utiliser la fonction de messagerie directe, plage horaire automatiquement définie de 21 heures à 8 heures pendant laquelle les notifications push sont désactivées pour une certaine tranche d'âge, blocage des lives pour les mineurs, comptes mineurs de moins de 16 ans automatiquement définis comme privés, de même que leur contenu). En outre, le rapport de la Commission d'enquête rappelle qu'au niveau européen, il est nécessaire d'imposer des restrictions d'âge à certains services et fonctionnalités des réseaux sociaux. Il relève qu'une montée en puissance des enquêtes de la Commission européenne serait utile à ce titre, ainsi que le renforcement des leviers d'action du DSA afin de tendre vers un numérique plus éthique et responsable en "repensant les réseaux sociaux"[786].

[782] BEUC, Better Safe than sorry, BEUC position paper on how to keep children safe online in the EU, BEUC-X-2025-014, février 2025.
[783] Assemblée nationale, RAPPORT FAIT AU NOM DE LA COMMISSION D'ENQUÊTE *sur les* effets psychologiques *de* TikTok *sur les* mineurs, 4 septembre 2025.
[784] Rapport sur les effets psychologiques de TikTok sur les mineurs, préc., p.252 ss.
[785] Rapport sur les effets psychologiques de TikTok sur les mineurs, préc., p.138 ss.
[786] Rapport sur les effets psychologiques de TikTok sur les mineurs, préc., p.220 ss.

12.2. CADRE JURIDIQUE

12.2.1. France et Union européenne

Textes nationaux et européens concernant le contrôle de l'âge. Des conditions relevant de l'âge sont requises à différents égards pour encadrer l'accès aux réseaux sociaux ou aux contenus partagés par leurs services à la fois en droit français et européen[787]. Elles tiennent aux traitements des données des données à caractère personnel (1), aux obligations imposées aux plateformes au titre des services numériques qu'elles délivrent (2), à l'accès, par les mineurs français, aux réseaux sociaux (3) ou encore aux contenus pornographiques (4). Une vérification de l'âge en ligne est également rendue possible avec le règlement eIDAS (*Electronic Identification And trust Services)* qui vise notamment à créer un cadre européen de confiance pour l'identité numérique et l'authentification (5) et les moyens de mise en œuvre sont précisés dans les lignes directrices de la Commission européenne publiée dans leur version définitive le 14 juillet 2025 (6).

1. Contrôle de l'âge et traitement des données à caractère personnel : *Règlement général sur la protection des données (RGPD) et Loi informatique et libertés (LIL)*

Le cadre légal posé par le RGPD. La vérification de l'âge des utilisateurs découle implicitement de l'article 8 du RGPD qui pose un seuil d'âge à partir duquel le mineur peut consentir seul au traitement de ses données à caractère personnel. Les deux premiers alinéas dudit article prévoient en effet que "*le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en dessous de 13 ans. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles* ".

Ces dispositions ont été complétées par l'analyse du groupe 29, institution prédécesseur du Comité européen de la protection des données (CEPD). Celui-ci a adopté des lignes directrices sur le consentement le 28 novembre 2017 qui ont été révisées en 2018[788]. Le document précise que "*lorsqu'ils fournissent des services de la société de l'information à des enfants en se fondant sur le consentement, les responsables du traitement devront s'efforcer raisonnablement de vérifier que l'utilisateur a dépassé l'âge minimum de consentement numérique ; ces efforts devraient être proportionnels à la nature des activités de traitement et aux risques qui y sont liés*". Il précise

[787] Pour une étude approfondie, v. A. Humain-Lescop, *Towards Harmonised Online Age Verification? A Comparative Study of French and EU Legal Frameworks* (January 02, 2025). Forthcoming publication by the Digital, Governance and Sovereignty Chair at Sciences Po, 2025.

[788] Groupe de travail "Article 29", Lignes directrices sur le consentement au sens du règlement 2016/679; Adoptées le 28 novembre 2017, Version révisée et adoptée le 10 avril 2018.

également que "*la vérification de l'âge de la personne concernée ne doit pas entraîner un traitement de données supplémentaire excessif. Le mécanisme choisi pour vérifier l'âge d'une personne concernée devrait comprendre une évaluation des risques liés au traitement envisagé*"[789].

Par ailleurs, lors de sa réunion plénière de février 2025, le CEPD a adopté une déclaration sur l'assurance de l'âge[790]. Les principes proposés visent à concilier la protection des mineurs et la protection des données personnelles de l'ensemble des individus dans le contexte de l'assurance de l'âge. La priorité a été donnée au traitement des exigences concernant les principes fondamentaux énoncés à l'article 5 du RGPD (licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, confidentialité, intégrité et responsabilité), et à garantir que ces principes de protection des données sont correctement mis en œuvre et restent robustes dans le temps, conformément à l'article 25 du RGPD "Protection des données dès la conception et protection des données par défaut" et à l'article 32 du RGPD "Sécurité du traitement". Cette déclaration se concentre sur les principes applicables à différents cas d'utilisation en ligne, notamment lorsqu'un âge minimum est prescrit par la loi ou autrement pour l'achat de produits, pour l'utilisation de services susceptibles de nuire aux enfants ou pour l'accomplissement d'actes juridiques ; et lorsqu'il existe un devoir de diligence pour protéger les enfants.

Le cadre légal posé par la LIL. En France, l'âge à partir duquel un mineur peut consentir seul aux traitements de ses données personnelles a été fixé à 15 ans par la loi Informatique et Libertés. Comme rappelé par la CNIL, "*l'article 45 de la loi Informatique et Libertés prévoit que, dans le cadre des services en ligne et pour les traitements de données qui reposent sur le consentement non contractuel de l'utilisateur, le ou les titulaires de l'autorité parentale doivent donner leur accord conjointement avec celui de leur enfant si celui-ci a moins de 15 ans. Cela signifie que le consentement pour des fonctionnalités supplémentaires telles que le choix d'un profil public ou privé sur un réseau social ou l'activation de la géolocalisation optionnelle sur une application doit théoriquement résulter d'un commun accord de l'enfant et du ou des titulaires de l'autorité parentale. Autrement dit, les parents ne peuvent, pour ces traitements, aller contre la volonté de l'enfant et l'enfant passer outre l'opposition de ses parents. En revanche, pour les traitements de données qui résultent de contrats conclus en ligne avec le prestataire de service, soit le mineur peut conclure lui-même un tel contrat, soit les titulaires de l'autorité parentale peuvent seuls le conclure pour lui*"[791]. Selon la CNIL, l'ouverture d'un compte de réseau social n'est pas considérée comme un acte usuel de la vie courante et suppose l'accord de l'enfant et des parents[792].

2. Contrôle de l'âge et accès à des contenus sur les plateformes : la Directive SMA et le DSA

[789] Ibid.
[790] European Data Protection Board, Statement 1/2025 on Age Assurance, Adopted on 11 February 2025.
[791] CNIL, Recommandation 4 : rechercher le consentement d'un parent pour les mineurs de moins de 15 ans, 9 juin 2021.
[792] Ibid.

Directive Services de médias audiovisuels (SMA). Les articles 6 bis paragraphe 1) 28 ter de la directive dite SMA, transposée par les États membres dans leur droit national, soulignent la possibilité de mettre en œuvre des mesures de vérification de l'âge. Ainsi, les États membres peuvent imposer des mesures visant à mettre en place et utiliser des systèmes permettant de vérifier l'âge des utilisateurs des plateformes de partage de vidéos en ce qui concerne les contenus susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs.

Dans un projet de rapport du Parlement européen[793], il est proposé de réviser la directive SMA afin de renforcer la protection des mineurs face aux contenus préjudiciables diffusés en ligne. À ce titre, la Commission serait invitée à réévaluer la portée des définitions actuelles de la directive afin de s'assurer qu'elles englobent l'ensemble des services audiovisuels pertinents, notamment ceux proposés par les influenceurs et les créateurs de contenus professionnels. En outre, il est préconisé d'étendre certaines dispositions essentielles de ladite directive, en particulier celles relatives à la transparence de la publicité et à la protection des mineurs, aux grandes plateformes de partage de vidéos. Cela permettrait ainsi de rapprocher les responsabilités des plateformes de celles des fournisseurs de services de médias traditionnels et de combler les failles réglementaires persistantes en matière de protection des jeunes publics.

Règlement sur les services numériques (DSA). Les mineurs sont considérés comme une catégorie particulièrement vulnérable des destinataires de services intermédiaires en ligne. À ce titre, l'article 28 du DSA consacre des obligations spécifiques pour garantir un haut niveau de protection de la vie privée, de la sécurité et de la sûreté des mineurs en ligne. Ce texte comprend également des obligations supplémentaires applicables aux très grandes plateformes en ligne et très grands moteurs de recherche en ligne pour ce qui concerne la protection des mineurs. Ces derniers doivent (i) identifier et (ii) atténuer tout risque systémique pour la protection des mineurs et les droits des enfants (articles 34 et 35). Si le DSA n'impose pas explicitement la vérification d'âge, les lignes directrices publiées en juillet 2025[794] sont venues préciser les moyens de mises en œuvre de telles mesures[795]. Cependant, il est prévu que les très grandes plateformes en ligne et les grands moteurs de recherche en ligne peuvent mettre en place, au titre des mesures d'atténuation des risques prévu par l'article 35 dudit texte, « *l'adoption de mesures ciblées visant à protéger les droits de l'enfant, y compris la vérification de l'âge et des outils de contrôle parental, ou des outils permettant d'aider les mineurs à signaler les abus ou à obtenir un soutien, s'il y a lieu* ». Le contrôle de l'âge est également mentionné par le considérant 71 qui rappelle que l'un des objectifs du DSA réside dans la garantie d'une protection des mineurs utilisateurs de services numériques[796]

---

[793] Parlement européen, Projet de rapport sur l'incidence des médias sociaux et de l'environnement en ligne sur les jeunes (2025/2081(INI)), Commission de la culture et de l'éducation, 10 septembre 2025.

[794] Commission européenne, Lignes directrices sur l'article 28 du DSA, préc., pt.6.1.

[795] V. développement (6) sur les Lignes directrices de la Commission européenne.

[796] V. not. DSA, considérant 71 : « *La protection des mineurs est un objectif stratégique important de l'Union. Une plateforme en ligne peut être considérée comme accessible aux mineurs lorsque ses conditions générales permettent aux mineurs d'utiliser le service, lorsque son service s'adresse aux mineurs ou est utilisé de manière prédominante par des mineurs, ou lorsque le fournisseur sait par ailleurs que certains des destinataires de son service sont des mineurs, par exemple parce qu'il traite déjà des données à*

En vertu des dispositions du DSA, la Commission européenne a demandé en juin 2024 aux très grandes plateformes de contenus pornographiques Pornhub, Stripchat et XVideos de lui transmettre des informations sur les mesures qu'elles ont prises pour évaluer et atténuer les risques liés à la protection des mineurs en ligne, ainsi que pour prévenir l'amplification des contenus illégaux et la violence sexiste[797]. La Commission avait exigé notamment des détails sur les mécanismes de garantie de l'âge des utilisateurs adoptés par ces plateformes pornographiques.

En outre, dans le document intitulé "*Une décennie numérique pour les enfants et les jeunes : la nouvelle stratégie européenne pour un internet mieux adapté aux enfants"*[798], la Commission européenne a annoncé qu'elle allait encourager et faciliter l'élaboration d'un code de conduite global de l'UE sur la conception adaptée à l'âge. Le code devrait s'appuyer sur le cadre réglementaire prévu par le DSA tout en étant conforme à la directive SMA et au RGPD.

Par ailleurs, la Commission européenne a mis en place, au début de l'année 2024, un groupe de travail sur la vérification de l'âge avec les États membres afin de soutenir la mise en œuvre du DSA[799]. L'objectif est d'encourager la coopération avec les autorités nationales des États membres ayant une expertise dans le domaine afin d'identifier les meilleures pratiques et normes en matière

---

caractère personnel des destinataires de son service révélant leur âge à d'autres fins. Les fournisseurs de plateformes en ligne utilisées par des mineurs devraient prendre des mesures appropriées et proportionnées pour protéger les mineurs, par exemple en concevant leurs interfaces en ligne ou des parties de celles-ci avec le plus haut niveau de protection de la vie privée, de sécurité et de sûreté des mineurs par défaut, s'il y a lieu, ou en adoptant des normes de protection des mineurs, ou en participant à des codes de conduite pour la protection des mineurs. Ils devraient tenir compte des bonnes pratiques et des orientations disponibles, telles que celles fournies dans la communication de la Commission intitulée "Une décennie numérique pour les enfants et les jeunes: la nouvelle stratégie européenne pour un internet mieux adapté aux enfants". Les fournisseurs de plateformes en ligne ne devraient pas présenter de publicité qui repose sur le profilage utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils savent avec une certitude raisonnable que le destinataire du service est un mineur. Conformément au règlement (UE) 2016/679, et notamment au principe de minimisation des données prévu à l'article 5, paragraphe 1, point c), dudit règlement, cette interdiction ne devrait pas conduire le fournisseur de la plateforme en ligne à conserver, à acquérir ou à traiter davantage de données à caractère personnel qu'il n'en détient déjà afin d'évaluer si le destinataire du service est un mineur. Par conséquent, cette obligation ne devrait pas inciter les fournisseurs de plateformes en ligne à recueillir l'âge du destinataire du service avant l'utilisation de ces plateformes. Ceci devrait s'appliquer sans préjudice du droit de l'Union en matière de protection des données à caractère personnel ».

[797] Commission européenne, "DSA : la Commission demande à Pornhub, XVideos et Stripchat des informations sur les contenus illégaux et la protection des mineurs", communiqué de presse, 14 juin 2024. Il convient de relever que, depuis le 27 mai 2025, Stripchat n'est plus reconnu comme atteignant les seuils pour être qualifié de très grande plateforme.

[798] Commission européenne, Une stratégie européenne pour un meilleur internet pour les enfants (BIK+).

[799] Commission européenne, Working Group 6 of the European Board for Digital Services – Protection of Minors, décembre 2024.

de vérification de l'âge et d'élaborer une approche de l'UE en matière de vérification de l'âge. Cette équipe spéciale est intégrée au groupe de travail 6 dédié à la protection des mineurs du Comité européen des services numériques. Lors de la deuxième réunion de ce groupe de travail en mars 2024, les États membres insistaient sur la nécessité d'une approche harmonisée de l'UE en matière de vérification de l'âge et sur le rôle important du portefeuille d'identité numérique de l'UE à cet égard[800].

Enfin, la Commission européenne a publié en juillet 2025 des lignes directrices sur la protection des mineurs en ligne[801] dans le cadre du DSA. La Commission européenne a envisagé plusieurs recommandations permettant une mise en œuvre effective des mesures d'assurance de l'âge au niveau européen[802].

3. Contrôle de l'âge et accès aux réseaux sociaux : Loi majorité numérique

Le cadre légal posé par la Loi majorité numérique. Bien qu'il n'existe pas de définition générale de la majorité numérique, la France a été l'un des premiers pays, avec la loi du 7 juillet 2023 visant à instaurer une majorité numérique[803], "*à prévoir un cadre légal pour l'inscription des mineurs sur les réseaux sociaux*"[804]. Cette loi ne consacre pas un régime spécial de la capacité d'exercice du mineur dans l'environnement numérique mais prévoit diverses obligations pour les fournisseurs de services réseaux sociaux et modifie la LCEN. Précédemment, une obligation similaire avait été posée pour d'autres types de services numériques, la loi du 30 juillet 2020 prévoyant l'obligation pour les sites pornographiques de mettre en place un contrôle de l'âge de leurs visiteurs[805].

Ce texte prévoit de s'appliquer aux comptes déjà créés et détenus par des mineurs de moins de 15 ans, les réseaux sociaux ayant deux ans pour recueillir l'accord des titulaires de l'autorité parentale sur ce dernier. Selon la loi, lors de l'inscription du mineur de moins de 15 ans, les entreprises doivent également l'informer, ainsi que les titulaires de l'autorité parentale, sur les risques liés aux usages numériques et les moyens de prévention ainsi que concernant les conditions d'utilisation de ses données et l'existence de ses droits, tels que garantis par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elles sont également tenues d'activer un dispositif permettant de contrôler le temps d'utilisation de leur service par le mineur de moins de 15 ans et de l'informer régulièrement de cette durée par des notifications[806]. Il est également prévu que les fournisseurs de services de réseaux sociaux soient tenus de vérifier l'âge des utilisateurs et

---

[800] Commission européenne, Deuxième réunion de l'Équipe spéciale sur la vérification de l'âge, 20 mars 2024.

[801] Commission européenne, Lignes directrices sur l'article 28 du DSA, préc.

[802] V. développement (6) sur les Lignes directrices de la Commission européenne.

[803] Loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne.

[804] T. Petelin, "La majorité numérique en question : Commentaire de la loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne", *Dalloz IP/IT* 2023. 667.

[805] Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales, art. 23.

[806] Ibid.

l'autorisation de l'un des titulaires de l'autorité parentale en utilisant des solutions techniques conformes à un référentiel élaboré par l'Arcom, après consultation de la CNIL. Le fait pour un fournisseur de services de réseaux sociaux en ligne de ne pas satisfaire à ces obligations peut être puni d'une amende ne pouvant excéder 1 % de son chiffre d'affaires mondial pour l'exercice précédent. Enfin, la loi permet également à tout titulaire de l'autorité parentale sur le mineur de moins de 15 ans de pouvoir demander aux réseaux sociaux la suspension du compte de ce dernier[807].

Quant aux sanctions[808], la loi prévoyait que "*lorsqu'un fournisseur de services de réseaux sociaux en ligne n'a pas mis en œuvre de solution technique certifiée pour vérifier l'âge des utilisateurs finaux et l'autorisation de l'un des titulaires de l'autorité parentale de l'inscription des mineurs de quinze ans, l'Arcom adresse à ce fournisseur, une mise en demeure de prendre toutes les mesures requises pour satisfaire aux obligations. Le fournisseur dispose d'un délai de quinze jours à compter de la mise en demeure pour présenter ses observations"*. À défaut de mise en conformité, une amende peut être prononcée dont le montant peut s'élever jusqu'à 1% du chiffre d'affaires mondial de la plateforme.

Une loi à l'application compromise. Cette loi devait entrer en vigueur à "*une date fixée par décret qui ne peut être postérieure de plus de trois mois à la date de réception par le Gouvernement de la réponse de la Commission européenne permettant de considérer le dispositif législatif lui ayant été notifié comme conforme au droit de l'Union européenne*"[809]. Les décrets d'application n'ayant pas été publiés et la conformité de la loi au droit de l'Union ayant été contesté, la loi n'est pas entrée en application. C'est une approche européenne sur la vérification de l'âge mise en place par la Commission européenne qui est désormais discutée[810].

4. Contrôle de l'âge et accès aux contenus pornographiques : Loi sécuriser et réguler l'espace numérique (SREN)

L'arsenal législatif concernant l'interdiction d'accès des mineurs aux sites pornographiques a été récemment complété par la loi SREN pour l'accès aux contenus pornographiques[811]. Ainsi, le nouvel article 10-I de la LCEN créé par l'article 1 de loi SREN prévoit que "*L'Autorité de régulation de la communication audiovisuelle et numérique veille à ce que les contenus pornographiques mis à la disposition du public par un éditeur de service de communication au public en ligne, sous sa responsabilité éditoriale, ou fournis par un service de plateforme de partage de vidéos, au sens de l'article 2 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, ne soient pas accessibles aux mineurs"*. Par ailleurs, la loi SREN confie

[807] Ibid.

[808] Loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, article 4-II.

[809] Loi n°2023-566 , art. 7.

[810] European Commission, The EU approach to age verification, july 2025.

[811] Sur ce point, v. les développements consacrés à l'exposition à des contenus à caractère pornographique.

à l'Arcom un pouvoir de blocage administratif des services de communication au public en ligne ayant une responsabilité éditoriale et des services de plateforme de partage de vidéos diffusant des contenus à caractère pornographique qui resteraient accessibles aux mineurs après avoir été mis en demeure de se conformer à l'article 227-24 du Code pénal.

Afin de respecter les exigences du droit de l'Union européenne, la loi SREN opère une distinction entre, d'une part, les sites établis au sein de l'UE et, d'autre part, ceux établis en France et hors UE pour restreindre l'obligation de vérification de l'âge des utilisateurs uniquement à ces derniers. Ainsi, les sites concernés pourront être mis en demeure par l'Arcom d'appliquer les règles sous 30 jours sous peine de sanctions. Les services pourront adopter la solution de leur choix pour la vérification de l'âge de leurs utilisateurs tant qu'ils respectent les conditions posées par le référentiel (fiabilité et respect de la vie privée). Si la vérification par la carte bancaire est admise à titre temporaire pour une durée de 6 mois et sous certaines conditions, la vérification de l'âge devra ensuite se conformer au référentiel de l'Arcom en proposant au moins un dispositif reposant sur le double anonymat et respectant les conditions de fiabilité et de respect de la vie privée. Ces services mettant en place des systèmes de vérification de l'âge devront en outre se conformer aux exigences du RGPD (droit d'accès, droit de retrait, limitation du traitement…). Les services mettant à disposition du contenu pornographique en ne respectant pas ce référentiel encourent une procédure de blocage administratif décidée par l'Arcom.

Afin de préciser le respect de ces dispositions, un référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge est publié par l'Arcom après avis de la CNIL[812] *"conformément à l'article 1er de la loi SREN précisant que ces exigences portent sur la fiabilité du contrôle de l'âge des utilisateurs et sur le respect de leur vie privée. Ce référentiel est actualisé en tant que de besoin dans les mêmes conditions*". Ce référentiel soulève des défis techniques, éthiques et légaux liés à la mise en place de tels dispositifs, tout en insistant sur le respect des principes fondamentaux de protection des données personnelles comme rappelé par la CNIL dans son avis du 26 septembre 2024 concernant le référentiel proposé par l'Arcom sur la vérification de l'âge en ligne[813].

Une première version de ce référentiel a été publié en octobre 2024[814]. En substance, il est prévu que la vérification de l'âge soit effectuée par un prestataire de système de vérification de l'âge indépendant du site pornographique. Par ailleurs, après une période transitoire, les sites concernés devront proposer aux internautes au moins une solution de vérification de l'âge dite en "*double anonymat*". Ce référentiel, qui est présenté comme une mesure temporaire, vise à éviter que des mineurs accèdent à des contenus inappropriés. Bien qu'il conserve les lignes directrices du projet soumis à consultation en avril, il propose des ajustements, notamment une formulation plus

[812] Loi SREN, article 1.

[813] CNIL, Délibération n° 2024-067 du 26 septembre 2024 portant avis sur un projet de référentiel de l'Autorité de régulation de la communication audiovisuelle et numérique (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.

[814] Arcom, Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne, oct. 2024.

nuancée en introduisant des « considérations générales » au lieu de critères stricts. L'Arcom précise certains points sur la non-discrimination des utilisateurs et l'absence de contournement de ces mesures. Ce référentiel, qui s'applique aux sites français, extra-européens et européens sans législation en place, laissera un délai de trois mois aux sites pour se conformer aux principes initiaux, avec une période transitoire d'usage des cartes bancaires pour une durée de trois mois supplémentaires. L'Arcom souligne l'urgence d'adopter des solutions, en attendant l'émergence d'un standard européen.

Depuis le 11 janvier 2025, les sites pornographiques hébergés en France ou en dehors de l'Union européenne doivent mettre en place des systèmes de vérification de l'âge conformes aux neuf exigences du référentiel technique. Les acteurs concernés avaient jusqu'au 11 avril 2025 pour se conformer aux nouvelles obligations de la loi SREN. En cas de non-respect des exigences énoncées dans le référentiel, l'Arcom peut mettre en demeure les services de s'y conformer, puis si le manquement perdure, elle peut prononcer une sanction pécuniaire.

Le 6 mars 2025, l'Arcom a annoncé avoir constaté qu'aucun des six services parmi les plus fréquentés n'avait mis en œuvre un système de vérification de l'âge. L'un d'entre eux n'avait pas non plus rendu disponibles l'identité de son fournisseur, ni son adresse, en violation de la loi SREN ce qui a conduit l'Arcom a adressé à plusieurs fournisseurs d'accès à internet, fournisseurs de systèmes de résolution de noms de domaine et moteurs de recherche des demandes de blocage ou de déréférencement, visant à garantir que l'accès au site contrevenant soit empêché. Pour les cinq autres services, l'Arcom a décidé d'envoyer, comme prévu par la loi, des lettres d'observations, première étape à un éventuel blocage si le manquement devait perdurer[815]. Ce même jour, a été publié un arrêté listant 17 sites pornographiques soumis à l'obligation de mise en conformité avec les règles de vérification de l'âge, conformément à la loi SREN dont Pornhub, XNXX, Xvideos, YouPorn et RedTube[816]. Le lendemain de cet arrêté, la société Aylo (qui détient notamment Pornhub, YouPorn et RedTube) a annoncé qu'elle allait contester celui-ci en justice[817] considérant la vérification de l'âge « *inefficace, hasardeuse et dangereuse* » et invoquant des risques pour la protection des données personnelles des utilisateurs. Elle plaide pour une solution alternative consistant à vérifier l'âge directement sur l'appareil de l'utilisateur. [818]. Le 15 avril 2025, le tribunal administratif de Paris a rejeté un recours contre la décision de l'Arcom du 6 mars 2025 enjoignant à la société Cloudflare de bloquer le site de la plateforme Camschat de partage de vidéos pornographiques dans un délai de quarante-huit heures[819]. Le tribunal a jugé que le dispositif de

[815] Arcom, Pornographie en ligne : de nouvelles étapes franchies pour la protection des mineurs, 6 mars 2025

[816] Arrêté du 26 février 2025 désignant les services de communication au public en ligne et les services de plateforme de partage de vidéos établis dans un autre État membre de l'Union européenne soumis aux articles 10 et 10-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°0056 du 6 mars 2025.

[817] Pour plus d'informations, v. K. Durand et É. Marzolf, "Contrôle de l'âge : l'Arcom se prépare à débrancher Pornhub dès cet été", *Politico*, 11 avril 2025.

[818] Sur ce risque de contentieux, v. L. Huttner, "Le contrôle de l'accès des mineurs aux sites pornographiques", *Dalloz IP/IT* 2024, 7, pp. 400.

[819] Tribunal administratif de Paris, 5ème section - 4ème chambre, décision N° 2506972/5-4. Voir le communiqué de presse.

contrôle par l'Arcom porte une atteinte proportionnée aux libertés d'entreprise et d'expression. Il a en effet relevé que la loi poursuit l'objectif légitime d'empêcher l'accès des mineurs à des contenus à caractère pornographique en ligne et qu'aucun dispositif moins attentatoire à l'exercice des droits ne permet d'atteindre cet objectif. Le tribunal a jugé que le dispositif de contrôle par l'Arcom porte une atteinte proportionnée aux libertés d'entreprise et d'expression. Il a en effet relevé que la loi poursuit l'objectif légitime d'empêcher l'accès des mineurs à des contenus à caractère pornographique en ligne et qu'aucun dispositif moins attentatoire à l'exercice des droits ne permet d'atteindre cet objectif.

En outre, par un arrêt rendu le 22 juillet 2025[820], la cour administrative d'appel de Paris a jugé que l'Arcom peut enjoindre à un service de bloquer l'accès des utilisateurs français à une plateforme de partage de vidéos pornographiques qui ne mettrait pas en place une solution effective permettant de vérifier l'âge[821].

Enfin, en application de la loi SREN du 21 mai 2024, l'Arcom[822] avait mis en demeure, le 1er août 2025, cinq sites pornographiques établis dans l'Union européenne et désignés par l'arrêté ministériel du 26 février 2025[823] pour absence de vérification de l'âge. Ayant ensuite constaté que, depuis, les sites concernés avaient mis en place une ou plusieurs solutions de vérification de l'âge, le collège de l'Arcom a pris la décision de ne pas engager de procédure de blocage et de déréférencement à leur égard. Le collège a également décidé de ne pas mettre en demeure un sixième site pornographique qui avait de nouveau activé son système de vérification de l'âge après avoir reçu une lettre d'observations envoyée début août.

5. Contrôle de l'âge et identité numérique : le Règlement eIDAS2

Cadre légal du Règlement eIDAS. Le règlement n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement "eIDAS "[824], vise à faciliter la sécurité des transactions transfrontalières en établissant un cadre pour l'identité numérique et l'authentification. Il s'agit de garantir la confiance dans les interactions électroniques et de promouvoir des services numériques homogènes dans l'Union

[820] CA Paris, N° 25PA02012, 22 juillet 2025.
[821] Cour administrative d'appel de Paris, Sites pornographiques accessibles aux mineurs : l'Arcom peut imposer le blocage de l'accès aux plateformes, 22 juillet 2025.
[822] Arcom, Communiqué de presse - Protection des mineurs en ligne : l'Arcom constate la mise en place de dispositifs de vérification de l'âge par six nouveaux sites pornographiques, 28 août 2025.
[823] Arrêté du 26 février 2025 désignant les services de communication au public en ligne et les services de plateforme de partage de vidéos établis dans un autre État membre de l'Union européenne soumis aux articles 10 et 10-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[824] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

européenne et ce, en constituant un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

Le règlement eIDAS se divise en deux parties distinctes. La première concerne l'harmonisation des systèmes d'identification électronique au sein de l'Union européenne. Elle impose aux administrations publiques des États membres de reconnaître les identifiants électroniques de leurs homologues européens afin de l'accès aux services en ligne pour l'ensemble des citoyens de l'UE. La seconde partie du règlement eIDAS porte sur les signatures électroniques.

Ce texte définit trois niveaux qui permettent d'apporter une garantie sur l'identité qui est fournie au fournisseur de service avec des exigences différentes :

- Faible : l'objectif est simplement de réduire le risque d'utilisation abusive ou d'altération de l'identité ;
- Substantiel : l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- Élevé : l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

À titre illustratif, FranceConnect délivre des identités de niveau faible aux fournisseurs de service, quel que soit le fournisseur d'identité utilisé.

Révision du texte et introduction des portefeuilles numériques. Le 20 mai 2024, une révision du règlement eIDAS datant de 2014 est intervenue avec la publication du règlement "eIDAS 2" n°2024/1183[825]. Bien que l'ambition du texte demeure inchangée, la principale nouveauté du texte repose sur l'obligation pour les États membres de délivrer des portefeuilles européens d'identité numérique devant être opérationnels d'ici la fin de l'année 2026 afin de permettre notamment aux citoyens de s'identifier électroniquement avec un niveau de garantie élevé. Le portefeuille d'identité numérique désigne selon l'article 2, j), 42, "*un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifié*s". Ces portefeuilles permettront donc aux individus de s'identifier numériquement, de stocker et de gérer leurs données d'identité et leurs documents officiels tels que des permis de conduire des prescriptions médicales ou des diplômes sous un format électronique.

Lien du Règlement eIDAS2 avec le contrôle de l'âge. Les portefeuilles européens d'identité numérique pourront permettre aux individus de prouver leur identité lorsque cela est nécessaire pour accéder aux services en ligne, pour partager des documents numériques, ou simplement pour prouver un attribut personnel spécifique, tel que l'âge, sans révéler leur identité ou d'autres données personnelles. Bien que les portefeuilles européens d'identité numérique ne soient pas

[825] Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique, JOUE, 2024/1183, 30.4.2024.

mentionnés dans le cadre du DSA, le règlement eIDAS mentionne leur utilisation pour la vérification de l'âge.

Lors d'une réunion informelle des ministres de l'UE responsables du portefeuille des télécommunications des 11 et 12 avril 2024, a été signée à Louvain-La-Neuve une déclaration intitulée "*Declaration on promoting a safer, responsible and trustworthy online environment*"[826]. Cette déclaration appelle à une application rigoureuse et efficace du DSA et des portefeuilles européens d'identité numérique afin de mieux protéger les mineurs en ligne et d'assurer une expérience en ligne sûre, saine et adaptée à leur âge. Ce texte invite la Commission européenne à élaborer des directives destinées aux plateformes en ligne, afin d'assurer un niveau de confidentialité, de sécurité et de sûreté adéquat pour tous les utilisateurs, en particulier les mineurs, ainsi que sur la manière d'atténuer les risques systémiques particulièrement importants pour la protection des enfants. Ce document promeut le recours à des outils de vérification de l'identité numérique et de l'âge, tels que les portefeuilles d'identité numérique. Les signataires de la déclaration ont également envisagé d'harmoniser les normes techniques de vérification de l'âge en ligne à l'échelle de l'Union européenne, en utilisant les fonctionnalités offertes par les portefeuilles numériques européens

Dans ce contexte, la Commission européenne a lancé, le 15 octobre 2024, un appel d'offres pour le développement, le conseil et le soutien d'une solution de vérification de l'âge avec un budget de 4 millions d'euros[827]. Il est précisé que cet appel d'offres vise "*à élaborer des spécifications techniques, avec les contributions des États membres et d'autres parties prenantes, pour une solution de vérification de l'âge préservant la vie privée*"[828]. Cela pourrait prendre la forme d'une application en marque blanche prenant en charge un protocole de preuve de connaissance zéro qui peut être localisé et publié par les États membres dans les boutiques d'applications. Les protocoles de preuve de connaissance zéro (en anglais "*Zero-knowledge proofs*") permettent de vérifier la véracité d'un attribut sans divulguer d'autres détails[829].

Depuis, la Commission a publié, le 14 juillet 2025, une version initiale du blueprint européen de vérification de l'âge permettant de tester une solution harmonisée, interopérable et respectueuse de la vie privée[830]. Ce blueprint prendra la forme d'un "mini-wallet" de vérification d'âge, aligné sur les spécifications techniques du futur portefeuille d'identité numérique européen (EUDI Wallet), ce qui garantit sa compatibilité future[831].

Dans le cadre de ce projet, des États membres tels que la France, l'Italie, l'Espagne, le Danemark et la Grèce testeront cette solution de vérification de l'âge, éventuellement intégrée dans leur

---

826 Informal Telecom Council, Louvain-La-Neuve Declaration on promoting a safer, responsible and trustworthy online environment, 11-12 April 2024.

827 Commission européenne, Appel d'offres: Développement, conseil et assistance pour une solution de vérification de l'âge, 16 oct. 2024.

828 Ibid.

829 Sur le fonctionnement technique des portefeuilles numériques : Commission européenne, Security and privacy : The security and privacy features of EU Digital Identity Wallets.

830 European Commission, Commission makes available an age-verification blueprint, 14 july 2025.

831 European Commission, The EU approach to age verification.

portefeuille national ou déployée en tant qu'application nationale autonome[832]. L'utilisateur pourra prouver qu'il est majeur sans partager d'autres données personnelles puisque le service concerné ne recevra qu'une attestation de majorité. Enfin, ce projet de "blueprint" prévoit l'intégration des notions de minimal disclosure, unlinkability, et données non persistantes, pour limiter les risques de suivi ou de profilage[833].

Mise en place de portefeuilles d'identité numérique par les États membres avec des dispositifs de contrôle de l'âge. L'Espagne est l'un des premiers pays à avoir divulgué, en juillet 2024, un portefeuille d'identité numérique pour aider les plateformes pornographiques à vérifier l'âge des utilisateurs. L'application, baptisée Cartera Digital Beta, permet aux plateformes de vérifier si un consommateur de contenu pornographique est majeur[834]. Les utilisateurs souhaitant accéder à du contenu pornographique sont ensuite invités à utiliser l'application pour vérifier leur âge. Une fois la vérification effectuée, ils reçoivent des crédits pornographiques valables un mois, leur donnant accès à des contenus pornographiques[835].

La Grèce a également annoncé le lancement de l'application Kids Wallet qui permettra de vérifier l'âge des utilisateurs et de lutter contre la dépendance en ligne des mineurs. Ce système de vérification de l'âge s'appuiera sur l'identité numérique grecque d'un parent ou d'un tuteur, validée par TaxisNet, le service national d'autorisation du pays[836]. Selon le média Euractiv, le représentant légal du mineur pourra sélectionner le profil de ce dernier sur l'application d'identification numérique, qui validera le profil du mineur avec des données du registre civil national[837]. L'application sera en mesure de déterminer l'âge de l'enfant en fonction de sa date de naissance et des applications tierces pourraient récupérer l'âge de l'enfant via une API avec le consentement des parents. L'application Kids Wallet s'accompagne également de conseils parentaux. Le représentant légal est aussi en mesure de sélectionner les applications que le mineur sera autorisé à utiliser, fixer des limites de temps et bloquer des applications spécifiques.

La Grèce présidera le Conseil de l'Union européenne en 2027 et a déclaré faire de la protection des mineurs en ligne une de ses priorités. Elle plaide pour un "*âge de majorité numérique*" fixé à 15 ans, qui nécessiterait le consentement explicite des parents pour l'utilisation des réseaux sociaux par les mineurs en dessous de cet âge[838]. La Grèce souhaite également que tous les appareils vendus dans l'UE et disposant d'un accès à Internet soient équipés d'un logiciel de contrôle parental intégré obligatoire.

---

[832] European Commission, Commission makes available an age-verification blueprint, 14 july 2025.
[833] EFF, Age Verification in the European Union: The Commission's Age Verification App, 29 avril 2025.
[834] Ministerio para la transformación digital y de la función pública, Especificaciones técnicas para la herramienta de verificación de edad
[835] Plus d'informations: D. Vidal, "Espagne : un « passeport » virtuel pour bloquer l'accès des mineurs aux films pornographiques", Ouest-france.fr, 3 juillet 2024.
[836] Anupriya Datta et Claudie Moreau, "La Grèce lance « Kids Wallet » pour inciter l'UE à agir contre la dépendance en ligne des mineurs", Euractiv.fr, 13 mars 2025.
[837] Ibid.
[838] Ibid.

6. Les lignes directrices de la Commission européenne

La Commission européenne, dans ses lignes directrices d'application du règlement (UE) 2022/2065 relatif aux services numériques (DSA)[839], consacre un développement spécifique à la question de la vérification de l'âge des utilisateurs en ligne en retenant une approche par les risques. Elle rappelle que le recours à des restrictions d'accès fondées sur des méthodes de vérification de l'âge peut constituer une mesure appropriée et proportionnée pour assurer un haut niveau de protection de la vie privée, de la sûreté et de la sécurité des mineurs[840].

La Commission identifie plusieurs situations dans lesquelles le recours à de telles mesures se justifie. Premièrement, lorsqu'il s'agit de produits ou services présentant un risque élevé pour les mineurs et que ces risques ne peuvent être réduits par des mesures moins restrictives. Sont expressément mentionnés la vente d'alcool, de tabac ou de produits liés à la nicotine, l'accès à des contenus pornographiques, ainsi que l'accès aux jeux d'argent[841]. Deuxièmement, lorsque les conditions générales d'utilisation ou les obligations contractuelles d'un service imposent un âge minimum de 18 ans, même en l'absence d'exigence légale formelle, en raison de risques spécifiques identifiés pour les mineurs[842]. Troisièmement, dans toute hypothèse où un fournisseur de plateforme en ligne accessible aux mineurs a identifié des risques pour leur vie privée, leur sécurité ou leur sûreté. Ces risques peuvent être liés aux contenus et aux pratiques commerciales, mais également aux fonctionnalités techniques facilitant les contacts non sollicités (chat en direct, partage d'images ou de vidéos, messagerie anonyme). Dans ce cadre, le recours à la vérification de l'âge s'impose si aucune autre mesure moins intrusive n'apparaît aussi efficace[843]. Enfin, lorsque le droit de l'Union ou le droit national prévoit un âge minimum pour l'accès à certains produits ou services proposés en ligne, y compris certaines catégories de services de médias sociaux expressément définies par la législation[844].

Toutefois, la Commission européenne précise que la vérification de l'âge ne se limite pas à un contrôle strict et unique. Les méthodes d'estimation de l'âge pourront jouer un rôle complémentaire ou transitoire, en particulier lorsque des solutions de vérification robustes, respectueuses de la vie privée et conformes aux critères définis à la section 6.1.4, ne sont pas encore disponibles[845]. Ces méthodes peuvent, à titre temporaire, remplacer la vérification stricte de l'âge, mais uniquement si elles présentent un niveau de fiabilité comparable, notamment pour les services proposant des contenus réservés aux adultes. La Commission prévoit de compléter ultérieurement les lignes directrices par une analyse technique des méthodes existantes

---

839 Commission européenne, Approval of the content on a draft Communication from the Commission - Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, C(2025) 4764 final, 14 juillet 2025.

840 Commission européenne, Lignes directrices article 28 DSA préc., pt. 37.

841 Commission européenne, Lignes directrices article 28 DSA préc., pt. 37a.

842 Commission européenne, Lignes directrices article 28 DSA préc., pt. 37b.

843 Commission européenne, Lignes directrices article 28 DSA préc., pt. 37c.

844 Commission européenne, Lignes directrices article 28 DSA préc., pt. 37d.

845 Commission européenne, Lignes directrices article 28 DSA préc., pt. 38.

d'estimation de l'âge, afin d'évaluer leur conformité avec les exigences en matière de protection des données, d'exactitude et d'efficacité[846].

Par ailleurs, les lignes directrices de la Commission européenne soulignent la nécessité de distinguer clairement la vérification de l'âge des autres traitements de données réalisés par les plateformes. À ce titre, la vérification de l'âge doit être conçue comme un processus distinct, qui n'autorise pas la collecte ou la conservation de données personnelles au-delà de l'information strictement nécessaire à la détermination de la tranche d'âge de l'utilisateur[847].

Afin d'être considérées comme appropriées et proportionnées, les technologies de vérification de l'âge doivent présenter un caractère robuste et difficilement contournable. Une méthode facilement évitable par les mineurs ne pourra être qualifiée de mesure efficace d'assurance de l'âge au sens du règlement[848]. C'est en ce sens que la Commission envisage plusieurs pistes technologiques.

Tout d'abord, l'utilisation de pièces d'identité délivrées par l'État, associées à des jetons d'âge anonymisés. Ces jetons, émis par un tiers indépendant après une vérification fiable, permettent de confirmer l'âge de l'utilisateur sans transmettre d'autres données personnelles à la plateforme[849]. La Commission considère que les protocoles cryptographiques tels que la rotation des clés ou les preuves à divulgation nulle de connaissance constituent une base appropriée pour fournir une assurance de l'âge sans transmettre de données à caractère personnel. Par ailleurs, le développement des portefeuilles d'identité numérique de l'UE, qui offriront un moyen sécurisé, fiable et respectueux de la vie privée pour partager uniquement l'information pertinente avec un service en ligne, par exemple l'attestation que l'utilisateur a dépassé un certain âge[850].

Dans l'attente de ce déploiement, la Commission expérimente une solution européenne autonome de vérification de l'âge, conçue pour respecter les critères d'efficacité décrits à la section 6.1.4. Cette solution devrait servir de référence normative et offrir un modèle de conformité pour les fournisseurs de services soumis à l'article 28 du règlement[851]. Sa mise en œuvre pourra prendre la forme d'applications publiques ou privées, ou être intégrée directement aux futurs portefeuilles d'identité numérique[852]. La Commission admet que les plateformes puissent recourir à d'autres méthodes de vérification, à condition que celles-ci garantissent un niveau élevé de confidentialité et de sécurité des mineurs, qu'elles soient interopérables et qu'elles respectent les critères de robustesse et de minimisation des données prévus par les lignes directrices[853].

Enfin, les lignes directrices encouragent les plateformes à privilégier des méthodes dites "en double aveugle", afin de garantir le respect des principes de minimisation des données et de limitation des finalités. Concrètement, un tel système empêche à la fois la plateforme d'accéder à des informations supplémentaires permettant d'identifier l'utilisateur, et le fournisseur du service

[846] Ibid.
[847] Commission européenne, Lignes directrices article 28 DSA préc., pt. 39.
[848] Commission européenne, Commission européenne, Lignes directrices article 28 DSA préc., pt. 40.
[849] Commission européenne, Lignes directrices article 28 DSA préc., pt. 41.
[850] Commission européenne, Lignes directrices article 28 DSA préc., pt. 42.
[851] Commission européenne, Lignes directrices article 28 DSA préc., pt. 43.
[852] Commission européenne, Lignes directrices article 28 DSA préc.,, pt. 44.
[853] Commission européenne, Lignes directrices article 28 DSA préc., pt. 45.

de vérification de l'âge de connaître la nature des services pour lesquels la preuve d'âge est utilisée. Ces méthodes peuvent reposer sur le traitement local des dispositifs, sur des jetons cryptographiques anonymisés ou sur des preuves à divulgation nulle de connaissance[854].

12.2.2. États-Unis

Divergence d'approches entre les niveaux fédéral et étatique. Plusieurs projets de lois visant à imposer la vérification de l'âge des utilisateurs pour accéder à du contenu ont été discutés depuis la création d'Internet aux États-Unis. Ces propositions ont connu un essor ces dernières années notamment compte tenu des débats relatifs à l'impact des réseaux sociaux sur la santé mentale des adolescents.

Distinction "*Age verification*" et "*Parental consent*". Dans le cadre de la protection des mineurs en ligne aux États-Unis, la distinction entre la vérification de l'âge et le consentement parental est essentielle. La vérification de l'âge ("*Age verification*") a pour objectif de demander à une personne des informations sur son âge et vérifier la catégorie d'âge de la personne à l'aide d'une méthode ou d'un processus disponible dans le commerce et raisonnablement conçu pour garantir l'exactitude des informations[855]. Si la méthode de vérification de l'âge détermine que la personne est mineure, la plateforme devra exiger que le compte soit affilié à un compte parental et devra obtenir le consentement parental ("*parental consent*") vérifiable du titulaire du compte parental affilié avant d'autoriser le mineur à télécharger ou à acheter une application ou à effectuer un achat intégré à l'application[856].

Au niveau fédéral. Au niveau fédéral, le Children's Online Privacy Protection Act[857] adopté par le Congrès en 1998 impose aux entreprises de limiter la collecte de données personnelles provenant de mineurs sans le consentement de leurs parents[858]. Afin de renforcer la protection des mineurs concernant leurs usages des services numériques, diverses propositions de loi sont en cours d'examen, dont le projet du Kids Online Safety Act (KOSA)[859]. Si ce projet de texte ne doit pas être interprété comme exigeant la mise en œuvre par les plateformes d'une fonctionnalité de contrôle de l'âge (section 10), il mentionne toutefois que le "*Director of the national Institute of standards*", en coordination avec la FTC, mènera une étude afin d'évaluer les moyens les plus réalisables sur le plan technique pour développer des systèmes de contrôle de l'âge. Par ailleurs, le texte précise (section 4.1) qu'une plateforme doit fournir à une personne dont elle sait qu'elle est mineure des mesures de sécurité facilement accessibles et faciles à utiliser en limitant notamment la capacité d'autres personnes à communiquer avec le mineur. En outre la plateforme

---

854 Commission européenne, Lignes directrices article 28 DSA préc., pt. 46.

855 S.737 - SCREEN Act, 119th Congress (2025-2026).

856 Ibid.

857 Children's Privacy. Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505

858 Pour plus de détails, v. partie "Dispositions transversales - Droit américain".

859 S.1409 - Kids Online Safety Act, 118th Congress (2023-2024). Le projet a été présenté une première fois au Sénat en février 2022 (117th Congress) ; une nouvelle version du texte a été introduite en mai 2023 (118th Congress) ; il a été inscrit à l'ordre du jour du Sénat américain pour être examinée en séance plénière.

doit empêcher d'autres utilisateurs, qu'ils soient enregistrés ou non, de consulter les données personnelles du mineur collectées ou partagées sur la plateforme couverte, en restreignant l'accès public aux données personnelles ; en limitant les fonctionnalités qui augmentent, soutiennent ou prolongent l'utilisation de la plateforme concernée par le mineur, telles que la lecture automatique de médias, les récompenses pour le temps passé sur la plateforme, les notifications et autres fonctionnalités qui entraînent une utilisation compulsive de la plateforme concernée par le mineur et enfin, en contrôlant les systèmes de recommandation personnalisés. Le texte est toujours en cours d'examen par le Sénat et fait l'objet de nombreuses divergences de points de vue sur la manière de réguler les acteurs numériques[860].

Par ailleurs, le projet du Kids Off Social Media Act[861] , envisage de limiter l'accès des enfants aux plateformes de réseaux sociaux et exige que ces dernières ainsi que les établissements scolaires mettent en place certaines restrictions concernant l'utilisation des réseaux sociaux par les enfants. Il propose à ce titre qu'aucun compte pour les enfants de moins de 13 ans ne puisse être créé sur la plateforme (section 103). Toutefois, la section 105 précise que cela ne doit pas être interprété comme obligeant une plateforme de médias sociaux à mettre en œuvre une fonctionnalité de contrôle de l'âge ou de vérification de l'âge. Ainsi, la loi exigerait des plateformes de médias sociaux qu'elles prennent des mesures pour supprimer non seulement les utilisateurs dont elles ont "*la connaissance effective"* qu'ils ont moins de 13 ans, mais aussi tous ceux dont elles ont *"la connaissance implicite sur la base de circonstances objectives*". Le texte précise toutefois explicitement qu'aucun contrôle ou vérification de l'âge n'est imposé afin d'éviter que les dispositions enfreignent le Premier amendement relatif à la liberté d'expression. Ce texte vise également à interdire aux entreprises de réseaux sociaux de diffuser du contenu ciblé à l'aide d'algorithmes auprès des utilisateurs de moins de 17 ans. Il est également prévu de confier à la FTC et aux procureurs généraux des États le pouvoir de faire appliquer les dispositions du texte et de suivre le cadre existant de la Children's Internet Protection Act avec des modifications, pour exiger des écoles qu'elles œuvrent de bonne foi à limiter l'utilisation des réseaux sociaux sur leurs réseaux financés par le gouvernement fédéral.

Le projet SCREEN Act[862] quant à lui, entend imposer une vérification de l'âge au niveau fédéral (vérification de l'IP et des VPN). La section 2 décrit les problèmes posés par l'exposition des enfants à des contenus pornographiques et la section 4 de la loi entend obliger les sites pornographiques à adopter des mesures de vérification de l'âge pour s'assurer que les utilisateurs ne sont pas mineurs. Ces mesures ne doivent pas correspondre à la simple saisie de la date de naissance puis qu'est exigée la transparence publique du processus de vérification telle que les adresses IP. Il importe de préciser que cet article interdit aux entreprises de collecter des données au-delà de ce qui est le minimum nécessaire.

---

[860] A. Deysine, "L'impossible régulation des plateformes et des réseaux sociaux aux États-Unis", *La revue européenne des médias et du numérique* n°71, 2024.

[861] S.278 - Kids Off Social Media Act; 119th Congress (2025-2026).

[862] S.737 - SCREEN Act, 119th Congress (2025-2026).

Vérification d'âge sur le magasin d'application. La proposition de loi App Store Accountability Act[863] propose d'imposer aux magasins d'applications ("*AppStore*") des obligations de vérification d'âge des utilisateurs ainsi que d'obtention du consentement parental pour les mineurs. La proposition de loi définit les catégories d'âges[864] et exige que les magasins d'application utilisent des méthodes "*commercialement raisonnables*" pour vérifier ces catégories d'âge[865]. Si l'utilisateur est identifié comme un mineur, le téléchargement d'applications ou les achats in-app ne pourront se faire qu'avec l'accord du parent ou tuteur[866]. En outre, le respect de ces obligations sera assuré par la Federal Trade Commission (FTC) à travers notamment des mécanismes de contrôle, de sanctions[867] et une clause de "*safe harbor*"[868].

Décision de la FTC en lien avec le contrôle de l'âge. En 2024, la FTC a rejeté trois demandes de sociétés qui entendaient mettre en place un nouveau mécanisme de consentement parental s'appuyant sur des technologies biométriques pour déterminer l'âge d'un utilisateur, cette décision étant prise sur la base de l'approbation d'un système d'estimation de l'âge du visage protégeant la vie privée. La FTC a confirmé que cela soulevait des difficultés quant aux capacités de collecte et de stockage des données, et en particulier en ce qui concerne la génération de deepfakes[869].

Au niveau étatique. En 2022, la Louisiane a été le premier État à adopter une loi imposant une vérification de l'âge pour accéder à des sites contenant une part de contenus pour adultes [870], à ce titre les plateformes sont désormais tenues de recourir à des systèmes capables de vérifier un justificatif d'identité ou des données transactionnelles pour s'assurer que l'utilisateur a au moins 18 ans. Depuis 2023, 22 États ont introduit ou voté des textes imposant des formes de vérification de l'âge notamment pour l'accès aux contenus pornographiques ainsi que pour l'accès aux réseaux sociaux[871]. Certains imposent une forme de majorité numérique[872]. Cependant, certaines de ces lois ont été remises en question par les tribunaux de certains États, notamment en Arkansas[873] pour violation du 1er amendement ou du droit à la vie privée. Les juges ont considéré que l'obligation

[863] S.1586 - App Store Accountability Act, 119th Congress (2025-2026).
[864] S.1586 - App Store Accountability Act, 119th Congress (2025-2026), SECTION 2.
[865] S.1586 - App Store Accountability Act, 119th Congress (2025-2026), SECTION 3.
[866] Ibid.
[867] S.1586 - App Store Accountability Act, 119th Congress (2025-2026), SECTION 5-6-7.
[868] S.1586 - App Store Accountability Act, 119th Congress (2025-2026), SECTION 8.
[869] FTC, FTC Denies Application for New Parental Consent Mechanism Under COPPA, mars 2024.
[870] Louisiana, ACT No. 440 ou Louisiana – HB 142 Passed 06/15/2022 and Effective 01/01/2023.
[871] Par exemple : Oregon HB 2032 ; Minnesota HF 1875, Pennsylvania SB 603 ; Mississippi – SB 2346 Passed and Effective 07/01/2023 ; Montana – SB 544 Passed 05/19/2023 and Effective ; Texas – HB 1181 Passed 06/12/2023 and Effective 09/01/2023.01/01/2024 ; Utah – SB 287 Passed 03/14/2023 and Effective 05/03/2023.
[872] Par exemple, la Floride a adopté une loi qui interdit aux mineurs de moins de 16 ans d'accéder aux réseaux sociaux. Cette mesure devrait conduire les réseaux sociaux à supprimer les comptes existants des utilisateurs moins de 17 ans, et à mettre en place un système de vérification d'âge par une société tierce (v. Le Monde avec AFP, La Floride adopte une loi limitant l'accès des mineurs aux réseaux sociaux, 25 mars 2024).
[873] Arkansas SB 66 ou NetChoice, LLC v. Griffin, No. 5:2023cv05105 - Document 44 (W.D. Ark. 2023).

de fournir une pièce d'identité pour accéder à certains contenus pouvait avoir un effet dissuasif inconstitutionnel. Au Texas, le juge fédéral avait initialement bloqué la loi, la jugeant inconstitutionnelle. La Cour d'appel du 5e circuit a néanmoins annulé cette décision, autorisant l'application de la loi, à l'exception des avertissements sanitaires, jugés contraire à la liberté d'expression[874].

12.2.3. Angleterre et Pays de Galles

Approche réglementaire. Le Royaume-Uni a adopté une approche réglementaire pour renforcer la protection des mineurs en ligne, notamment avec l'Online Safety Act de 2023[875]. Cette loi impose aux fournisseurs de services en ligne des obligations visant à protéger les enfants contre les contenus préjudiciables. L'OSA exige qu'un fournisseur utilise la vérification de l'âge ou l'estimation de l'âge (ou les deux) pour empêcher les enfants de tout âge de rencontrer un contenu préjudiciable. Il oblige également les plateformes à rendre une évaluation, avant le 16 avril 2025, de l'accès potentiel des enfants à leurs services, afin de déterminer si ceux-ci sont susceptibles d'être utilisés par des mineurs. Dans de tels cas. Dans ce cadre, l'Ofcom a publié un guide "*Children's access assessments*"[876] afin d'aider les fournisseurs de services en ligne soumis à l'OSA à se conformer à leur obligation légale de réaliser une évaluation de l'accès des enfants dont l'échéance était le 16 avril 2025. Le guide précise ce que doit contenir une évaluation de l'accès des enfants, c'est-à-dire déterminer si un service est susceptible d'être consulté par des personnes de moins de 18 ans, fournit une méthodologie pratique et accessible pour effectuer cette évaluation, notamment pour les services de type user-to-user et les moteurs de recherche relevant de la partie 3 de la loi, clarifie les obligations ultérieures si un service est accessible aux enfants, il devra ensuite procéder à une évaluation des risques spécifiques pour les enfants et mettre en place des mesures de protection appropriées et prévient la confusion avec d'autres cadres juridiques, notamment le Children's Code de l'ICO, en soulignant que cette évaluation est distincte mais complémentaire à celle requise en matière de protection des données.

Code de conduite. En complément, le Children's Code[877], entré en vigueur en 2021, impose aux services numériques d'adapter leurs paramétrages et le traitement des données aux besoins des mineurs, ce qui implique également de pouvoir estimer l'âge des utilisateurs avec un niveau de confiance "*raisonnable*". Il contient à ce titre 15 normes que les services en ligne doivent respecter afin de se conformer à leurs obligations en vertu de la loi sur la protection des données pour protéger les données des enfants en ligne. Si la loi ne prescrit pas une méthode unique de vérification de l'âge, elle impose un résultat qui est celui de garantir que les mineurs ne soient pas exposés à des contenus qui leur sont inappropriés. En cas de violation grave des principes de protection des données, nous avons le pouvoir d'infliger des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

---

[874] United States Court of Appeals for the Fifth Circuit, Appeal from the United States District Court for the Western District of Texas USDC No. 1:23-CV-917, March 7, 2024.

[875] Online Safety Act 2023.

[876] OFCOM, Statement: Age Assurance and Children's Access, janvier 2025.

[877] ICO, Age appropriate design: a code of practice for online services, 2021.

Entrée en vigueur. Depuis le 25 juillet 2025, tous les sites et applications contenant des contenus à caractère pornographique doivent mettre en place des contrôles d'âge rigoureux pour garantir que les enfants ne puissent pas accéder à ce type de contenu ni à d'autres contenus préjudiciables (suicide, automutilation, troubles alimentaires)[878]. Cette mesure vise à protéger les enfants tout en permettant aux adultes d'accéder légalement à la pornographie et peut être mise en œuvre à travers plusieurs méthodes de vérification qui peuvent inclure : l'estimation de l'âge par reconnaissance faciale, la vérification via services bancaires ou cartes de crédit, les identités numériques sécurisées, la vérification par opérateur mobile, la comparaison avec pièce d'identité, ou une estimation par adresse e-mail. L'Ofcom souligne que ces contrôles doivent être techniquement précis, robustes, fiables et équitables, tout en respectant la vie privée des utilisateurs[879].

Plusieurs plateformes ont déjà commencé à se conformer à cette obligation, telles que Pornhub, Bluesky, Discord, Grindr, Reddit et X et l'Ofcom a précisé qu'elle procédera à des contrôles et prendra des mesures coercitives, pouvant aller jusqu'à 18 millions de livres sterling ou 10 % du chiffre d'affaires mondial à l'encontre de toute entreprise qui autorise les contenus pornographiques et ne se conforme pas aux exigences en matière de contrôle de l'âge avant la date limite[880]. Dans les cas les plus graves, l'Ofcom aura la possibilité de demander à un tribunal d'imposer des sanctions à des tiers, tels que les fournisseurs d'accès à Internet, ce qui pourrait entraîner le blocage ou la restriction du site au Royaume-Uni[881].

12.2.4. Australie

En Australie, le Online Safety Amendment, adopté en décembre 2024[882], a modifié le Online Safety Act 2021 afin de soumettre des réseaux sociaux à une restriction d'âge fixée à 16 ans minimum et exiger des réseaux sociaux qu'ils prennent des mesures raisonnables pour empêcher les australiens de moins de 16 ans de créer des comptes[883]. Il vise également à introduire une nouvelle définition[884] de "*plateforme de médias sociaux soumise à une limite d'âge*" à laquelle s'applique l'obligation d'âge minimum pour y accéder, ainsi que des pouvoirs réglementaires permettant au ministre des Communications de restreindre ou de cibler davantage cette définition et à préciser qu'aucun Australien ne sera contraint d'utiliser une pièce d'identité officielle (y compris une carte d'identité numérique) à des fins de vérification de l'âge, et que les plateformes devront proposer des alternatives raisonnables aux utilisateurs[885].

Le Online Safety Amendment, met également en place des mesures de protection pour la vie privée, en limitant l'utilisation des informations collectées par les plateformes pour satisfaire à

---

878 Ofcom, Online age checks now in force, 24 July 2025.
879 Ofcom, Age checks for online safety – what you need to know as a user, 26 June 2025.
880 Ofcom, Age checks for online safety – what you need to know as a user, 26 June 2025.
881 Ibid.
882 Online Safety Amendment (Social Media Minimum Age) Bill 2024.
883 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Part 1 - 2.Section 5.
884 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Part 1 - 3.Section 5.
885 Online Safety Amendment (Social Media Minimum Age) Bill 2024, 63C Age-restricted social media platform.

l'obligation d'âge minimum et en exigeant la destruction des informations après leur utilisation[886]. Il donne en outre à l'eSafety Commissioner le pouvoir de rechercher des informations pertinentes pour le contrôle de la conformité, et de les publier[887].

Enfin, il impose des sanctions maximales pouvant aller jusqu'à 30 000 unités de pénalité en cas de non-respect de l'obligation relative à l'âge minimum par les plateformes[888].

Avant que les exigences n'entrent en vigueur en décembre 2025, l'eSafety Commissioner formulera des directives concernant les mesures raisonnables à prendre pour empêcher les utilisateurs soumis à des restrictions d'âge d'avoir des comptes. Cela comprendra une consultation approfondie. Une fois les exigences entrées en vigueur, l'eSafety Commissioner pourra obtenir des informations auprès des fournisseurs de services concernant la conformité et pourra faire appliquer la conformité[889].

La consultation du eSafety Commissioner concernant la vérification de l'âge[890] contient également une analyse plus approfondie des opportunités et des risques associés aux diverses méthodes d'évaluation de l'âge[891]. En outre, l'eSafety Commissioner tiendra compte des résultats de l'essai externe du gouvernement australien sur les technologies d'assurance de l'âge, qui examine les technologies de vérification, d'estimation et d'inférence de l'âge[892]. Ces technologies seront envisagées comme options pour empêcher l'accès à la pornographie en ligne par les enfants et les jeunes de moins de 18 ans, et pour limiter l'accès aux plateformes de médias sociaux aux personnes de moins de 16 ans. Les premiers résultats publiés en juin 2025[893] ont donné lieu à la publication d'un guide réglementaire par l'eSafety Commissioner[894] expliquant les principes directeurs avant de présenter les lignes directrices à l'intention du secteur concernant les mesures raisonnables à prendre pour se conformer à l'obligation relative à l'âge minimum pour les réseaux sociaux.

12.2.5. Au niveau international

De meilleures méthodes de vérification de l'âge pour protéger les mineurs font partie de de la Déclaration de l'OCDE pour un avenir numérique fiable, durable et inclusif[895]. Un groupe de

[886] Online Safety Amendment (Social Media Minimum Age) Bill 2024, 63DA Information that must not be collected.
[887] Ibid.
[888] Online Safety Amendment (Social Media Minimum Age) Bill 2024, 63D Civil penalty for failing to take reasonable steps to prevent age-restricted users having accounts.
[889] ESafety, Social medial age restriction.
[890] eSafety Commissioner, Age verification consultation.
[891] eSafety Commissioner, Age assurance trends and challenges, issues paper, consultation.
[892] Gouvernement australien, Evaluating the effectiveness, maturity and readiness of age assurance for Australia, trial.
[893] eSafety Commissioner, Social medial age restriction.
[894] eSafety Commissioner, Social Media Minimum Age Regulatory Guidance, September 2025.
[895] OCDE, Declaration on a Trusted, Sustainable and Inclusive Digital Future, OECD/LEGAL/0488.

travail international informel réunit notamment plusieurs régulateurs européens, dont l'Arcom et le régulateur britannique (Ofcom), pour échanger des informations et retours d'expérience sur les problématiques de protection des mineurs en ligne et de vérification de l'âge, ainsi que sur l'état des dossiers en cours. L'Initiative Child Online Protection est un réseau multipartite lancé par l'Union internationale des télécommunications (UIT) pour promouvoir la sensibilisation de la sécurité des enfants dans le monde en ligne et pour développer des outils pratiques pour aider les gouvernements, les entreprises et les éducateurs. Les Lignes directrices de l'UIT pour la protection des enfants en ligne[896] sont un ensemble de recommandations à l'attention de tous les partenaires pertinents sur la façon de contribuer au développement d'un environnement en ligne sain et sûr pour les enfants et les jeunes et contiennent notamment des recommandations générales sur les techniques de vérification de l'âge.

Par ailleurs, l'Organisation internationale de normalisation (ISO) développe la norme ISO/CEI 27566 relative aux systèmes de garantie de l'âge. Cette norme technique et internationale concerne le processus de vérification de l'âge d'une personne (généralement afin d'empêcher les enfants d'accéder à des contenus, services et biens réservés aux adultes en ligne) sans compromettre leur vie privée[897].

[896] IUT, Guidelines on Child Online Protection, 2020.

[897] ISO, ISO/IEC 27566 — Information security, cybersecurity and privacy protection — Age assurance systems *[three parts, all DRAFT]*.

CHAPITRE 13 : CONTRÔLE PARENTAL

13.1. PRATIQUES ET FONCTIONNALITÉS DE CONTRÔLE PARENTAL

Définition et statistiques. D'après la Commission nationale informatique et libertés (CNIL), "*le contrôle parental est une fonctionnalité ou un logiciel qui permet notamment de restreindre l'accès à certains contenus en ligne. L'activation du contrôle parental doit permettre de protéger l'enfant d'une exposition à des contenus choquants, violents ou pornographiques*"[898].

Si 78% des 11-17 ans sont présents sur les réseaux sociaux, 71% d'entre eux déclarent utiliser au moins un compte ado ou supervisé par un parent[899]. Toutefois, 33% des parents n'ont installé aucun outil de contrôle parental et 73% des 11-17 ans déclarent avoir des discussions régulières avec leurs parents sur les risques en ligne[900]. La majorité des mineurs interrogés dans le cadre d'une étude de l'Arcom[901], affirme en outre qu'en cas d'exposition à un risque qu'ils ne maîtrisent pas, les parents sont un soutien pour résoudre le problème. À ce titre, cette même étude de l'Arcom[902] relève une mise en place d'outils de contrôle parental pour les plus jeunes 12 / 13 ans que les parents consentent à assouplir voire à lever totalement vers 15/16 ans.

Fonctionnalités et diversités des contrôles parentaux. La majorité des logiciels de contrôle parental offrent une diversité de fonctionnalités essentielles pour encadrer les usages numériques des mineurs[903]. Ils permettent la création de profils personnalisés afin d'adapter les restrictions en fonction de l'âge de l'enfant. À titre d'exemple, les jeunes enfants ont accès uniquement à une sélection restreinte de sites, tandis que les adolescents bénéficient d'un filtrage plus large des contenus inappropriés[904]. Ils permettent également de limiter le temps d'écran en définissant des horaires précis ou des quotas de connexion[905]. Certaines solutions offrent la possibilité de restreindre l'accès à des jeux, logiciels ou applications spécifiques[906]. Enfin, le contrôle parental

---

898 CNIL, La CNIL rend son avis sur les décrets relatifs au contrôle parental, 31 juillet 2023.
899 Arcom, Mineurs en ligne : Quels risques ? Quelles protections ?, Résultats du volet d'étude quantitatif, septembre 2025.
900 Ibid.
901 Arcom, Étude qualitative, Mineurs en ligne : Quels risques ? Quelle protection ?, septembre 2025, p.60.
902 Ibid.
903 CNIL, La CNIL rend son avis sur les décrets relatifs au contrôle parental, 2023.
904 e-Enfance, Contrôle parental : Un outil pour limiter les dangers qui ne saurait remplacer le dialogue et l'accompagnement des parents, 2021.
905 ANFR, Les dispositifs de contrôle parental - État des lieux au regard des dispositions réglementaires applicables en juillet 2024, 2024, p.16.
906 e-Enfance, Contrôle parental - Activer, installer et configurer un contrôle parental, 2023.

inclut un suivi des usages numériques grâce à la consultation de l'historique de navigation et des statistiques d'utilisation[907].

Certains réseaux sociaux intègrent également leur propre système de contrôle parental. À titre d'illustration, Instagram propose une supervision parentale qui permet de suivre le temps passé sur l'application, les abonnements et les signalements effectués[908]. Sur Snapchat, après acceptation d'une invitation, les parents peuvent voir la liste d'amis et les interactions de leur enfant[909]. TikTok[910] offre des fonctionnalités telles que la limitation du temps de visionnage, des restrictions sur les messages directs et une gestion avancée des paramètres de confidentialité. Par ailleurs, en octobre 2025, Meta a présenté[911] le nouvel encadrement choisi pour les comptes adolescents sur Instagram selon la classification PG-13 jugé utile par 90% d'adolescents[912]. Désormais, l'ensemble des comptes adolescents seront paramétrés en mode "restreint", ce qui limitera l'accès à certains contenus jugés d'inadaptés. À ce titre, les adolescents ne pourront plus suivre des comptes identifiés comme partageant régulièrement des contenus inadaptés, en plus des termes de recherche liés à certains sujets sensibles, comme le suicide, l'automutilation et les troubles alimentaires déjà bloqués, ce blocage sera étendu à d'autres résultats de recherche destinés à un public mature, comme "*alcool*" ou "*gore*" et ces termes resteront bloqués même en cas de faute de frappe. Les adolescents ne seront pas confrontés à des contenus contraires aux CGU dans les recommandations de contenus (Explore, Reels et fil d'actualité), le fil principal et les Stories, même lorsqu'il est partagé par quelqu'un qu'ils suivent, ni dans les commentaires. Enfin, Meta dit avoir mis à jour leurs expériences basées sur l'IA pour les adolescents afin qu'elles soient guidées par la classification « déconseillé aux moins de 13 ans » par défaut.

Les consoles de jeux et appareils mobiles intègrent également des dispositifs de contrôle parental. Ces outils permettent de restreindre l'accès à certains contenus, de bloquer les achats et téléchargements non autorisés et de limiter le temps d'écran, assurant ainsi un encadrement renforcé de l'usage numérique des jeunes utilisateurs[913].

Enfin, la majorité des fournisseurs d'accès à internet (FAI) mettent à disposition de leurs clients des moyens de contrôle parental. Il est possible de citer les dispositifs proposés par Orange, SFR Family Coach ou encore Free Angel. C'est d'ailleurs sur ces acteurs que pèsent les obligations légales depuis le 13 juillet 2024 puisque les outils de contrôle parental proposés au niveau des FAI permettent d'agir au niveau du réseau et protègent ainsi tous les appareils reliés à la box.

---

907 Ibid.

908 Instagram, Présentation des paramètres de messagerie plus stricts pour les ados sur Instagram et Facebook, janvier 2024.

909 Snapchat, Outils et ressources pour les parents.

910 TikTok, Guide à l'usage des parents, mars 2025.

911 Meta, Les Comptes Ado sur Instagram seront désormais encadrés selon la classification PG-13, 14 octobre 2025.

912 Étude Ipsos pour Meta, 2025.

913 Internet sans crainte, Contrôle parental : comment paramétrer les consoles de vos enfants ? 2022.

Limites des contrôles parentaux. Les contrôles parentaux sont confrontés à différentes problématiques tenant à des enjeux techniques, de protection des données ou encore de relations entre les mineurs et leurs parents ou représentants légaux. Concernant la confidentialité des données, certains outils de contrôle parental collectent des données sur l'utilisation d'Internet par les enfants, ce qui peut soulever des préoccupations en matière de vie privée (notamment sur la localisation, les recommandations…). Il existe également un risque de perte d'attention des parents et des contournements possibles par les enfants. En effet, avec un contrôle parental, certains parents pensent avoir le contrôle total sur l'usage numérique de leurs enfants. Or ces derniers peuvent et savent contourner les restrictions en ligne, que ce soit par inadvertance ou délibérément. Par exemple, ils peuvent utiliser des proxys, des VPN ou trouver d'autres moyens pour accéder à du contenu non autorisé, dépasser le temps d'écran, ou créer d'autres comptes sans contrôle parental.

À cela s'ajoutent des risques d'obsolescence des contrôles parentaux : sans mise à jour régulière, certains contrôles parentaux ne sont pas adaptés à l'évolution des pratiques en ligne (par exemple des tendances sur TikTok, le développement de deepfakes, des groupes de discussion sur Telegram, l'émergence de nouveaux réseaux qui pourraient échapper aux contrôles parentaux).

Les contrôles parentaux peuvent également aboutir à un filtrage insatisfaisant des contenus dans la mesure où certains contenus inappropriés peuvent échapper aux filtres de contrôle parental. Certains filtres peuvent être trop restrictifs, bloquant même des contenus éducatifs. D'autres ne sont au contraire pas assez stricts, laissant passer des contenus potentiellement dangereux et choquants.

Enfin, les contrôles parentaux ont des conséquences sur les rapports entre les mineurs et leurs parents ou responsable légal. D'une part, une dépendance excessive aux outils de contrôle parental peut entraver le développement de compétences d'autorégulation chez les enfants et porter atteinte à leur vie privée. D'autre part, les outils de contrôle parental permettent un blocage automatique des contenus, sans possibilité ou incitation au paramétrage, ce qui ne favorise pas le dialogue entre parents et enfants s'agissant des usages numériques et des risques subséquents. C'est la raison pour laquelle il est important que les parents éduquent également leurs enfants sur les risques en ligne en les responsabilisant et leur expliquant pourquoi ils utilisent cet outil. Cela étant, les obligations légales visent à mieux informer les parents des outils existants.

13.2. CADRE JURIDIQUE

Obligations des équipements selon la loi n°2022-300 dite Studer. Les fournisseurs d'accès à Internet sont tenus de proposer un dispositif de contrôle parental gratuit[914]. La Loi n°2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet oblige les fabricants d'appareils connectés à intégrer un contrôle parental préinstallé[915]. L'obligation porte

[914] Article 6 III A) de la Loi pour la confiance dans l'économie numérique.
[915] Article L34-9-3 du Code des postes et des télécommunications électroniques.

sur « *les équipements terminaux destinés à l'utilisation de services de communication au public en ligne donnant accès à des services et des contenus susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs* ». Cette disposition est relativement large afin de couvrir les équipements qui permettent de naviguer sur internet et qui disposent d'un magasin d'applications. Sont ainsi notamment concernés les ordinateurs, les smartphones, les tablettes, les télévisions et montres connectées, les systèmes de navigation embarqués, les consoles de jeux ou encore les liseuses.

La loi impose plusieurs exigences à l'égard des dispositifs de contrôle parental afin de garantir une protection efficace des mineurs lorsqu'ils utilisent des appareils connectés. Tout d'abord, ces outils doivent être facilement accessibles et compréhensibles pour les utilisateurs[916]. Leur activation doit être simplifiée et possible dès la première mise en service de l'appareil[917]. Ensuite, le contrôle parental doit permettre un blocage efficace des contenus illégaux ou inappropriés. Cela implique notamment qu'il doit permettre d'interdire le téléchargement ou l'accès à des contenus dangereux et susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs[918]. Enfin, il est précisé que le dispositif sera proposé à l'utilisateur lors de la première mise en service de l'équipement et que les données personnelles des mineurs collectées ou générées lors de l'activation de ce dispositif ne doivent pas être utilisées à des fins commerciales, notamment à des fins de marketing direct, profilage et publicité ciblée sur le comportement.

Précision d'application de la loi Studer selon le décret d'application. Le décret n°2023-588 du 11 juillet 2023 précise l'application de l'article 1er de la loi du 2 mars 2022. Il détermine les obligations des fabricants en matière de mise à disposition d'équipements terminaux intégrant des dispositifs de contrôle parental conformes, les obligations des importateurs, distributeurs et prestataires de services d'exécution des commandes au titre du contrôle de la conformité des équipements terminaux mis à disposition et précise le pouvoir de contrôle dont dispose l'Agence nationale des fréquences (ANFR).

En mars 2024, l'ANFR avait d'ailleurs remis un rapport afin d'éclairer les fabricants sur la mise en place de cette nouvelle législation[919]. Ce rapport établissait un état des lieux des dispositifs de contrôle parental en prévision de l'entrée en vigueur de la loi Studer, le 13 juillet 2024. Il présentait à ce titre, les équipements concernés et étudiait leur conformité aux exigences réglementaires à venir. Il analysait enfin les écarts observés entre les dispositifs actuels et les futures obligations, notamment en matière de fonctionnalités minimales et de protection des mineurs.

En parallèle, dans une délibération du 9 mars 2023, la CNIL s'est prononcée sur le projet du décret et préconisait que les dispositifs de contrôle parentaux assurent une protection renforcée des

[916] Article 1er de la loi visant à renforcer le contrôle parental sur les moyens d'accès à internet.
[917] Ibid.
[918] Service public, Contrôle parental : de nouvelles obligations pour les fabricants de matériels connectés, 11 juillet 2024.
[919] ANFR, Les dispositifs de contrôle parental - Etat des lieux au regard des dispositions réglementaires applicables en juillet 2024, 2024.

données personnelles des mineurs[920]. À ce titre, il était recommandé que le traitement de ces données soit effectué uniquement en local, sur l'appareil utilisé, sans possibilité de collecte à distance. Cette interdiction est désormais explicitement prévue à l'article 5 du décret n°2023-588[921], garantissant ainsi que les informations des mineurs ne puissent être exploitées ou stockées par des tiers. Cette exigence est essentielle dans la mesure où certains outils de contrôle parental collectent des données sur l'utilisation d'Internet par les enfants, ce qui peut soulever d'importantes préoccupations en matière de vie privée (notamment sur la localisation, les recommandations…). C'est en ce sens que le stockage en local des dispositifs de contrôle parentaux est à préférer, conformément aux nouvelles dispositions du Code des procédures civiles d'exécution (CPCE).

En outre, le décret prévoit un régime de sanctions graduées. Lorsque l'ANFR constate un manquement aux obligations prévues, elle peut d'abord adresser une mise en demeure au fabricant ou à l'opérateur économique concerné, l'enjoignant de prendre, dans un délai qu'elle fixe, toutes les mesures correctrices nécessaires afin de mettre les appareils en conformité ou de les retirer du marché. A l'issue de ce délai, si aucune mise en conformité n'a été réalisée, l'ANFR est habilitée à ordonner le retrait temporaire des produits concernés, voire leur rappel du marché national.

En cas de non-respect de cette mise en demeure dans le délai imparti, l'ANFR peut également infliger à l'opérateur une amende administrative, conformément aux dispositions du II bis de l'article L. 43 du code des postes et des communications électroniques. Cet article prévoit que le montant de l'amende peut atteindre jusqu'à 1 500 € pour une personne physique et 7 500 euros pour une personne morale. Par ailleurs, lorsque plusieurs sanctions administratives sont prononcées à l'encontre d'un même auteur dans le cadre d'une même procédure ou de procédures distinctes, pour des manquements concomitants passibles de sanctions dont les montants cumulés excèdent 3 000 euros pour une personne physique ou 15 000 euros pour une personne morale, celles-ci s'exécutent de manière cumulative, dans la limite du plafond légal le plus élevé.

Il convient de préciser que le recours formé par le Syndicat des éditeurs de logiciels de loisirs (SELL) pour contester certaines dispositions du décret n°2023-588 a été rejeté par le Conseil d'Etat, ce dernier ayant considéré que les dispositions visées étaient conformes à la loi et aux principes juridiques en vigueur[922]. Ainsi, les obligations imposées aux fournisseurs d'accès à Internet en matière de contrôle parental, telles que définies par le décret du 11 juillet 2023, ont été maintenues.

Désormais, depuis le 13 juillet 2024, tous les appareils connectés à internet commercialisés en France doivent pouvoir proposer une fonctionnalité de contrôle parental. Il importe de préciser que les équipements terminaux d'occasion mis sur le marché avant le 13 juillet 2024 ne sont pas soumis

---

[920] CNIL,Délibération n° 2023-023 du 9 mars 2023 portant avis sur un projet de décret portant application de la loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet (demande d'avis n° 22017855).

[921] Décret n° 2023-588 du 11 juillet 2023 pris pour l'application de l'article 1er de la loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet.

[922] Conseil d'État, 10ème - 9ème chambres réunies, 26/07/2024, 488159.

aux exigences légales. Toutefois, les opérateurs les commercialisant sont tenus d'une obligation d'information concernant l'existence de dispositifs de contrôle parental pouvant être installés.

13.3. PRÉCONISATIONS

Préconisation 51 - Évaluer l'effectivité des solutions disponibles :

a. imposer la publication de leur taux d'usage ;

b. réaliser des enquêtes périodiques sur les freins à l'usage ;

c. mener des travaux de collecte des données nécessaires à l'évaluation des moyens engagés par les plateformes ;

d. mener des travaux afin d'évaluer l'ergonomie des outils mis en place par les opérateurs ;

b. plus généralement, déployer des outils d'identification de l'évolution des usages et des risques subséquents et assurer l'envoi d'informations ou d'alertes diffusées par les autorités publiques et les associations spécialisées dans la protection des mineurs en ligne, notamment pour diffuser toute information utile sur les pratiques émergentes préjudiciables aux mineurs.

Préconisation 52 - Assurer la diversité des solutions disponibles :

a. informer les utilisateurs de l'existence de dispositifs indépendants de celui pré-installé sur l'appareil connecté,

b. centraliser le téléchargement de ces différentes applications ;

c. garantir leur interopérabilité dans le prolongement des dispositions du DSA.

Préconisation 53 - Afin de préserver la vie privée, la protection des données à caractère personnel et l'autonomie des enfants, privilégier les solutions : (1) respectueuses du privacy by design ; (2) reposant sur le stockage des données en local, sans remontée de données personnelles sur le serveur ; (3) qui ne permettent pas de géolocaliser l'enfant par défaut.

Préconisation 54 - Organiser l'accompagnement des parents en les informant et en les formant quant à l'utilisation de ces solutions et promouvoir un dialogue parents-enfants concernant les usages numériques :

a. afin de promouvoir le dialogue parents-enfants, renommer les outils de contrôle parental pour préférer une terminologie évoquant la parentalité numérique ;

b. diffuser des campagnes d'information adaptées aux besoins des utilisateurs donnant notamment accès aux informations relatives aux associations de défense des victimes ; s'assurer de l'adéquation des ressources proposées en les évaluant périodiquement au moyen d'enquêtes utilisateurs.

c. Lors de ces campagnes et dans le cadre de ces ressources disponibles, mettre l'accent sur l'importance d'une communication ouverte entre parents et enfants pour favoriser les échanges sur leurs expériences en ligne :

    - inciter les parents à expliquer les raisons de l'installation et le réglage des paramètres de solution de parentalité numérique ;

    - préconiser que le paramétrage soit réalisé à l'issue d'un dialogue parents-enfants afin que ces derniers soient plus susceptibles de respecter les limites établies et, plus généralement, pour faire de ces solutions de parentalité numérique un instrument d'éducation aux usages numériques (cf. les recommandations Internet sans crainte, je protège mon enfant des écrans).

    - à cette fin, promouvoir by design l'organisation de ce dialogue : le design des solutions de parentalité numérique devrait être conçu afin de favoriser un tel dialogue y compris après l'activation du contrôle parental ;

    - informer les parents de la nécessité de faire des mises à jour régulières (sur les pratiques en ligne et les applications) afin de garantir une protection optimale ;

    - informer les parents de la nécessité de prendre connaissance régulièrement des comptes rendus du contrôle parental, éventuellement en proposant des notifications à cet effet.

V. PRÉCONISATIONS GÉNÉRALES

14.1. ÉVALUER ET FAIRE ÉVOLUER L'ARSENAL JURIDIQUE

14.1.1. Modifications à apporter

Préconisation 55 - Renforcer les moyens de la justice, de la police, des autorités publiques compétentes (dont l'Arcom et la CNIL) et des associations désignées comme signaleurs de confiance pour veiller à l'effectivité de l'arsenal juridique visant à protéger les mineurs en ligne. Porter une attention particulière à l'information et à la formation de l'ensemble de la chaîne des acteurs notamment en réalisant des guides sur le contexte juridique applicable à l'utilisation des réseaux sociaux par les mineurs et de bonnes pratiques à destination des magistrats ou de la police (ex. guide OFCOM, formation des magistrats).

Préconisation 56 - Mener une étude d'impact exhaustive du cadre juridique existant et de sa mise en œuvre afin de définir précisément ses éventuelles lacunes (celles du cadre légal et réglementaire, et celles tenant à leur mise en œuvre). Seules ces lacunes devraient justifier l'adoption de nouvelles mesures pour éviter un phénomène d'inflation normative préjudiciable à l'effectivité des actions normatives conduites tout en s'assurant que les éventuels textes présentés au niveau français n'enfreignent pas l'applicabilité directe de textes du droit de l'Union européenne dont le règlement sur les services numériques. Pour ce faire, s'appuyer notamment sur la plateforme https://www.betterinternetforkids.eu/practice/research.

(1) afin d'élaborer un état des lieux le plus exhaustif possible des propositions et une cartographie des controverses en prenant en compte les différentes études réalisées par les institutions publiques et les académiques (publiées ou en cours) sur « Enfants, réseaux sociaux et risques d'ordre sanitaire et tenant à la désinformation » et

(2) pour réaliser une veille des différentes solutions mises en œuvre par les États membres de l'UE, le Royaume-Uni, l'Australie et les Etats-Unis et identifier les avancées permises par des solutions innovantes consacrées par ces systèmes juridiques.

Préconisation 57 - Garantir que les enfants soient acteurs de la protection de leurs droits

(1) en rendant les textes juridiques accessibles aux enfants sur le modèle des dispositions du RGPD relatives au consentement ou encore du DSA s'agissant des CGU ;

(2) en les impliquant dans les consultations législatives au niveau français et européen en cas d'évolution du cadre légal en s'appuyant sur les ressources du laboratoire de la protection de l'enfance en ligne et sur les recommandations de la stratégie BIK de la Commission européenne

(3) en créant un comité des jeunes utilisateurs des réseaux sociaux pour les associer aux évolutions des services proposés (Commission d'enquête sur les effets psychologiques de TikTok, Recommandation du Président n°12).

14.1.2. Des évolutions à accompagner

Préconisation 58 - Instituer un dispositif de suivi transversal de la mise en œuvre du DSA impliquant les représentants des différentes autorités de régulation concernées, services ministériels et experts du sujet (dont les académiques et les magistrats). Analyser en particulier :

(1) les mesures relatives l'analyse de risques imposées aux très grandes plateformes – dont, plus spécifiquement, en ce qui concerne les conséquences graves sur le bien-être et la santé des mineurs – et des mesures d'atténuations des risques mises en œuvre par ces acteurs (mesures ciblées pour la protection de l'enfance, comme la vérification de l'âge, un contrôle parental, des outils visant à aider les mineurs à signaler les abus ou obtenir de l'aide) avec une attention particulière concernant la conception des interfaces en ligne et le paramétrage de leurs services;

(2) les mesures concernant l'exploitation des données des mineurs à des fins publicitaires (publicité commerciale reposant sur le profilage est interdite dès lors que la plateforme a connaissance avec une « certitude raisonnable » que l'utilisateur est un mineur);

(3) la mise en œuvre de l'accès aux données pour les chercheurs prévue par l'article 40 du DSA afin de mieux objectiver les risques sanitaires pour les mineurs en cas d'usage des réseaux sociaux.

Préconisation 59 - Favoriser la diffusion des bonnes pratiques

(1) promouvoir l'identification et la prise en compte des modèles de bonnes pratiques identifiés par la société civile et les académiques, par exemple s'agissant de modèles d'interfaces de choix non trompeuses et manipulatrices, du paramétrage des comptes utilisateurs ou encore du fonctionnement des algorithmes de recommandation de contenus ;

(2) assurer au niveau européen un suivi des bonnes pratiques selon un format multipartite en y associant les enfants (cf. point 14 Parlement européen BIK + qui invite la Commission à veiller à ce que la stratégie BIK + soit cohérente avec d'autres priorités et propositions législatives, à ce que les informations soient présentées aux enfants dans un langage adapté, à ce que les enfants de tous âges soient associés au processus de suivi et à la mise en œuvre effective de la stratégie, et à ce qu'un suivi adéquat soit assuré pour comparer les bonnes pratiques et les résultats dans tous les États membres).

Préconisation 60 - Assurer des sanctions efficaces

(1) en engageant des poursuites plus systématiques pour faire baisser le sentiment d'impunité et mieux accompagner les victimes ;

(2) en promouvant le recours à des stages de citoyenneté conformément au dispositif prévu par l'article 5 ter A de la loi SREN qui modifie le Code pénal en prévoyant un stage de sensibilisation au respect dans l'environnement numérique.

14.2. S'ASSURER DE LA PRISE EN COMPTE DES PRATIQUES ÉMERGENTES

Préconisation 61 - Mettre en place un dispositif de veille agile pour identifier et répondre au plus vite aux risques résultant des pratiques émergentes sur les réseaux sociaux telles que, en ce moment, la sextorsion ou chantage sexuel (par le biais de nude ou de deepfake à caractère sexuel), la diffusion non consentie d'image intime et les challenges, en organisant un canal d'écoute efficace de la société civile qui s'appuie notamment sur l'expertise des signaleurs de confiance.

Préconisation 62 - S'assurer de l'existence ou construire un réseau au niveau de l'Union européenne pour déterminer et faire évoluer de façon réactive les priorités de la Commission européenne pour la mise en œuvre du DSA afin d'appréhender au plus vite ces pratiques émergentes en s'appuyant sur les Safer Internet Center in Europe.

Préconisation 63 - Conduire des études prospectives afin d'anticiper au mieux ces évolutions en y associant les enfants pour une meilleure gouvernance anticipative (cf. recommandation de l'UNICEF, 2023).

Préconisation 64 - Assurer plus généralement un suivi de l'incidence de la transformation numérique sur le bien-être des enfants conformément aux recommandations de la Commission européenne par l'intermédiaire du portail Betterinternetforkids.eu (partage d'études scientiques sur la plateforme) à mettre en lien en France avec les travaux du laboratoire de protection des enfants en ligne au niveau gouvernemental ou le programme Tralalere (Internet sans crainte).

14.3. RENFORCER L'INFORMATION, LA FORMATION ET L'ACCOMPAGNEMENT DES VICTIMES

Préconisation 65 - Renforcer sur les réseaux sociaux des redirections lors d'un signalement et lorsqu'une requête utilisateur est relative à une pratique dangereuse (v. sur Instagram avec "suicide" ou "anorexie"), vers : (1) des ressources d'information notamment sur les démarches à suivre (signalement, plaintes…) et, (2) une ligne d'écoute.

Préconisation 66 - Réaliser des campagnes de sensibilisation dans et hors le milieu scolaire pensées de façon adaptée tant à l'égard des adultes référents (enseignants, éducateurs, responsables de l'autorité parentale) que des jeunes publics en adoptant pour ces derniers une approche distincte selon les catégories de jeune public et en les impliquant dans l'élaboration de ces campagnes afin d'atteindre la cible en ce qui concerne le medium, le format et le contenu de l'information. En cas d'identification de pratiques émergentes (cf. proposition 7), conduire des campagnes de sensibilisation à brefs délais pour prévenir les risques encourus par les mineurs.

En ce qui concerne plus particulièrement l'information et la formation en milieu scolaire,

(1) sensibiliser et réviser la certification PIX ;

(2) mener une étude portant sur la mise en œuvre des diverses mesures d'éducation et de sensibilisation prévues par le Code de l'éducation, que celles-ci soient relatives directement aux usages numériques, à la sexualité, aux addictions et à l'alimentation ;

(3) recenser les difficultés rencontrées par le personnel enseignant, le temps consacré à ces séances ainsi que leur effectivité perçue ;

(4) envisager de confier ces séances de sensibilisation à des tiers, notamment des associations spécialisées ;

(5) assurer une plus grande sensibilisation à la santé mentale, à tous les niveaux de la société, afin notamment de détecter les cas de harcèlement, dépression, pensées suicidaires, troubles du comportement alimentaire et de prévenir leur survenance.

Préconisation 68 - Prévoir dans chaque établissement scolaire la désignation d'une personne ayant la qualité d'écoutant qui pourrait jouer le rôle de médiateur et de personne extérieure à même de recueillir les récits des mineurs et d'être attentif à leur santé mentale

14.4. RENFORCER LES ACTIONS AU NIVEAU COLLECTIF

Préconisation 69 - Penser des moyens d'action au niveau collectif en soutenant les actions menées par la société civile pour ne pas mettre à la charge des seules victimes la défense de leurs droits.

Préconisation 70 - Renforcer les moyens alloués aux associations reconnues comme bénéficiant d'une expertise forte dans la lutte contre les violences sur mineurs en ligne, dont le harcèlement en ligne et la lutte contre la désinformation, avec une attention particulière pour les enfants de milieu défavorisé. À cet égard, plusieurs axes de financement pourraient être envisagés (cf. Rapport Mission Enfants et Ecrans, proposition 27 et Commission d'enquête TikTok recommandation du Président n°11):

(1) envisager le partage des gains attendus des frais de supervision dont les grandes plateformes sont redevables au titre du DSA, ainsi que des amendes imposées par le juge et le régulateur tant à l'échelle européenne qu'à l'échelle des États membres qui hébergent les sièges des entreprises visées ;

(2) consacrer la reconnaissance générale en droit d'un principe de pollueur / payeur, sur le modèle du droit environnemental.

Il pourrait également être envisagé la création d'un fonds de financement dédié à la sécurité numérique et l'émancipation des enfants.

Préconisation 71 - Garantir le soutien clair et ferme de l'État, en particulier au regard des enjeux du DSA, concernant les actions de signalement des associations notamment en inscrivant dans un plan national que les ministères aient dans leurs prérogatives de les accompagner dans leurs actions en termes de signalement sur le modèle des actions menées par la DILCRAH.

Préconisation 72 - Soutenir la constitution d'un espace de mutualisation des moyens et des actions conduites par la société civile dans une perspective de renforcer l'action collective afin :

(1) d'assurer une meilleure protection des jeunes utilisateurs,

(2) de renforcer l'information des pouvoirs publics au niveau national et européen et

(3) de mettre en place une stratégie de « contrepouvoir » à l'égard des grands services numériques.

Préconisation 73 - Plus généralement, mettre en place une réserve citoyenne sur le modèle proposé dans le cadre du Conseil de la refondation numérique dans sa feuille de route "apaiser l'espace public" et reprise par la loi SREN (mais a minima) ; ces actions de la société civile, auxquelles les jeunes utilisateurs devraient être associés, devrait être soutenues, organisées et rendues visibles par les services de l'État afin de leur assurer une réelle effectivité (cf. Rapport Mission Enfants et Ecrans, proposition 5).

Préconisation 74 - Créer une Délégation Interministérielle pour la Protection des Mineurs en Lignes placée sous la tutelle du Premier Ministre (sur le modèle de la DILCRAH) afin de :

(1) soutenir les actions de la société civile ;

(2) accompagner, sous la forme d'un incubateur, l'émergence de projets innovants ;

(3) assurer le lien entre les actions des différents ministères ;

(4) suivre le sujet au niveau européen et international ;

(5) assurer l'existence d'un guichet unique pour favoriser l'accès au public à l'information nécessaire sur la sensibilisation aux pratiques à risque, l'identification des associations spécialisées ou encore le cadre réglementaire applicable ;

(6) mettre en place une plateforme de remontée d'informations relatives aux pratiques en ligne afin d'évaluer les tendances et, s'il y a lieu, d'accompagner une évolution du cadre juridique ;

(7) en s'appuyant sur un conseil scientifique pour étudier l'opportunité et la compatibilité avec le droit de l'Union de toute réforme du cadre légal sur le sujet.

14.5. ACTIONS PRIORITAIRES

Préconisation 75 - Faire de la lutte contre les comportements en lien avec les contenus d'abus et d'exploitation sexuels d'enfants une priorité nationale.

Préconisation 76 - Renforcer de toute urgence les moyens d'action concernant la lutte contre la diffusion de deepfakes à caractère sexuel de mineurs et contre la diffusion d'abus sexuels d'enfants réalisée par un tiers et commanditée par un « consommateur » (dont en live streaming).

Préconisation 77 - À des fins préventives, mener de toute urgence des actions de sensibilisation de grande envergure concernant ces pratiques à l'égard des enfants et des adultes référents.

Préconisation 78 - A des fins préventives, mener de toute urgence des actions de sensibilisation de grande envergure concernant le fonctionnement et les impacts potentiellement des interactions entre l'humain et les systèmes d'Intelligence artificielle type AI Compagnon.

ANNEXE 1 - LISTE DES ENTRETIENS RÉALISÉS

SYSTÈME FRANÇAIS - EUROPÉEN

AI FORENSICS

FADDOUL Marc

Arcom

PECAUT-RIVOLIER Laurence

BOULE Camille

BOYER César

PETIT Lucile

MILLET Manon

BODYGUARD

TOUMI Majdi

CNCDH

LAFOURCADE Magali

CHESNEL Laurène

CNIL

DELPORTE Xavier

ARFOUI Mehdi

BIERI Martin

ELBAZ Jennifer

COUTOR Olivier

CNNUM

CATTAN Jean

HURSTEL Joséphine

DILCRAH

BENOUALID Shani

E-ENFANCE
CHIBOUT Romain
COMBLEZ Samuel

Google
VERGNES Arnaud

I3S NICE
VILLATA Serena, DR CNRS

JESUISLÀ
BRANDAO Xavier

LINC
HARY Estelle

META

ATTESTI Anton

OFMIN
BÉCHU Véronique

PARQUET DES MINEURS
BROUILLET Aurélien

POINT DE CONTACT

MATEO Flora

POLYTECHNIQUE
BLAZY Olivier

RENAISSANCE NUMÉRIQUE
GALISSAIRE Jessica
Me RICHARD Annabelle

SNAPCHAT
BOUCHAHOUA Sarah
BEAUCHÈRES Jacqueline

STOPFISHA

CLEMOT MCLAREN Shanley

MUSSON Margot, Docteur en droit

SYSTÈMES COMPARÉS

CAMPAGNE #MYBODYMYCHOICE

COMPTON Sophie

CAMPAGNE #NOTYOURPORN

MICHAEL Elena

CURTIN LAW SCHOOL / DIGITAL CHILD

BUNN Anna

CORNELL INSTITUTE, WASHINGTON UNIVERSITY IN SAINT LOUIS

RICHARDS Neil

DURRIE Ryan, JD

ZEIDE Elana

ESAFETY COMMISSIONER, Australie

SERRY Ella

ONLINE RESILIANCE TOOL/UNIVERSITÉ DE KEELE

STREET Louisa

RESET
FARTHING Rys

REVENGE PORN HELPLINE / STOPNCII
MORTIMER Sophie

BOSTON UNIVERSITY
BHARTZOG Woody

UNIVERSITÉ DE KEELE
HIGSON-BLISS Laura

OFCOM
COOKE Julia

UNIVERSITÉ DE DURHAM
MCGLYNN Clare

HUMER Caroline

ANNEXE 2 : LES PRINCIPAUX ACTEURS

Au niveau international, européen et national, plusieurs acteurs étatiques et non étatiques sont chargés de veiller au respect des droits fondamentaux des mineurs et à leur sécurité sur les réseaux sociaux. On citera ci-dessous plusieurs acteurs de manière non exhaustive aux niveaux international, européen et national.

1. AU NIVEAU INTERNATIONAL ET EUROPÉEN

Au niveau international, l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), en tant qu'institution spécialisée internationale de l'Organisation des Nations unies (ONU), figure parmi l'un des premiers acteurs institutionnels au niveau mondial concernant la protection des enfants en ligne.

Au niveau de l'Union européenne, le programme **Better Internet for Kids (BIK+)** vise à créer un environnement numérique plus sûr et adapté pour les enfants. Il promeut des outils éducatifs, le développement des compétences numériques, et la sensibilisation aux risques en ligne, tout en soutenant des plateformes et contenus appropriés. La stratégie BIK+ favorise la coopération entre gouvernements, ONG et entreprises technologiques pour garantir la protection des droits des enfants dans le monde numérique. Il instaure à ce titre les réseaux INSAFE et INHOPE au sein de l'Union européenne.

Le **National Center for Missing and Exploited Children (NCMEC)**, fondé en 1984, est une organisation à but non lucratif dédiée à la localisation des enfants disparus, à la lutte contre l'exploitation sexuelle des mineurs et à la prévention des abus. En soutenant les forces de l'ordre et les familles, il offre des formations spécialisées et des outils de prévention. Sa plateforme CyberTipline permet au public et aux fournisseurs de services numériques de signaler des cas de pédocriminalité en ligne. En 2023, plus de 36,2 millions de signalements ont été analysés, permettant de mobiliser les autorités compétentes.

Le NCMEC collabore à l'international via **l'International Center for Missing and Exploited Children (ICMEC)**, créé en 1998, qui évalue et compare les lois de 196 pays concernant l'exploitation sexuelle des mineurs en ligne. Ce travail a contribué à l'amélioration ou à l'adoption de lois dans 150 pays, avec des progrès notables : 140 pays incriminent la possession de contenus illégaux, et 125 définissent juridiquement l'exploitation sexuelle. Cependant, seuls 32 exigent que les fournisseurs d'accès internet signalent les cas suspects. Ces efforts renforcent la lutte globale contre les contenus d'exploitation des mineurs.

La **Tech Coalition** regroupe plusieurs grandes entreprises technologiques, dont Google, Meta (Facebook, Instagram), Discord, Roblox, Snap, Twitch, Quora et Mega, pour lutter contre l'exploitation sexuelle des mineurs en ligne à travers le projet Lantern. Ce programme vise à établir

une base de données collaborative contenant des informations sur les contenus sensibles ou illicites, grâce à un mécanisme de partage de signalements (*signal sharing)*.

Lorsqu'une plateforme identifie un contenu illicite (image, vidéo, ou texte), elle prend des mesures immédiates pour le traiter à son niveau, comme le retrait ou le signalement. Elle transmet ensuite à la base Lantern des données clés, telles que les caractéristiques techniques du contenu (hachage cryptographique), ou dans certains cas, le contenu lui-même. Cela permet aux autres plateformes membres de détecter et supprimer automatiquement ces fichiers s'ils réapparaissent ailleurs.

En plus des hachages de fichiers, la base Lantern peut contenir des informations contextuelles liées à ces activités criminelles, comme des adresses e-mail associées à des comptes pédopornographiques, des pseudonymes utilisés par les délinquants, des mots-clés fréquemment employés pour attirer des enfants, ou encore des indications sur les pratiques de vente et d'échange de contenus illicites. Ce partage d'informations renforce l'efficacité collective des entreprises dans la prévention et l'éradication des contenus pédopornographiques en ligne, tout en aidant à identifier les auteurs et les réseaux responsables de ces abus.

Au niveau européen, **l'European Police Office (EUROPOL)** est une agence de police créée en 1998 spécialisée dans la répression de la criminalité. Elle facilite l'échange de renseignements entre polices nationales notamment en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie.

L'Internet Crime Complaint Center (IC3) est le centre du FBI chargé de centraliser l'ensemble des plaintes en ligne concernant la cybercriminalité et de lancer des enquêtes concernant ces crimes. Lesdites plaintes et signalements sont dès lors partagés *"à travers son vaste réseau de bureaux locaux du FBI et de partenaires chargés de l'application de la loi, renforçant ainsi la réponse collective*"[923].

L'UNICEF (Fonds des Nations unies pour l'enfance) est une organisation internationale dédiée à la défense des droits des enfants, à la satisfaction de leurs besoins fondamentaux et à leur épanouissement. À travers son Bureau des éclairages mondiaux et des politiques, l'UNICEF analyse des problématiques émergentes et propose des stratégies, notamment concernant l'usage de l'intelligence artificielle (IA). Elle met en lumière les risques associés à l'IA générative, notamment la création de contenus pédopornographiques réalistes (CSAM), souvent facilitée par des modèles en open source et l'exploitation de photos issues du "sharenting" sur les réseaux sociaux.

L'alliance WeProtect Global Alliance, devenue une organisation indépendante en 2020, se consacre à la protection des enfants contre les abus et l'exploitation sexuelle en ligne. Elle publie régulièrement des évaluations mondiales des menaces, identifiant les formes d'abus numériques et proposant des solutions concrètes pour y faire face. Dans le cadre de sa mission, elle organise des sommets internationaux, tels que "Turning the Tide on Child Sexual Abuse Online" en 2022, qui réunissent acteurs publics et privés pour renforcer la lutte contre ces crimes.

[923] Federal Bureau of Investigation. *Internet Crime Complaint Center (IC3).*

2. AU NIVEAU NATIONAL

La **Commission nationale de l'informatique et des libertés (CNIL)** est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Elle veille à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction. Les 8 recommandations de la CNIL énoncés en 2021 pour renforcer la protection des mineurs en ligne sont : (1) Encadrer la capacité d'agir des mineurs en ligne, (2) Encourager les mineurs à exercer leurs droits, (3) Accompagner les parents dans l'éducation au numérique, (4) Rechercher le consentement d'un parent pour les mineurs de moins de 15 ans, (5) Promouvoir des outils de contrôle parental respectueux de la vie privée et de l'intérêt de l'enfant, (6) Renforcer l'information et les droits des mineurs par le design, (7) Vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée, (8) Prévoir des garanties spécifiques pour protéger l'intérêt de l'enfant[924]. Par ailleurs, pour la période 2025-2028, la CNIL orientera son action autour de 4 principaux axes au cœur du développement de la société numérique dont la protection des mineurs. Il est notamment prévu que la CNIL renforce son dialogue avec les enfants, leur entourage constitués des parents, des enseignants et des éducateurs ainsi que l'écosystème éducatif (acteurs publics, entreprises, régulateurs et organisations internationales) "*pour créer un environnement numérique plus sûr pour les enfants et adolescents*"[925].

Le **Défenseur des droits auprès des enfants est** une organisation désignée constitutionnellement et reconnue par le Comité des droits de l'enfants des Nations Unies pour veiller au droit des enfants conformément à la loi et à la Convention internationale des Droits de l'Enfant (CIDE)[926]. Le Défenseur des Droits s'assure du respect de « *l'intérêt supérieur de l'enfant* », c'est-à-dire que l'intérêt de l'enfant soit considéré comme primordial et prioritaire sur tout autre. Il est possible de s'adresser au Défenseur des droits si les droits d'un enfant ne sont pas respectés ou si une situation met en cause son intérêt. Un enfant ou un adolescent peut contacter lui-même le Défenseur des droits. Par exemple, dans son rapport de novembre 2022 sur le respect de la vie privée des enfants, la Défenseure des droits et le Défenseur des Enfants avait appelé à mieux protéger le droit à l'image des enfants sur internet[927].

---

[924] CNIL, " La CNIL publie 8 recommandations pour renforcer la protection des mineurs en ligne", juin 2021.

[925] CNIL, "IA, mineurs, cybersécurité, quotidien numérique : la CNIL publie son plan stratégique 2025-2028", 16 janv. 2025.

[926] Convention internationale des droits de l'enfant (CIDE), ou Convention relative aux droits de l'enfant, est un traité international adopté par l'Assemblée générale des Nations Unies le 20 novembre 1989.

[927] Défenseur des droits, Rapport annuel 2022 - La vie privée : un droit pour l'enfant, novembre 2022.

L'Arcom (Autorité de régulation de la communication audiovisuelle et numérique) prête une grande attention à la protection des mineurs sur Internet. L'Arcom est ainsi chargée de faire respecter l'interdiction de l'accès des mineurs aux sites pornographiques conformément à la loi visant à protéger les victimes de violences conjugales[928]. Depuis le 11 janvier 2025, l'éditeur de site pour adultes dont le dispositif de contrôle d'âge n'est pas satisfaisant peut être mis en demeure par l'Arcom et voir son service bloqué et/ou déréférencé des moteurs de recherches, sur décision du président du tribunal judiciaire de Paris. L'Arcom a également listé des outils de contrôle parental disponibles sur l'ensemble des supports et équipements utilisé par votre enfant, de la tablette au smartphone, en passant par l'ordinateur et adaptés en fonction de son âge sur le site jeprotegemonenfant.gouv.fr[929]. L'Arcom est enfin le coordinateur pour les services numériques au titre du DSA.

L'Arcep (Autorité de régulation des communications électroniques et des Postes) propose des solutions pour renforcer le contrôle parental sur les différents équipements. Elle publie régulièrement notamment des fiches pratiques à destination des parents concernant les outils destinés à protéger les mineurs en ligne[930].

L'Arcep et l'Arcom collaborent étroitement depuis 2020 dans le cadre d'un pôle numérique notamment pour la protection des enfants par exemple en réunissant mensuellement le Comité de suivi du protocole d'engagements pour la prévention de l'exposition des mineurs aux contenus pornographiques[931].

La plateforme PHAROS (Portail national de signalement des contenus illicites de l'Internet) permet à chaque internaute de signaler les contenus ou comportements illicites auxquels il est confronté lors de sa navigation. Par ailleurs, cet outil propose une série de conseils à destination des parents afin de les aider à protéger les mineurs sur internet.

Le **pôle d'expertise de la régulation numérique** (PeREN) a rassemblé les règles relatives à la protection des mineures et de leurs données prises par les très grandes plateformes et les très grands moteurs de recherche[932].

L'Office mineurs (OFMIN), lancé en novembre 2023, est une unité centrale de la police judiciaire dédiée aux infractions commises contre des mineurs, telles que les abus sexuels, la traite ou la pédocriminalité en ligne. Le groupe central des mineurs victimes y est intégré pour assurer une expertise renforcée dans ces affaires sensibles. L'OFMIN collabore au niveau international pour développer des technologies capables d'identifier et de trier efficacement les contenus incriminés, facilitant ainsi le travail des enquêteurs. Ces outils visent à améliorer la rapidité et l'efficacité des investigations, notamment face au volume croissant de signalements d'abus en ligne. Malgré son rôle clé, l'OFMIN fait face à un déficit de ressources humaines et techniques,

---

[928] Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

[929] Plus d'information sur les outils :https://jeprotegemonenfant.gouv.fr/pornographie/vos-outils/

[930] V. not. : Arcep, Protection des mineurs : quelles solutions pour protéger votre enfant des images à caractère pornographique sur internet ?, déc. 2024.

[931] Arcom, Protection des mineurs contre la pornographie en ligne.

[932] PeREN,Protection des mineurs en ligne.

ce qui limite sa capacité à traiter l'ensemble des dossiers signalés (870 signalements reçus chaque jour).

Le **juge judiciaire** et plus particulièrement, au sein des tribunaux judiciaires, **le juge aux affaires familiales, le juge des enfants ou les magistrats du parquet** ; par ailleurs, le **pôle national de lutte contre la haine en ligne** (dit **parquet national numérique** ou **parquet numérique**) est une institution judiciaire française chargée des affaires de haine en ligne. Créé en 2021 et rattaché à la section « *Presse et protection des libertés publiques* » de la cinquième division du parquet de Paris, il a une compétence nationale.

Le Safer Internet France fournit également les services suivants :

(1) Le centre de sensibilisation aux usages d'internet Internet Sans Crainte qui s'adresse aux jeunes aux parents, éducateurs et professeurs afin d'éduquer à un meilleur usage d'internet. Le centre offre aussi des outils de sensibilisation et des services mis en place en coopération avec d'autres acteurs tels que les écoles, le secteur privé et d'autres acteurs nationaux.

(2) Le 3018, le numéro national pour lutter contre les violences numériques, qui aide les jeunes et leurs parents à faire face à des contenus dangereux, indésirables ou offensants (par exemple le harcèlement en ligne, le discours haineux, le sexting).

(3) La hotline Point de Contact, le service de signalement de contenus illicites. Ce dispositif de signalement permet à tout internaute de signaler un contenu potentiellement illicite rencontré lors de sa navigation. Point de Contact analyse et traite les signalements adressés par les internautes et traite les signalements transmis par ses homologues membres du réseau INHOPE, le réseau mondial des hotlines.