RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Conseil de l'IA et du Numérique

Note

Protection des mineurs en ligne par le contrôle de l'âge : comment aller plus loin ?

mars 2026

Synthèse

Le 26 janvier 2026, l'Assemblée nationale a adopté en première lecture la proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, dans un mouvement convergent avec le gouvernement, qui a fait de l'encadrement des usages numériques des mineurs l'une de ses priorités. La France s'inscrit ainsi dans la dynamique internationale de régulation des plateformes s'agissant des usages des mineurs et s'apprête à devenir le premier État membre de l'Union européenne (UE) à se doter d'un dispositif d'interdiction ciblant directement l'accès des mineurs aux réseaux sociaux, quelques semaines après le vote de l'*Online Safety Amendment Act* en Australie.

Ces initiatives législatives récentes interviennent après des années de relative inertie politique, marquées par les réticences à confronter le pouvoir économique des grandes plateformes et les défis juridiques autour de la régulation de leur modèle. Quinze ans après les Printemps arabes, lors desquels les réseaux sociaux s'étaient imposés comme de véritables outils pour la démocratie, le constat est désormais sans appel : **ces mêmes réseaux sociaux sont aujourd'hui des outils très ambivalents, bien loin des espaces sains et des vecteurs d'émancipation auxquels beaucoup ont aspiré et exposent les utilisateurs – en particulier les plus jeunes – à des risques majeurs bien identifiés.** Les études successives révèlent en effet une situation alarmante. Les mineurs sont quotidiennement exposés à des contenus violents, haineux ou incitant à des comportements autodestructeurs, tout en étant la cible de pratiques commerciales intrusives et de mécanismes de design conçus pour capter leur attention. En France, 77 % des 11-17 ans ont déjà été confrontés à des contenus choquants dont 48 % régulièrement et pour un quart d'entre eux avec des conséquences néfastes sur leur bien-être.

Faute d'alternative et pressés par l'urgence, les législateurs se résolvent à une mesure drastique et qui se veut symboliquement forte : l'interdiction de l'accès des mineurs aux plateformes, via l'imposition du contrôle de l'âge. À court terme, il y a lieu de prendre acte de cette décision répondant aux besoins de court terme qui sont bien réels, tout en révélant que **cette approche n'est qu'une réponse partielle aux causes structurelles** des risques que font peser ces services en ligne. Si l'éviction des mineurs des réseaux sociaux peut sembler une solution de dernier recours, elle ne doit pas devenir l'alternative à une refonte en profondeur des espaces numériques, au service de l'ensemble des utilisateurs.

Cette note dresse un panorama des **risques pluriels** rencontrés par les mineurs en ligne (I) et **des réglementations** actuelles/envisagées et de leurs limites (II). Elle se conclue par une **analyse des angles morts de ces dispositions et des pistes** pour repenser en profondeur l'encadrement de ces services numériques (III).

Il ressort que les réglementations qui visent à protéger les mineurs en ligne sont confrontées à plusieurs questions de méthodologie :

- Quel est le périmètre d'application de la loi ? L'enjeu réside dans le choix entre régulation ciblée, au risque de tendre vers une régulation au cas par cas et approche globale, qui peut se heurter à des difficultés d'application.
- Quelle méthode de contrôle de l'âge mettre en place, en prenant en compte leurs éventuels contournements ou effets délétères ? Le contrôle de l'âge des utilisateurs est communément devenu le préalable des politiques de protection des mineurs dans l'espace numérique. Pourtant, des voix s'élèvent pour dénoncer le caractère contre-productif de cette mesure qui ne ferait que repousser une immersion soudaine et non préparée dans les environnements numériques complexes. Les méthodes de vérification de l'âge sont également perméables à des contournements, à commencer par l'usage de VPN et présentent des risques pour les mineurs les plus vulnérables en termes d'inclusivité et d'accessibilité.
- Quels sont les contenus devant être assujettis à la réglementation ? Certains textes ciblent des catégories de contenus de manière précise en raison des risques qu'ils présentent pour certains publics dits *« vulnérable »*, quand d'autres ont une visée plus large, englobant différentes catégories de contenus et en privilégiant une approche par les risques.

Des méthodes alternatives pour protéger les mineurs sont également sur la table, aux quatre coins du monde – vérification de l'âge au niveau du terminal, plages horaires de déconnexion imposée, interfaces numériques sécurisées – et viennent enrichir les débats.

Pour autant, si les risques pour les mineurs sur les réseaux sociaux sont réels, le contrôle de l'âge ne suffira pas à répondre à tous les écueils, ni à garantir à une vie numérique apaisée pour l'ensemble des utilisateurs, pilier désormais essentiel pour la démocratie. En outre, il est essentiel de garder à l'esprit que **les mineurs doivent pouvoir trouver en ligne les outils et les moyens de s'émanciper, découvrir, apprendre et partager en toute sécurité**. C'est la promesse initiale du numérique et un droit fondamental pour les enfants.

Enfin, **le débat sur la protection des mineurs en ligne ne doit pas évincer les enjeux structurels que la plupart des réglementations actuelles tendent à délaisser**. Face à ces angles morts, la France et l'Europe doivent, sans plus attendre, accélérer réflexions et travaux sur cinq chantiers structurants :

1. **Créer un standard européen de protection des mineurs en ligne ;**
2. **Ouvrir les fonctionnalités des plateformes, consacrer un droit au paramétrage et renforcer la transparence des algorithmes ;**
3. **Repenser la dichotomie hébergeur/éditeur ;**
4. **Considérer les usages pluriels des services numériques, en particulier ceux qui relèvent de l'IA générative ;**
5. **Renforcer et structurer l'éducation au numérique, aux médias et à l'information.**

Table des matières

Introduction

Le 26 janvier 2026, l'Assemblée nationale a adopté en première lecture la proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux[1], dans un mouvement convergent avec le gouvernement qui souhaitait aussi encadrer les usages numériques des mineurs. La France s'inscrit ainsi dans la dynamique internationale de régulation des plateformes s'agissant des usages des mineurs et s'apprête à devenir le premier État membre de l'Union européenne (UE) à se doter d'un dispositif d'interdiction ciblant directement l'accès des mineurs aux réseaux sociaux.

Ces initiatives législatives récentes interviennent après des années de relative inertie politique, marquées par les réticences à confronter le pouvoir économique des grandes plateformes et les défis juridiques autour de la régulation de leur modèle, fondé sur la captation de l'attention des utilisateurs et la monétisation des données. À titre d'exemple, force est de constater que les propositions formulées par la commission « Enfants et écrans » et par les États généraux de l'information[2] qui évoquaient des alternatives aux réseaux sociaux actuels n'ont pas trouvé de relais politique.

Quinze ans après les Printemps arabes, le constat est sans appel : **les réseaux sociaux, tels qu'ils fonctionnent aujourd'hui, sont des outils très ambivalents sur le plan démocratique.** Ils s'éloignent **des espaces sains et des vecteurs d'émancipation auxquels beaucoup ont aspiré et exposent les utilisateurs – en particulier les plus jeunes – à des risques majeurs.** Malgré les alertes répétées sur les risques qu'ils engendrent et des années de dialogue et d'initiatives en tous genres, les plateformes n'ont pas intégré les garde-fous nécessaires. Faute d'alternative, les législateurs se résolvent à une **mesure drastique et qui se veut symboliquement forte : l'éviction des mineurs des plateformes, via l'imposition du contrôle de l'âge.** Il y a lieu de prendre acte de cette décision répondant aux besoins de court terme qui sont bien réels, tout en révélant que cette approche n'est qu'une réponse partielle aux causes structurelles des risques que font peser ces services en ligne.

Cette note s'articule par conséquent en trois temps : un rappel des risques pluriels rencontrés par les mineurs en ligne (I), suivi d'un panorama des réglementations actuelles/envisagées et de leurs limites (II). Elle se conclue par une analyse des angles morts de ces dispositions et des pistes pour repenser en profondeur l'encadrement de ces services numériques (III).

En somme, **si l'éviction des mineurs des réseaux sociaux peut sembler une solution de dernier recours, elle ne doit pas servir d'alibi à une refonte en profondeur des espaces numériques, au service de l'ensemble des utilisateurs**.

[1] Assemblée nationale, Protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, déposée le 18 novembre 2025.

[2] Rapport des Etats généraux de l'information, Protéger et développer le droit à l'information : une urgence démocratique,12 septembre 2024.

I. Utilisation des réseaux sociaux : des risques pluriels pour les mineurs en ligne

Le constat est univoque : les réseaux sociaux tels qu'ils fonctionnent actuellement, exposent les mineurs à des risques préjudiciables en ligne en raison des contenus diffusés mais aussi de leurs fonctionnalités, d'après l'Agence nationale de sécurité sanitaire (Anses)[3]. Ces risques, pluriels, ont été catégorisés en « 5C » par l'OCDE en 2021[4] :

- **Les contenus préjudiciables** : il s'agit de l'exposition à des contenus inappropriés, violents, pornographiques, haineux, ou susceptibles de promouvoir les troubles du comportement alimentaire, l'automutilation, voire même les comportements suicidaires.
- **Les contacts risqués**, à l'image d'interactions avec des adultes mal intentionnés (prédation, *grooming*[5]) ou avec des pairs adoptant des comportements toxiques (cyberharcèlement, intimidation, sextorsion[6]). Les mineurs peuvent être manipulés, harcelés ou exposés à des sollicitations dangereuses.
- **Les conduites à risque** concernent les comportements adoptés par les mineurs eux-mêmes, comme le partage excessif d'informations personnelles, la participation à des défis dangereux (comme les défis viraux sur les réseaux sociaux), ou l'engagement dans des activités illégales ou nuisibles (cyberviolence, diffusion de contenus intimes).
- **La consommation excessive et compulsive** des contenus, à même de perturber le sommeil, les relations sociales, les performances scolaires et la santé mentale des mineurs.
- **La contractualisation et les données** : ce dernier point couvre les risques liés à la collecte, à l'exploitation et au partage non maîtrisé des données personnelles des mineurs. Par la signature des conditions générales d'utilisation, les plateformes peuvent utiliser ces données à des fins publicitaires, de profilage ou de monétisation, souvent sans que les mineurs ou leurs parents en aient pleinement conscience.

Si ces risques concernent d'une certaine façon l'ensemble des utilisateurs de réseaux sociaux, ils sont particulièrement prégnants pour les mineurs et sont accentués par plusieurs facteurs, comme le montrent plusieurs études :

- **L'accès de plus en plus précoce aux services numériques**[7] : l'âge moyen de création de compte en France étant 8 ans et demi[8].
- **L'exposition à des contenus traumatisants** : 77 % des 11-17 ans ont déjà été confrontés à des contenus choquants dont 48 % régulièrement et pour un quart d'entre eux avec des conséquences néfastes sur leur bien-être.

[3] Anses, « Usages des réseaux sociaux numériques et santé des adolescents - Connaître, évaluer, protéger », Rapport d'expertise collective, décembre 2025.
[4] OCDE, « Children in the digital environment. Revised typology of risks », OCDE digital economy papers n° 302, Janvier 2021.
[5] Le *grooming*, ou pédopiégeage, désigne *« les mesures prises par une personne qui cherche à établir une relation de confiance avec un enfant (pour éventuellement organiser une rencontre) à des fins sexuelles »*, Action Innocence.
[6] La sextorsion est une menace de montrer des photos de nudité ou des vidéos sexuelles d'une personne à une autre si la première ne fait pas ce qui est demandé, en échange d'argent ou d'autres photos ou vidéos, Ministère de l'Intérieur.
[7] Définis par la Commission européenne comme *« les services intermédiaires tels que les fournisseurs d'hébergement, les places de marché en ligne et les réseaux de médias sociaux »*.
[8] Arcom, « Protection des mineurs : quels risques ? Quelles protections ? », 25 septembre 2025.

- **Le temps croissant passé** sur les contenus en ligne : les 6-17 ans passent en moyenne 4h11 par jour devant un écran (hors école)[9]. Et 31 % des 11-18 ans déclarent rester éveillés ou se réveiller la nuit pour utiliser un écran.
- **L'anxiété**, partagée par 45 % des adolescents après la consultation des réseaux sociaux[10].

Si le lien de cause à effet est difficile à prouver, le *KidsRights Index* 2025 avance **une *« corrélation inquiétante »* entre la dégradation de la santé mentale des mineurs et une utilisation excessive et addictogène des réseaux sociaux**. Il est à noter que si les troubles du jeu vidéo (et des jeux de hasard) sont reconnus sur le plan international comme une *« addiction »*, les médias sociaux, bien que présentant des éléments de conception de type *« addictogène »*, ne sont en l'état pas reconnus comme *« addictifs »*. L'addictivité de ces services est néanmoins de plus en plus questionnée. En 2023, le rapport d'Amnesty International révélait déjà que TikTok *« s'appuyait sur une conception addictive pour générer un maximum d'engagement »*[11]. Le rapport de la commission dite « Enfants et écrans » plaide en ce sens pour reconnaître l'existence de l'addiction aux réseaux sociaux[12]. La Commission européenne a récemment reconnu que l'algorithme de TikTok présentait des caractéristiques addictives[13].

De récentes décisions judiciaires rendues aux États-Unis, fondées sur la conception des plateformes et le rôle joué par leurs interfaces utilisateurs (et non plus sur les contenus), ouvrent la voix aux nombreuses actions intentées, y compris en Europe, à l'encontre des plateformes. Le 24 mars 2026, Meta a été condamnée par un tribunal civil de Santa Fe (Nouveau-Mexique)[14] pour avoir enfreint la loi de l'État sur la protection des consommateurs en omettant de divulguer les risques liés à ses plateformes pour les enfants. En outre, le 25 mars 2026, un tribunal civil de Los Angeles (Californie)[15] a condamné Meta et YouTube pour négligence, pour **avoir sciemment conçu leurs produits afin de les rendre addictifs au détriment de la santé mentale de leurs jeunes utilisateurs.**

L'Anses identifie de son côté des effets néfastes sur la santé des mineurs : **altération du sommeil, dévalorisation de soi, comportements à risque, exposition aux cyberviolences**. L'Autorité de régulation de la communication audiovisuelle et numérique (Arcom)[16] pointe une **exposition plus importante des filles** aux contenus favorisant les troubles du comportement alimentaire. En conclusion, pour l'Anses, le constat est désormais clair : **les réseaux sociaux tels qu'ils existent aujourd'hui ne sont pas adaptés aux jeunes utilisateurs**.

[9] Rapport « Enfants écrans : à la recherche du temps perdu », avril 2024.
[10] Ipsos, « Baromètre du moral des adolescents : un jeune sur quatre fait l'objet d'une suspicion d'un trouble anxieux généralisé », 14 mars 2025.
[11] Amnesty International, « "Je me sens vulnérable"Pris·e au piège de la surveillance intrinsèque à TikTok », 2023.
[12] Rapport « Enfants écrans : à la recherche du temps perdu », avril 2024 , page 46.
[13] Commission européenne, « La Commission conclut à titre préliminaire que la conception addictive de TikTok est contraire à la législation sur les services numériques », 6 février 2026.
[14] Le Monde, « Meta reconnu coupable de mise en danger de mineurs sur ses plateformes par un tribunal du Nouveau-Mexique », 24 mars 2026.
[15] Le Monde, « Instagram et YouTube jugés responsables de la dépression d'une adolescente en Californie : une amende de 6 millions de dollars et un verdict « historique » » , 25 mars 2026.
[16] Arcom, « Protection des mineurs : quels risques ? Quelles protections ? », 25 septembre 2025.

II. Panorama des réglementations sur la protection des mineurs en ligne et grandes questions associées

Face à ce constat alarmant, la France et un nombre grandissant de pays agissent pour tenter de répondre à ces risques qui touchent les utilisateurs des plateformes numériques et plus particulièrement les mineurs. Ces actions sont avant tout réglementaires et peu d'initiatives structurées tendent à proposer des réseaux sociaux au fonctionnement alternatif.

France

La proposition de loi sur l'interdiction d'accès aux réseaux sociaux aux mineurs de moins de 15 ans

L'Assemblée nationale a voté le 26 janvier, en première lecture, la proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, portée par la députée Laure Miller.

➪ **Contexte législatif** dans lequel s'inscrit cette initiative :

- 2023 : Adoption de la loi Marcangeli[17] visant à instaurer une majorité numérique à 15 ans qui n'a pas été mise en œuvre, faute de conformité au droit européen[18].
- 14 juillet 2025 : Publication des lignes directrices de l'article 28 du RSN sur la protection des mineurs, autorisant les États membres à définir un seuil d'âge minimal pour accéder aux réseaux sociaux.
- 18 novembre 2025 : Dépôt de la proposition de loi au Parlement.
- 26 au 27 janvier 2026 : Vote de la proposition de loi à l'Assemblée nationale dans le cadre de la procédure accélérée.

➪ **Contenu de la loi** :

Plateformes concernées :

- Le texte vise les **réseaux sociaux** de manière générale, c'est-à-dire les ***« services de réseau social en ligne »*** au sens du règlement sur les marchés numériques (RMN ou *Digital Market Act*, DMA)[19] et les ***« plateformes en ligne »*** du règlement sur les services numériques (RSN ou *Digital Services Act*, DSA)[20].

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

[18] Cette loi n'a pas respecté les délais de notifications à la Commission européenne, nécessaires pour les propositions de loi qui touchent aux « services de la société de l'information » (plateformes, réseaux sociaux) et tombent donc dans le champ de la directive (UE) 2015/1535.

[19] Le règlement sur les marchés numérique *« vise à lutter contre les pratiques anticoncurrentielles des géants d'internet et corriger les déséquilibres de leur domination sur le marché numérique européen »*, pour en savoir plus voir vie-publique.fr.
Règlement (UE) 2022/1925 sur les marchés numériques, article 2 7) « *service de réseaux sociaux en ligne » : « une 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* ».

[20] Le règlement sur les services numérique *« fixe un ensemble de règles pour responsabiliser les plateformes numériques et lutter contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux : attaques racistes, images pédopornographiques, désinformation, vente de drogues ou de contrefaçons… »*, pour en savoir plus voir vie-publique.fr.

- Sont exclus de manière générale : les services qui ne proposent que de manière accessoire des fonctionnalités sociales ouvertes.
    - Exemple : Toute plateforme de partage de vidéo sans fonctionnalités sociales ouvertes. Ces plateformes restent accessibles par défaut.

- Sont exclus de manière spécifique : les encyclopédies en ligne, les répertoires éducatifs ou scientifiques, les plateformes de développement et de partage de logiciels libres. Les mineurs pourront donc y accéder.

Interdiction du téléphone portable :

- Extension de l'interdiction du téléphone portable au lycée. Il appartient à chaque établissement d'introduire l'interdiction dans son règlement intérieur et de la moduler selon les usages de l'établissement.

➪ **Articulation avec le droit de l'UE** :

La Commission européenne a validé la compétence de la France à interdire les réseaux sociaux aux moins de 15 ans[21], tout en précisant qu'il appartenait à la Commission seule d'imposer des obligations supplémentaires aux très grandes plateformes.

Contrôle et surveillance : l'Arcom sera chargée de veiller au respect de l'interdiction et aura pour rôle de :

- Contrôler le respect de la majorité numérique sur les réseaux sociaux établis en France et en dehors de l'UE ;
- Saisir les États membres d'origine pour les services installés dans l'UE mais hors de France ;
- Saisir la Commission européenne ou les autorités nationales compétentes en cas de manquement à la vérification de l'âge par les plateformes, conformément au RSN.

Sanctions : En cas de non-respect des obligations, la Commission européenne est compétente au titre du RSN pour imposer des sanctions pouvant aller jusqu'à 6 % du chiffre d'affaires mondial annuel réalisé au cours de l'exercice précédent.

Règlement (UE) 2022/206 sur les services numériques, article 3 : *« plateforme en ligne » : « un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse au public des informations, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d'un autre service ou une fonctionnalité mineure du service principal qui, pour des raisons objectives et techniques, ne peut être utilisée sans cet autre service et pour autant que l'intégration de cette caractéristique ou de cette fonctionnalité à l'autre service ne soit pas un moyen de contourner l'applicabilité du présent règlement ».*

[21] Le Monde, « La France a le droit d'interdire les réseaux sociaux aux moins de 15 ans, juge la Commission européenne », 27 janvier 2026.

➪ **Prochaines étapes** :
- Procédure de notification lancée auprès de la Commission européenne dont les résultats sont encore attendus et *statu quo* pendant trois mois[22].
- Première lecture par la commission de la culture du Sénat le 25 mars 2026.
- Débat au Sénat[23] en séance publique à partir du 31 mars, dans le cadre de la procédure accélérée.

Au **niveau européen**, le **Parlement** a adopté en novembre 2025 une résolution appelant à fixer l'âge minimum à 16 ans pour pouvoir accéder aux réseaux sociaux, aux plateformes de partage de vidéos et aux compagnons IA au sein de l'UE, tout en permettant l'accès aux 13-16 ans, à condition de disposer d'un consentement parental. Du côté de la **Commission européenne**, un panel d'experts est réuni[24] pour évaluer les moyens de renforcer la protection juridique des mineurs, au-delà du RSN.

Ces initiatives ne sont pas isolées et s'inscrivent dans un **mouvement international de régulation des services numériques au bénéfice d'une meilleure protection des mineurs en ligne**. Le cas australien, pionnier en la matière, a été abondamment souligné, mais des mesures ont également été prises au Royaume-Uni, en Chine, en Californie et sont en voie de définition ailleurs, comme en Espagne[25], au Portugal[26], en Norvège[27], au Danemark[28], en Autriche[29] ou en Slovénie[30].

Australie

L'Online Safety Act australien[31]

L'Australie est devenue le premier pays au monde à mettre en œuvre l'interdiction de l'accès aux réseaux sociaux pour les mineurs de moins de 16 ans. Cette mesure a été introduite en novembre 2024 par un amendement sur le ***Social Media Minimum Age***[32], modifiant l'*Online Safety Act* de 2021. Le texte est entré en vigueur le 10 décembre 2025.

[22] Conformément à la directive (UE) 2015/1535, les États membres doivent informer la Commission de tout projet de règle technique avant son adoption. À partir de la date de notification du projet, une période de statu quo de trois mois débute – au cours de laquelle l'État membre, auteur de la notification, ne peut pas adopter la règle technique en question – permettant à la Commission et aux autres États membres d'examiner le texte notifié et de répondre de façon appropriée. Plus d'informations sur le site de la Commission européenne.
[23] Sénat, Ordre du jour des prochaines séances du Sénat, 18 février 2026.
[24] Commission européenne, « La Commission tient la première réunion du groupe spécial sur la sécurité des enfants en ligne », 5 mars 2026.
[25] Contexte, « L'Espagne se lance à son tour dans l'interdiction des réseaux sociaux (aux moins de 16 ans) », 4 février 2026.
[26] El Pais, « Portugal avanza para controlar el accesso de los menores a las redes sociales », 2 février 2026.
[27] 20minutes, « La Norvège souhaite interdire les réseaux sociaux aux moins de 15 ans », 25 octobre 2025.
[28] Contexte, « Le Danemark aux avant-postes sur la majorité numérique », 9 octobre 2025.
[29] France Info, « L'Autriche va interdire les réseaux sociaux aux moins de 14 ans », 27 mars 2026.
[30] Contexte, « La Slovénie, nouveau candidat à la majorité numérique », 6 février 2026.
[31] Online Safety Act, 2021.
[32] Australian Government, Social Media Minimum Age .

Ce texte impose aux plateformes de réseaux sociaux de *« prendre des mesures raisonnables »* pour veiller à ce qu'elles ne soient accessibles qu'aux utilisateurs âgés de plus de 16 ans, qu'il s'agisse d'utilisateurs nouveaux ou d'utilisateurs déjà inscrits. Les comptes existants appartenant à des moins de 16 ans doivent donc être désactivés ou supprimés. Cette interdiction ne précise pas quelles mesures techniques les plateformes doivent privilégier pour se conformer à la loi et fixe ainsi un objectif de résultats plutôt que de moyens.

Par ailleurs et fait notable, cette obligation s'applique à une liste restreinte de réseaux sociaux officiellement désignés en novembre 2025. Sont ainsi concernés **Facebook, Instagram, Reddit, Snapchat, TikTok, Twitter, Threads, Twitch, Kick et YouTube**.

Les plateformes qui ne respectent pas ces obligations s'exposent à des amendes pouvant atteindre 50 millions de dollars australiens (environ 30,7 millions d'euros) imposées par le e*Safety Commissioner* et le Bureau du Commissaire australien à l'information (OAIC).

Si le recul manque à ce jour, de nombreux comptes d'utilisateurs de moins de 16 ans ont été supprimés. Un mois après l'entrée en vigueur de la loi, l'Australie recensait déjà 4,7 millions de comptes désactivés, restreints ou supprimés par les dix plateformes concernées[33]. Ce chiffre reste toutefois à mettre en perspective : 2,5 millions des 8-15 ans possèdent chacun plusieurs comptes sur différentes plateformes. Les utilisateurs de moins de 16 ans peuvent télécharger et sauvegarder le contenu de leurs comptes qui seront désactivés jusqu'à leur 16 ans. Ils pourront alors le récupérer.

En cas d'erreur, les utilisateurs concernés peuvent contester la décision de désactivation de compte auprès de la plateforme. Ils devront alors transmettre une pièce d'identité officielle ou une vidéo faciale pour confirmer leur âge au réseau social.

La question préalable qui se pose au législateur est de définir un seuil d'âge en dessous duquel l'utilisateur ne peut accéder à certains services numériques, ce qui n'est pas sans susciter de nombreux débats.

La **proposition d'une *« majorité numérique »* en France** s'inscrit également dans cette logique. Pour rappel, une majorité numérique avait déjà été fixée à 15 ans en 2023 en droit français[34] mais, faute de décret d'application et d'aval de la Commission européenne quant à sa conformité au droit européen, celle-ci n'est pas appliquée. La doctrine de la Commission a

[33] Libération, « Vu de Melbourne - En Australie, un mois après la loi interdisant les réseaux sociaux aux moins de 16 ans : «Ils sont tous restés sur Snapchat» », 25 janvier 2026.

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

évolué via la publication de ses lignes directrices[35] qui permettent désormais aux États membres de fixer cette majorité. Le Conseil d'État, dans son avis[36] sur la proposition de loi, propose un système hybride où les services de réseaux sociaux demeurent accessibles en ligne pour les mineurs de moins de 15 ans avec une autorisation parentale.

Aux **États-Unis**, le *Children's Online Privacy Protection Act* (COPPA) fixe l'âge minimal à 13 ans pour la **collecte de données personnelles sans consentement parental**. Ce seuil est d'ailleurs largement adopté par les plateformes internationales comme seuil limite à la création d'un compte.

Au sein de l'**UE**, le RGPD fixe à 16 ans l'âge minimal pour que les mineurs puissent consentir seuls au traitement de leurs données personnelles. Cependant, les États membres peuvent ajuster ce seuil. L'Irlande l'a ainsi établi à 13 ans et la France à 15 ans.

Ces différences de choix de seuil d'âge témoignent de la complexité à le définir et de leur variabilité selon les thématiques auxquelles ils s'appliquent.

Au-delà du choix de ce seuil, les réglementations qui visent à protéger les mineurs en ligne sont confrontées à plusieurs questions de méthodologie :

- Quel est le périmètre d'application de la loi ? (a.)
- Quelle méthode de contrôle de l'âge mettre en place, en prenant en compte leurs éventuels contournements ou effets délétères ? (b.)
- Quels sont les contenus devant être assujettis à la réglementation ? (c.)

Ces différentes variables seront analysées et illustrées par des exemples de réglementations ou d'initiatives mises en place par les plateformes.

(a) Quel périmètre d'application de la loi ?

Lorsqu'un périmètre est défini, l'enjeu est de choisir entre régulation ciblée, au risque de tendre vers une régulation du cas par cas et approche globale, qui peut se heurter à des difficultés d'application.

(1) Les réglementations qui visent certaines catégories de services numériques

Certains États ont fait le choix de viser des plateformes spécifiques comme en Australie où seules les plateformes qualifiées de *« réseaux sociaux »* et nominativement listées sont soumises à la législation. L'intégration de YouTube (et non de YouTube Kids) a par exemple suscité de nombreux débats quant à sa

[35] 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.

[36] Conseil d'Etat, avis consultatif sur une proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, 13 janvier 2026.

qualification en tant que réseau social. La plateforme a finalement été incluse pour ses *« contenus inappropriés »* et ses *« algorithmes prédateurs »* selon les termes de la ministre de la Communication du pays, Anika Wells.

Cependant, la délimitation restrictive du périmètre pose question au regard des finalités poursuivies par le texte : de nombreux autres services numériques peuvent présenter des risques pour les moins de 16 ans, comme les messageries privées et les jeux vidéo en ligne. Pour ne citer qu'un exemple, le jeu en réseau Roblox n'est pas assujetti à ce texte. Pourtant, sur les 111,8 millions d'utilisateurs actifs[37] par jour à travers le monde, la moitié ont moins de 13 ans. Or, la plateforme présente des fonctionnalités proches de celles d'un réseau social : profil personnalisé, constitution d'un réseau d'ami, chat pour communiquer avec d'autres utilisateurs etc. Et les risques existent : la société de recherche Hindenburg Research qualifiait même la plateforme *« d'enfer pédophile pour les enfants »*[38], montrant qu'il existerait une cinquantaine de groupes réunissant plus de 100 000 membres s'échangeant des contenus pédocriminels et sollicitant des actes sexuels auprès de mineurs.

Face à cette liste indicative, il existe un risque réel de report sur d'autres plateformes plus obscures, voire sur de nouvelles plateformes créées à la suite de l'entrée en vigueur de la loi. S'il est encore trop tôt pour mesurer ces éventuels reports, certains usages sont révélateurs. Des adolescents rapportent passer plus de temps à jouer à des jeux vidéo ou à communiquer avec leurs amis via d'autres canaux comme WhatsApp ou Messenger[39] depuis l'entrée en vigueur de l'interdiction. D'autres plateformes alternatives ont enregistré une hausse des téléchargements, en particulier les concurrents à l'audience moins importante tels que Bluesky, Yubo, plateforme communautaire française et Lemon8, une plateforme de vidéo semblable à TikTok et détenue par la même société mère, ByteDance[40]. Cette hausse reste toutefois limitée car, après avoir enregistré un pic de 25 000 téléchargements quotidiens dans les jours suivants l'interdiction, les téléchargements des plateformes de réseaux sociaux interdits sont revenus à leur niveau habituel dix jours plus tard[41].

Le 6 mars 2026, le eSafety a annoncé[42] le lancement de nouveaux codes de sécurité en ligne (*Age-Restricted Materials Codes*) visant à assurer que les enfants vivent des expériences en ligne adaptées à leur âge et ne soient pas exposés à des contenus nocifs. Ce pas complémentaire, visant cette fois-ci les contenus et non les plateformes en tant que telles, marque une nouvelle étape dans le cadre australien. Sont visés les **contenus violents à fort impact, la pornographie, les contenus promouvant le suicide, l'automutilation et les troubles alimentaires**. Ces codes

[37] Statista, Utilisateurs actifs quotidiens du jeux Roblox dans le monde entier du 4ème trimestre 2018 au 2ème trimestre 2025.
[38] France inter, « Roblox, la plateforme de jeu pour enfants est un "enfer pédophile" », 14 octobre 2024.
[39] BBC, « Australia social media ban: Teens share their views one month on », 9 janvier 2026.
[40] Financial Times, « Social media companies purge 4.7mn accounts after landmark Australia ban », 16 janvier 2026.
[41] Apptopia, dans BBC, « Australia social media ban: Teens share their views one month on », 9 janvier 2026.
[42] eSafety Commissioner, *Online safety codes introduce real-world protections for children online*, 6 mars 2026.

couvriront également les ***chatbots* compagnons alimentés par l'IA** pour les empêcher d'engager des conversations sexuelles explicites avec des mineurs ou encourageant l'automutilation et le suicide (les contenus visés), **les magasins d'application pour le téléchargement d'applications catégorisées plus de 18 ans, les messageries pour adulte spécialisées dans la distribution des contenus visés, les jeux en ligne classés plus de 18 ans, les moteurs de recherche lorsque les recherches portent sur les contenus visés, les services de médias sociaux** qui permettent d'accéder aux contenus visés.

À l'inverse, la France cible les *« services de réseaux sociaux en ligne fournis par une plateforme en ligne »*[43], sans proposer de liste limitative mais en discriminant selon leurs fonctionnalités, c'est-à-dire dès lors qu'ils permettent de communiquer avec des utilisateurs.

En ne visant que certains services numériques, de manière limitative ou non, le risque est de ne pouvoir contrôler et sanctionner d'autres plateformes dont les contenus peuvent pourtant être nocifs car elles n'entrent pas dans le périmètre de la loi. L'exemple australien qui, au moment du vote de la loi, paraissait ambitieux, semble aujourd'hui montrer ses limites alors que de nombreuses autres plateformes à risque demeurent accessibles, l'élargissement par type de contenus ayant rapidement été nécessaire.

(2) Les réglementations qui assujettissent des services numériques à de nouvelles obligations selon leur nombre d'utilisateurs

Le champ d'application peut également varier en fonction du nombre d'utilisateurs, distinction notamment opérée par le RSN qui constitue une réglementation *« asymétrique »*, dont les obligations varient selon la nature des services et leur taille. Le règlement distingue ainsi quatre catégories de plateforme en ligne : (i) les *« très grandes plateformes »* qui comptent plus de 45 millions d'utilisateurs par mois dans l'UE, (ii) les fournisseurs d'accès à internet, (iii) les services d'informatique en nuage (*cloud*) et (iv) les plateformes en ligne comme les places de marché, les réseaux sociaux, les plateformes de partage de contenus, les plateformes de voyage et d'hébergement. De manière générale, toutes les catégories de plateformes doivent lutter contre les contenus illicites, être davantage transparentes sur la modération des contenus et sur le fonctionnement de leurs algorithmes et ne pas proposer de publicité ciblée aux mineurs. Les très grandes plateformes se voient imposer d'autres mesures plus contraignantes pour atténuer les risques qu'elles peuvent engendrer.

Quel que soit le périmètre choisi, des critiques émergent dans leur définition. Il peut sembler trop restreint ou trop large. Ainsi, certains soulignent la nécessité d'une régulation globale des services numériques pris dans leur diversité, qui s'illustre par exemple dans la position officielle du Parlement européen. Ce dernier invite à réguler à la fois les réseaux sociaux, les plateformes vidéo et les *« compagnons IA »*. Si cette vision semble nécessaire à l'heure où les usages évoluent et se déplacent, l'enjeu est de formuler des dispositions pouvant s'appliquer à des services aussi divers et dont le fonctionnement et les usages peuvent fortement différer. **Il apparaît aujourd'hui nécessaire de réglementer les usages numériques au-delà des réseaux**

[43] Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, adopté par l'Assemblée nationale en première lecture le 26 janvier 2026.

sociaux, sans attendre que ceux-ci ne soient trop installés et conduisent à une multiplication de risques inacceptables (voir *supra* II, point 2).

(b) Quelles méthodes de contrôle de l'âge et quels contournements ou effets délétères ?

Les mesures de protection combinent souvent vérification de l'âge, interdictions d'accès, limites de temps et interfaces adaptées. **La vérification de l'âge constitue fréquemment l'étape préalable à l'instauration de toute autre mesure complémentaire**[44]. Du côté du RSN, les mesures de vérification de l'âge sont jugées appropriées lorsqu'aucun autre moyen ne permet de mitiger les risques.

(1) Les différentes méthodes du contrôle de l'âge et leurs applications

Le contrôle de l'âge des utilisateurs est communément devenu le préalable des politiques de protection des mineurs dans l'espace numérique. Il s'agit de vérifier, de manière fiable et sécurisée, que l'accès à certains contenus, fonctionnalités, services ou plateformes est réservé aux publics autorisés, en fonction de leur âge.

La Commission européenne[45] distingue trois méthodes de vérification de l'âge :

- **L'auto-déclaration**, méthode la plus répandue, consiste, pour l'utilisateur, à indiquer son âge ou à confirmer sa tranche d'âge, *« soit en renseignant volontairement sa date de naissance ou son âge, soit en déclarant qu'il a plus d'un âge donné »*.
  Cette méthode s'avère peu efficace et facile à contourner. Une étude menée par l'Arcom[46] en 2025 révèle que près de deux tiers des jeunes interrogés (62 %) reconnaissent avoir déjà menti sur leur âge pour s'inscrire sur une plateforme. La principale raison avancée étant qu'ils n'avaient pas encore l'âge minimum requis (65 %).

- **L'estimation de l'âge**, peu utilisée, permet « *à un fournisseur de déterminer qu'un utilisateur est susceptible d'avoir un âge donné, de se situer dans une certaine tranche d'âge ou d'être plus âgé ou plus jeune que l'âge donné* ». En pratique l'âge peut être estimé par reconnaissance faciale, ce qui nécessite la collecte de données biométriques. L'âge peut également être estimé, par le croisement de données d'usages (habitudes de consommation, temps passé sur certains contenus, inscription sur les listes électorales, achats etc.) avec les données personnelles déclaratives (adresse e-mail, nom et prénom etc.). Cette méthode est considérée comme étant la moins fiable dans un rapport du gouvernement australien[47].

Pour autant, YouTube teste depuis août 2025 un outil d'intelligence artificielle (IA) pour estimer l'âge de ses utilisateurs aux États-Unis, dans le but de protéger les mineurs. Cet outil vise à

[44] Cette technique est préconisée ou mise en place dans de nombreux pays, notamment Australie, Chine, Malaisie, Turquie, Kenya, Pakistan, Papouasie-Nouvelle-Guinée, Nouvelle Zélande, Texas, Papouasie-Nouvelle-Guinée, Kenya, Malaisie.

[45] 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, paragraphes 28 et 29.

[46] Arcom, « Protection des mineurs : quels risques ? Quelles protections ? », 25 septembre 2025.

[47] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, « Age Assurance Technology Trial— Final Report », 31 août 2025.

déduire l'âge des utilisateurs, sans prendre en compte la date de naissance déclarée lors de la protection du compte, pour proposer *« des expériences et des protections adaptées »*[48], selon la plateforme. Ainsi, dès lors que l'outil identifie un utilisateur comme étant mineur, la publicité ne sera plus personnalisée et des mesures de restriction et de sécurité seront mises en place. Si les utilisateurs estiment que l'estimation d'âge est incorrecte, ils peuvent fournir une pièce d'identité officielle pour vérifier leur âge. Si l'expérience s'avère fructueuse, l'outil pourrait être généralisé au-delà des États-Unis.

En **Australie**, le seuil choisi est celui de 16 ans pour l'accès aux réseaux sociaux, quelle que soit la méthode retenue par les plateformes pour atteindre cet objectif. Ce choix peut traduire, en creux, le constat que les plateformes peuvent d'ores et déjà disposer des données suffisantes pour inférer l'âge des utilisateurs sans avoir besoin de vérifier de manière précise leur âge, même si cette estimation peut avoir des limites (voir *infra*).

Aussi, le nombre d'utilisateurs ayant contourné la mesure n'est pas encore estimé avec fiabilité. Toutefois, la Commissaire eSafety, Julie Inman Grant, a déclaré à la BBC qu'une série d'avis de préoccupation concernant des anomalies et des faiblesses dans la mise en œuvre de l'interdiction est sur le point d'être envoyée aux entreprises[49]. Snapchat est notamment visé car le réseau social – dont nombre d'utilisateurs sont mineurs – a recours à des méthodes d'estimation de l'âge fondées sur de la reconnaissance faciale sans vérifier qu'il s'agit d'images réelles[50].

Les nouveaux codes de sécurité en ligne (*Age-Restricted Materials Codes*) annoncés en mars 2025 précisent d'ailleurs qu'un contrôle de l'âge sera exigé, l'auto-déclaration ayant été jugée trop peu efficace[51].

- **La vérification de l'âge à l'aide d'« *identifiants physiques ou des sources d'identification vérifiées* »** est de plus en plus discutée par les législateurs[52]. Elle repose sur la communication de preuve d'âge, qui ont été certifiées et émises sur la base de documents officiels.

En France, la loi visant à sécuriser et à réguler l'espace numérique (SREN)[53] de mai 2024 impose aux services diffusant des contenus pornographiques de mettre en place un système de vérification de l'âge des utilisateurs. Le texte prévoit que l'Arcom *« établit et publie […], après avis de la Commission nationale de l'informatique et des libertés* [CNIL]*, un référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge. Ces exigences portent sur la fiabilité du contrôle de l'âge des utilisateurs et le respect de leur vie*

[48] AFP, « YouTube va deviner l'âge des utilisateurs grâce à l'IA », 14 août 2025.
[49] BBC, « Social media firms have come to ban 'kicking and screaming', says Australia eSafety boss », 23 janvier 2026.
[50] The Guardian, « Snapchat blocks more than 400,000 Australian accounts but warns of 'significant gaps' in under-16s social media ban », 1er février 2026.
[51] eSafety Commissioner, *Online safety codes introduce real-world protections for children online*, 6 mars 2026.
[52] Notamment au Royaume-Uni, en Australie, en Chine, en Malaisie, en Turquie, au Kenya, au Pakistan, en Papouasie-Nouvelle-Guinée, en Nouvelle Zélande, ainsi que dans certains États des États-Unis.
[53] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite loi « SREN ».

privée »[54]. À la suite de travaux conjointement menés par la CNIL et le Pôle d'Expertise de la Régulation Numérique (PEReN), un référentiel technique a été publié en octobre 2024. Celui-ci ne vise pas à certifier des solutions techniques mais laisse *« les services visés diffusant des contenus à caractère pornographique […] libres de choisir les solutions de protection des mineurs de leur choix, dès lors qu'elles respectent les exigences techniques du référentiel »*. Aujourd'hui, dix-sept sites pornographiques ont expressément été visés et soumis à l'obligation immédiate de mettre en place des dispositifs de vérification d'âge robustes et protecteurs des données personnelles pour empêcher les mineurs d'accéder à ces contenus. Plusieurs solutions ont été mises en place par ces sites comme l'envoi d'une photo ou courte captation vidéo de son visage qui est ensuite analysé par l'IA ou l'envoi d'une copie d'un document d'identité. Ces solutions entrent en contradiction avec la protection des données personnelles, qui sont collectées par les plateformes.

D'autres pays de l'UE ont mis en place des obligations similaires comme l'Espagne, l'Allemagne, le Danemark ou l'Italie. Les lignes directrices de la Commission européenne, prises en complément de l'article 28 du RSN[55], viennent sécuriser cette démarche en imposant la vérification de l'âge obligatoire pour l'accès aux sites ou plateformes pornographiques dans toute l'UE. Des travaux sont en cours pour offrir une solution harmonisée de vérification de l'âge au sein de l'UE.

L'*Online Safety Act* au **Royaume-Uni** impose aux services hébergeant des contenus nocifs pour les mineurs la vérification de l'âge par le téléchargement d'un document d'identité accompagné d'une image faciale de l'utilisateur, l'utilisation d'un **portefeuille numérique** ou le recours aux services bancaires, parmi d'autres moyens[56]. La plateforme Pornhub a ainsi annoncé, après avoir enregistré une baisse du trafic de 70 % au Royaume-Uni, empêcher les nouveaux utilisateurs d'accéder à son site, en justifiant sa mesure par l'OSA[57].

Le portefeuille numérique est également en vigueur en Papouasie-Nouvelle-Guinée, *via* l'application gouvernementale *SevisPassWallet*. Les utilisateurs y stockent leurs identifiants numériques[58]. Conçu comme une infrastructure publique numérique (DPI), ce portefeuille numérique permet de se connecter aux services publics en ligne, mais aussi d'ouvrir un compte bancaire et d'enregistrer une carte SIM mobile.

[54] Arcom, Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, octobre 2024.
[55] 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.
[56] Ofcom, « Age checks for online safety – what you need to know as a user », juin 2025.
[57] The Guardian, « Pornhub to stop new UK users accessing site from next week », 27 janvier 2026.
[58] Department of Information And Communications Technology, « Presentation - PNG eGov Portal », octobre 2024.

Des réflexions attendues sont portées au niveau européen avec le portefeuille numérique *European Digital Identity Wallet*. L'objectif est de fournir à chaque citoyen et à chaque entreprise un moyen d'identification numérique reconnu au sein de l'UE, **interopérable, sécurisé et respectueux du contrôle des données personnelles**. Chaque État membre devra proposer au moins un EUDI Wallet aux citoyens, résidents et entreprises, au plus tard fin 2026. Ces outils pourront notamment fournir une **preuve d'âge**. Dans ce cadre, la Commission européenne a lancé une expérimentation coordonnée dans cinq États membres, dont la France, concernant la vérification de l'âge[59] pour l'accès aux réseaux sociaux. L'application est fondée sur un prototype européen que chacun des cinq États membres peut moduler selon les règles en place sur son territoire dans le but de proposer des versions nationales personnalisées d'ici quelques mois.

(2) Enjeux sous-jacents au contrôle de l'âge

Au-delà de la question de l'âge plancher, **l'établissement d'une règle unique peut également interroger**. Un consensus pluridisciplinaire[60] s'accorde sur le fait qu'il est nécessaire de penser les besoins de l'enfant *« au regard de son âge, de son développement et de sa singularité »*. Les besoins de protection varient donc en fonction de l'âge mais aussi du degré de maturité, lequel n'est pas nécessairement corrélé à l'âge, ainsi que des usages numériques.

Ces questions sont le reflet des débats français sur la définition du seuil d'âge. D'une part, certains groupes politiques s'étonnent du choix de 15 ans porté par la proposition de loi alors que le seuil d'accès aux réseaux sociaux est aujourd'hui celui de 13 ans (principalement inscrit dans les conditions générales d'utilisation). L'Arcom veille au respect de ce seuil tout en notant que 44 % des jeunes accèdent aux réseaux sociaux avant 13 ans[61]. D'autre part, le choix du seuil de 15 ans est aligné, en France, sur la majorité sexuelle, l'âge à partir duquel il est possible de consentir, sans contrôle parental, à la collecte de données personnelles au titre du RGPD, l'âge à compter duquel il est possible de conclure un contrat d'apprentissage, de percevoir un salaire, de consulter un médecin sans autorité parentale etc. Enfin, les experts de la commission « Enfants et écrans » recommandent l'interdiction des réseaux sociaux aux mineurs avant l'âge de 15 ans, lequel *« correspond le plus souvent à l'âge de passage au lycée, qui représente une étape importante dans l'adolescence et dans le parcours du jeune vers son autonomie progressive »*[62].

D'autres voix font valoir que **l'interdiction d'accès avant un certain âge peut se révéler contre-productive, en privant les jeunes d'un apprentissage progressif et encadré de ces espaces numériques**. Le psychiatre Serge Tisseron alerte sur le fait que la chute sera plus dure, car *« découvrir les réseaux sociaux après 15 ans ne protège de rien »*[63]. Le mouvement européen de lutte pour les droits numériques, créé par et pour les jeunes, ctrl+alt+reclaim estime également

[59] Le Monde, « Cinq pays européens, dont la France, vont tester une application pour vérifier l'âge des utilisateurs sur Internet », 14 juillet 2025.
[60] Démarche de consensus sur les besoins fondamentaux de l'enfant en protection de l'enfance, Rapport remis par le Dr Marie-Paule Martin-Blachais à Laurence Rossignol, Ministre des familles, de l'enfance et des droits des femmes, 28 février 2017.
[61] Arcom, « Mineurs et internet : L'Arcom présente ses priorités en matière de régulation des plateformes numériques, afin de faire d'internet un lieu plus sûr pour les enfants et les adolescents », 25 septembre 2025.
[62] Rapport « Enfants écrans : à la recherche du temps perdu », avril 2024.
[63] Le Monde, « Serge Tisseron, psychiatre : « Découvrir les réseaux sociaux après 15 ans ne protège de rien »», 7 janvier 2026.

qu'*« interdire ne prévient pas les préjudices des réseaux sociaux »*[64]. Le report de l'accès aux réseaux sociaux pourrait exposer les adolescents à une **immersion soudaine et non préparée dans un environnement complexe**, où ils devront gérer des enjeux comme la gestion de leur image en ligne, les interactions sociales, ou encore l'exposition à des contenus variés, sans avoir bénéficié d'une expérience graduelle pour développer leur esprit critique et leur appropriation de ces outils et leurs paramètres.

Certaines plateformes profitent de ce débat sur le contrôle de l'âge pour s'exonérer de leurs responsabilités et plaident ainsi pour un contrôle de l'âge au niveau de l'appareil[65], lors de la création d'un compte sur un magasin d'applications sur *smartphone* ou via le système d'exploitation de l'appareil. Cette solution est présentée par les plateformes comme plus simple pour les utilisateurs et pour les acteurs numériques et moins perméable aux contournements, plus robuste en harmonisant les systèmes de vérification utilisés et les garanties associées en termes de fiabilité et de protection de la vie privée.

Toutefois, cette option semble avant tout trop extensive au regard du faible nombre d'applications *in fine* concernées par le contrôle de l'âge[66]. Cela pourrait également conduire les plateformes et les développeurs d'applications à se soustraire à leurs obligations alors qu'ils doivent être impliqués dans la réduction des risques liés à leurs services. En outre, ce système est peu compatible avec des outils numériques partagés par exemple au sein d'un foyer avec plusieurs utilisateurs d'âges différents.

(3) Le risque du contournement du contrôle de l'âge

- **Les contournements volontaires**

D'un point de vue technique, ces méthodes de vérification de l'âge sont perméables aux contournements. Le **recours à des VPN**[67] figure parmi les contournements les plus répandus.

Le téléchargement de Proton VPN, acteur majeur du marché, a, par exemple, connu en **France**[68] une hausse de 1 000 % suite à la mise en œuvre de la vérification de l'âge sur les sites pornographiques.
Ce chiffre doit néanmoins être nuancé puisque cette mesure a fait baisser la consommation de contenus pornographiques chez un Français sur quatre. 10 % disent même avoir totalement délaissé les sites spécialisés, pourcentage qui atteint 20 % chez les 18-24 ans. Si la baisse de la consommation apparaît comme une certaine réussite, le recours aux VPN est privilégié par

[64] Le Monde, « Interdiction des réseaux sociaux aux moins de 15 ans : « La voix des jeunes est absente du débat sur la régulation du numérique », 25 janvier 2026.
[65] Euractiv, « Meta demande une réglementation européenne sur la vérification de l'âge pour l'utilisation des réseaux sociaux », 5 novembre 2025 ; Next, « Vérification d'âge : Pornhub appelle Apple, Google et Microsoft à l'intégrer aux appareils », 21 novembre 2025.
[66] 01net, « Tim Cook en croisade contre la vérification d'âge obligatoire sur l'App Store », 11 décembre 2025 ; France 24, « Vérification de l'âge en ligne : Google opposé à tout contrôle au niveau des boutiques d'applications », 13 juin 2025.
[67] Un VPN (*virtual private network*, réseau privé virtuel) est un outil qui se comporte comme un fournisseur d'accès à internet (FAI) virtuel connectant des appareils à un réseau, masquant l'adresse IP de l'utilisateur en la remplaçant par celle du fournisseur de VPN, simulant une localisation géographique différente. Cette technologie rend le trafic opaque pour les FAI et les sites web visités.
[68] « Les VPN contournent la nouvelle réglementation de l'Arcom sur les contenus pour adulte », 15 octobre 2025.

60 % des interrogés. Aussi, 30 % des 18-24 ans se tournent en réponse vers d'autres plateformes en dehors du périmètre de la mesure[69].

> Au **Royaume-Uni**[70], malgré une profusion de gros titres de presse concernant l'utilisation des VPN, l'existence d'un lien direct entre l'introduction d'interdictions et **l'augmentation de l'usage des VPN n'est pas avéré**. L'*Ofcom* observe que, malgré un pic initial atteignant jusqu'à 1,5 millions d'utilisateurs quotidiens actifs à la suite de l'interdiction d'accès à la pornographie pour les mineurs et des dispositifs de vérification de l'âge pour certains réseaux sociaux en juillet 2025, l'usage est rapidement retombé sous 1 million avant octobre[71]. En outre, le *UK Safer Internet Center* précise que cette hausse n'était pas nécessairement imputable aux mineurs, mais principalement à des adultes préoccupés de leur anonymat en ligne[72].

En dehors des VPN, certains utilisateurs se tournent aussi vers d'autres méthodes, telles que le **marché noir des comptes vérifiés**[73] où s'achètent et se revendent des comptes vérifiés comme appartenant à des plus de 16 ans.

Parmi d'autres exemples, un article de la BBC cite le cas d'une adolescente ayant utilisé une photo de sa mère pour avoir accès à Snapchat alors que le réseau social lui annonçait que son compte allait être bloqué lors de l'entrée en vigueur de la loi australienne[74].

- **Les difficultés en termes d'inclusivité et d'accessibilité**

La vérification de l'âge fondée sur la transmission d'un document d'identité risque d'exclure les mineurs les plus vulnérables. L'UNICEF[75] alerte en effet sur le fait que les systèmes d'état civil de nombreux pays sont incomplets ou inégaux. Des millions de mineurs ne disposent pas de preuve officielle de leur identité. Ces mineurs seraient ainsi doublement pénalisés : victimes d'éloignement numérique et privés des mesures de protection reposant sur la vérification de l'âge, renforçant les inégalités. En France, pour rappel, il n'est pas obligatoire de détenir un titre d'identité.

Dans le même temps, **les mécanismes de vérification de l'âge doivent impérativement être accessibles aux personnes en situation de handicap**, notamment aveugles ou à faible vision et **se conformer aux normes nationales d'accessibilité**[76], en garantissant la compatibilité avec les technologies d'assistance, des interfaces compréhensibles et des alternatives aux captchas ou procédures reposant sur la seule vision. À défaut, ces dispositifs renforceraient les

[69] 01net, « Vérification de l'âge sur les sites pornos : 25% des Français ont réduit leur consommation », 17 décembre 2025.
[70] The Verge, « The UK is slogging through an online age-gate apocalypse », 28 juillet 2025.
[71] Ofcom, « Online Safety in 2025 », 4 décembre 2025.
[72] UK Safer Internet Centre, "Young People's Use of VPNs", 1er décembre 2025.
[73] Financial Times, « The countdown to the world's first social media ban for children », décembre 2025.
[74] BBC, « Can you ban kids from social media? Australia is about to, but some teens are a step ahead», 6 décembre 2025.
[75] UNICEF, « Digital Age Verification: Risks and Opportunities for Children », 2023.
[76] Center for Democraty and Technology, « Mitigating risk to rights with age verification : Privacy-preserving guardrails that should accompany deployments of age verification approaches », 10 octobre 2025.

vulnérabilités des mineurs en situation de handicap, pour lesquels les barrières d'accès au numérique seraient renforcées sous couvert de protection.

(c) Quels sont les contenus visés par ces législations ?

Certains textes ciblent des catégories de contenus de manière précise en raison des risques qu'ils présentent pour certains publics dits *« vulnérables »*, quand d'autres ont une visée plus large, englobant différentes catégories de contenus.

(1) Les réglementations ciblant des catégories de contenus en particulier

Les législations française et britannique ont opté pour le ciblage des contenus considérés comme nocifs. En France, la loi SREN a, entre autres, pour objectif de mettre en place des mesures de vérification de l'âge pour accéder aux contenus pornographiques.

> Au Royaume-Uni, l'*OSA* impose aux plateformes de réseaux sociaux et aux moteurs de recherche de mettre en place des mesures vérification de l'âge pour empêcher l'accès aux mineurs à des **contenus** qualifiés de ***« dangereux »*** qui englobent notamment les contenus pornographiques mais aussi les scènes violentes, ou les discours liés à l'automutilation ou aux troubles alimentaires.

Ces réglementations ont l'avantage de cibler directement certains risques auxquels les mineurs sont particulièrement exposés. Leur mise en œuvre peut toutefois s'avérer compliquée car elles nécessitent une grande adaptabilité aux différentes plateformes dans leur rédaction mais aussi et surtout des moyens importants pour la modération des contenus (voir *infra*), qui reste largement soumise au bon vouloir des plateformes.

(2) Les réglementations adoptant une approche par les risques

D'autres textes ont une portée plus large, comme le Règlement sur les services numériques (RSN) susmentionné **qui adopte une approche fondée sur les risques** que présentent les plateformes numériques, **plutôt que selon la nature même des contenus**. La protection des mineurs en ligne figure parmi les objectifs principaux du texte et a fait spécifiquement l'objet de lignes directrices[77] publiées par la Commission européenne en juillet 2025. Elles établissent une liste non exhaustive de mesures proportionnées et appropriées pour protéger les mineurs contre les risques en ligne tels que le *grooming*, l'exposition à des contenus préjudiciables, les comportements problématiques et addictifs ainsi que le cyberharcèlement et les pratiques commerciales préjudiciables. Elles recommandent également l'utilisation de méthodes d'assurance de l'âge, si elles sont précises, fiables, robustes, non intrusives et non discriminatoires.

[77] 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.

Les signaleurs de confiance jouent un rôle complémentaire à celui des régulateurs et aux plateformes. Créés par le RSN, ce statut regroupe des associations, agences gouvernementales et regroupement d'experts, lesquels sont chargés de détecter des contenus potentiellement illicites. Leurs signalements sont traités de façon prioritaires par les plateformes. Ces entités sont désignées par les coordinateurs nationaux pour les services numériques, dont l'Arcom en France. Certains ciblent spécialement la protection des mineurs, comme l'association e-Enfance / 3018[78], premier signaleur de confiance officiellement désigné en France, qui lutte contre le harcèlement et les violences numériques dont les jeunes sont victimes.

III. Face à la multiplication des dérives sur les réseaux sociaux, quel avenir numérique pour nos jeunes ?

Au début des années 2010, les réseaux sociaux étaient perçus comme les outils de la démocratie, de la liberté d'expression, du lien social et de l'émancipation. Une quinzaine d'années après, force est de constater que **les réseaux sociaux dominants**, dont le modèle économique est fondé sur la captation de l'attention et la concentration de la propriété, **se sont mus en espaces valorisant la polarisation des idées, les contenus toxiques et charriant des risques systémiques majeurs**, notamment pour les jeunes utilisateurs. **Le constat d'échec concerne aussi la régulation de ces plateformes**. À tâtons depuis quinze ans, celle-ci s'est trop longtemps focalisée sur la question de la légalité des contenus, en négligeant le rôle des algorithmes et a par ailleurs été trop confiée au bon vouloir des plateformes, par le biais d'initiatives volontaires et autres *« codes de conduite »* à la portée et à l'efficacité trop réduites. Il convient également de se demander si des espaces portant les promesses initiales sont encore possibles aujourd'hui et comment permettre leur développement.
Alors que les efforts d'encadrement se sont intensifiés en Europe ces dernières années, les risques en ligne n'ont pas décru, en particulier chez les plus jeunes utilisateurs qui se voient aujourd'hui barrer l'accès aux réseaux sociaux.

Toutefois, le contrôle de l'âge ne suffit pas à répondre à tous les enjeux et risques liés à la protection des mineurs, ni à garantir à une vie numérique apaisée pour l'ensemble des utilisateurs. Au-delà des contournements et questionnements techniques précédemment détaillés, il est important de rappeler que les mineurs doivent pouvoir trouver en ligne les outils et les moyens de s'émanciper en toute sécurité (a). Outre le contrôle de l'âge, des méthodes alternatives pour protéger les mineurs méritent d'être mises en lumière pour enrichir les débats (b). Enfin, le débat sur la protection des mineurs en ligne ne doit pas évincer les enjeux structurels que la plupart des réglementations actuelles tendent à délaisser (c).

(a) Comment renforcer les droits fondamentaux des mineurs en ligne ?

La Commission européenne rappelle dans ses lignes directrices sur l'article 28 du RSN[79] que **les mesures de protection des mineurs sur les plateformes en ligne doivent être appropriées et proportionnées aux droits des utilisateurs**, c'est-à-dire en l'espèce qu'elles ne doivent pas enfreindre l'exercice des droits des mineurs dans l'espace numérique.

[78] Pour plus d'informations : https://e-enfance.org/.
[79] 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.

(1) Miser sur l'émancipation en ligne

La Convention internationale des droits de l'enfant (CIDE) énonce les droits fondamentaux dont jouissent les mineurs et qu'ils peuvent exercer seuls dans l'espace numérique. Ces droits sont regroupés en quatre catégories par le *Child Rights International Network*[80] : (i) le droit d'accès à l'information et le droit à l'éducation, (ii) le droit à la vie privée et le droit à l'oubli, (iii) le droit à la liberté d'expression et le droit d'être entendu et (iv) le droit d'être protégé contre les abus.

> En **Australie** par exemple, la mesure d'interdiction d'accès aux moins de 16 ans a déjà fait l'objet d'un recours devant la *High Court* par des mineurs, accompagnés par le *Digital Freedom Project*, arguant une violation de leur droit d'accès aux communications politiques[81]. Cet exemple montre que les droits fondamentaux des utilisateurs sont (doivent être) centraux et rappelés.

Le droit à l'information (articles 17, 23, 24 et 28 de la CIDE) est au centre des débats, dans la mesure où il est collectivement acquis que les usages en la matière ont été bouleversés par le numérique. 49 % des mineurs disent utiliser les réseaux sociaux pour s'informer[82]. Pour ne prendre qu'un exemple, en France, HugoDécrypte est la source d'information la plus citée parmi les sondés du rapport Reuteurs[83] de 2024, devant Le Monde, Le Figaro et Libération réunis et notamment chez les mineurs. L'enjeu est alors de protéger les mineurs sans leur couper leur moyen privilégié d'accéder à l'information.

En l'état, la proposition de loi française devrait permettre aux mineurs de moins de 15 ans de continuer d'accéder aux applications d'actualités, aux messageries intégrant des canaux d'information, sans pouvoir interagir avec l'ensemble des utilisateurs.

Comme rappelé ci-dessus, **les réseaux sociaux sont historiquement des espaces de sociabilité et de socialisation fondateurs** dans un contexte où un nombre grandissant de jeunes indiquent souffrir de solitude et d'isolement. La commission de l'OMS sur les liens sociaux, montrent que les 13–29 ans sont les plus touchés par la solitude, un pourcentage encore plus élevé chez les adolescents[84]. Les espaces numériques ont en premier lieu été utilisés comme des véhicules de la liberté d'expression. Les réseaux sociaux ont aussi pu être des espaces politiques pour les jeunes face à la répression[85]. Leur force a été particulièrement démontrée lors des *« Printemps arabes »*, au cours desquels ces services encore nouveaux avaient joué un rôle de chambre d'échos amplificateur, réunissant les manifestants et diffusant leurs messages hors des frontières. Ces mouvements ont *« marqué l'entrée fracassante du politique dans l'ère numérique, révélant une vérité dérangeante : à chaque outil d'émancipation correspond son double de répression »*[86].

---

[80] Child Rights International Network, Briefing : Les droits de l'enfant à l'ère du numérique.
[81] BBC, « Teens launch High Court challenge to Australia's social media ban », novembre 2025.
[82] Fondation pour l'Enfance, Baromètre « Enfance & Numérique », 16 février 2026.
[83] Reuters, Digital News Report, 2024.
[84] OMS, *De la solitude aux liens sociaux*.
[85] *Children of Jihad: A Young American's Travels Among the Youth of the Middle East*, J. Cohen.
[86] Fondation Jean Jaurès, « Entre rues et réseaux : les printemps arabes, laboratoire d'un numérique politique », 11 septembre 2025.

Si la promesse démocratique portée par les réseaux sociaux à leurs débuts est aujourd'hui moins perceptible du fait de l'évolution de leur modèle économique, l'éviction des mineurs pourraient néanmoins les pousser à se **déporter vers d'autres services numériques, moins contrôlables**[87], **moins encadrés ou vers de nouvelles plateformes** mettant à disposition des contenus illicites. Les IA génératives connaissent ainsi une forte utilisation par de jeunes utilisateurs pour des usages personnels : 6 % des jeunes ont recours à une IA pour se confier ou demander des conseils personnels[88]. Les compagnons IA renforcent ce phénomène dans la mesure où ils sont conçus pour encourager et faciliter la simulation d'une interaction interpersonnelle ou émotionnelle, accélérant la tendance d'une anthropomorphisation accrue des *chatbots*.

L'enjeu est ici double. Bâtir, en premier lieu, des espaces numériques plus sains pour nos enfants. Des chercheurs comme Serge Tisseron insistent, en second lieu, sur la nécessité de **proposer des espaces de sociabilité alternatifs** aux réseaux sociaux comme l'ouverture des cours de récréation ou des gymnases des établissements scolaires le week-end[89], pour permettre aux adolescents de se retrouver et de prolonger leurs sociabilités hors de l'école. Cette recommandation est également partagée par la commission « Enfants et écrans ».

(2) Renforcer la protection des données personnelles

Les méthodes de contrôle de l'âge peuvent présenter des risques en matière de collecte de données personnelles selon la manière utilisée.

La collecte de données personnelles est d'autant plus problématique si des données sensibles comme les données biométriques sont collectées via des méthodes de contrôle de l'âge fondées sur la reconnaissance faciale, d'autant plus si le consentement spécifique de l'utilisateur n'est pas recueilli. Si le contrôle de l'âge repose sur la transmission d'une pièce d'identité, d'autres données que l'âge de l'utilisateur comme ses prénom(s) et nom(s), sexe, adresse, ville de naissance etc. seront transmises alors qu'elles ne sont pas nécessaires pour s'assurer qu'un utilisateur a plus d'un âge déterminé. Aussi, une telle mesure est souvent considérée comme **invasive et peu fiable** comme le montre un rapport du *Center for Democracy and Technology*[90].

La Commission européenne devrait rendre ses conclusions sur l'expérimentation de la vérification de l'âge (sans transmission de données personnelles à la plateforme) sur les sites pornographiques prochainement et ainsi déterminer si la collecte des données personnelles peut être davantage sécurisée et minimisée via cet outil européen de contrôle de l'âge.

À ce stade, la France s'inscrit dans la logique de protection européenne avec le développement de France identité, conforme à l'EUDI Wallet (mentionné *supra*). Cet outil est sécurisé puisque

[87] L'ADN, « Anne Cordier : « Avec l'interdiction des réseaux sociaux, les jeunes deviennent une population à contrôler plutôt qu'à éduquer », 13 novembre 2025.
[88] Ifop, *Les jeunes et l'IA en 2025*,novembre 2025.
[89] Le Monde, « Serge Tisseron, psychiatre : « Découvrir les réseaux sociaux après 15 ans ne protège de rien » », 7 janvier 2026.
[90] Center for Democraty and Technology, « What Kids and Parents wants: Policy Insights for Social Media Safety Features », 19 novembre 2025.

le site, sur lequel la vérification d'âge est requise, ne reçoit qu'un signal (positif ou négatif) que l'utilisateur a plus (ou moins) que le seuil d'âge nécessaire pour y accéder. Aucune information personnelle n'est transmise au service numérique.

(3) Consolider et diversifier l'éducation des mineurs

Pour que les espaces numériques restent les lieux d'émancipation, de sociabilisation et d'information, il est impératif d'accompagner davantage les mineurs dans leurs usages et de les sensibiliser aux risques auxquels ceux-ci les exposent. L'étude de l'Arcom pointant les risques auxquels les mineurs sont exposés montrent aussi que les 11-17 ans sont lucides face à ces risques et sont en **demande d'accompagnement dans leurs usages et d'une meilleure protection**[91].

Le collectif ctrl+alt+reclaim[92] parle d'un *« faux dilemme »* auquel la proposition de loi sur l'interdiction des réseaux sociaux aux moins de 15 ans les confronte, entre *« la privation d'espaces d'échange et d'apprentissage numériques ou l'exposition aux effets dévastateurs des algorithmes »*. Ces jeunes, qui estiment qu'ils sont laissés de côté dans les débats qui les concernent en premier lieu, estiment qu'*« **éduquer à l'usage critique du numérique** est une nécessité, dès l'enfance et tout au long de la vie »*.

Cette éducation doit d'abord leur permettre de **comprendre** les mécanismes des plateformes (algorithmes, collecte de données, *dark patterns etc.*) afin d'en **maîtriser** les paramètres et d'en limiter, le plus possible, les risques. Ensuite, elle doit les outiller pour adopter les bons réflexes : croiser les sources d'information, identifier les biais algorithmiques et développer un esprit critique face aux contenus. Il est aussi primordial de mieux comprendre les **options de paramétrage et de personnalisation** d'ores et déjà activables sur ces services numériques pour se protéger et bénéficier d'une expérience plus apaisée. Or, les études montrent que si les jeunes ont une conscience théorique des dangers[93], leurs pratiques restent peu adaptées aux risques (partage excessif de données personnelles, temps d'écran non régulé, repartage de fausses informations, partage de contenus choquants etc.).

Comme le déclarent le Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE) et le Comité consultatif national d'éthique numérique (CCNEN)[94], *« l'objectif à atteindre doit donc être de les accompagner afin qu'ils développent leur esprit critique et une autonomie numérique progressive. La liberté ne signifie pas l'absence de règles, mais la capacité à faire des choix éclairés concernant sa santé, en particulier mentale »*.

> Des solutions de politiques publiques intégrées sont déjà mises en place comme en **Finlande** où le programme *Media Literacy for All*[95] forme les élèves dès 7 ans à décrypter les médias numériques, avec des résultats mesurables sur leur résilience

[91] Arcom, « Protection des mineurs : quels risques ? Quelles protections ? », 25 septembre 2025.
[92] Le Monde, « Interdiction des réseaux sociaux aux moins de 15 ans : « La voix des jeunes est absente du débat sur la régulation du numérique », 25 janvier 2026.
[93] Arcom, « Protection des mineurs : quels risques ? Quelles protections ? », 25 septembre 2025.
[94] Déclaration commune CCNE et CCNEN, « Les jeunes face aux réseaux sociaux numériques : le questionnement éthique face à une menace confirmée », février 2026.
[95] Voici la Finlande, « La Finlande promeut l'éducation aux médias en tant que compétence civique », 2023.

face à la désinformation. Cette initiative est couplée à un travail de fond sur le développement de l'esprit critique des futurs citoyens finlandais dès les enseignements primaire et secondaire, où l'on apprend aux enfants les mécanismes de la propagande, que les statistiques sont manipulables ou encore qu'une œuvre d'art peut véhiculer des messages contradictoires.

La France avance peu à peu dans cette voie. L'éducation aux médias et à l'information fait partie des programmes scolaires nationaux. Le CLEMI (Centre pour l'éducation aux médias et à l'information) est notamment chargé en France de l'éducation aux médias et à l'information dans l'ensemble du système éducatif. Toutefois, ces seuls dispositifs ne suffisent pas à développer un système immunitaire et critique numérique robuste.

(b) Des réflexions alternatives et complémentaires

Certains pays, certaines plateformes, proposent des méthodes alternatives et complémentaires au contrôle de l'âge : vérification de l'âge au niveau du terminal (1), plages horaires de déconnexion imposée (2), interfaces numériques sécurisées (3).

(1) Les limites de temps : plages horaires de déconnexion imposée

Certaines législations prévoient des plages horaires de déconnexion imposée pour réduire l'exposition et diminuer les comportements addictogènes qui peuvent avoir des conséquences sur les mineurs. Une telle mesure nécessite de passer par un contrôle de l'âge, quel que soit la méthode retenue.

Cette technique n'est pas nouvelle et a, par exemple, été mise en œuvre en **Corée du Sud**[96] entre 2011 et 2021, sur une plage horaire de minuit à 6 heures du matin. La mesure a été levée en raison de son périmètre trop étroit qui visait uniquement les jeux en ligne. Une mesure similaire est actuellement en vigueur en **Chine** avec un *« mode mineur »*[97] bloquant l'accès entre 22 heures et 6 heures et l'instauration d'une limite de temps en fonction de leur tranche d'âge pour certains services numériques (voir *supra*).

Dans l'État de **Californie**, le « *Protecting Our Kids from Social Media Addiction Act* » (loi de protection des enfants contre l'addiction aux réseaux sociaux) de 2024, **interdit par défaut les *« flux addictifs »* pour les mineurs**, sauf autorisation parentale et instaure une **limite de temps par défaut fixée à une heure par jour**, modifiable par les parents. Ces mesures sont en vigueur depuis février 2025 malgré

[96] Youth Protection Revision Act, mai 2011.
[97] Pour plus d'informations, voir par exemple : France Inter, « "Réduire la dépendance" aux écrans : la Chine veut drastiquement limiter l'accès des jeunes à Internet », 3 août 2023.

le recours d'une association représentante des intérêts des plateformes, à la suite duquel un juge fédéral a partiellement dispensé les plateformes d'autres restrictions prévues dans le texte[98]. Une mesure similaire dans l'**Utah** introduite en mars 2023 a été rejetée en septembre 2024 car jugée contraire au premier amendement de la Constitution américaine. Un appel de cette décision a été formé.

La proposition de loi française initiale visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux contenait une mesure de couvre-feu numérique mais cette disposition a finalement été retirée avant son examen à l'Assemblée nationale le 26 janvier 2026.

Les exemples montrent que la limitation du temps d'écran des mineurs peut être appliquée soit strictement avec une interdiction ferme pendant une plage horaire définie par l'État, soit de manière plus souple, avec un paramétrage protecteur par défaut mais modulable par les utilisateurs ou leurs parents. Le rapport du *Center for Democracy and Technology*[99] précité considère **les mesures de couvre-feu strict comme trop intrusives et peu pratiques**, suggérant plus de flexibilité dans les fonctionnalités de temps d'écran. Certes, la conception des interfaces et les mécanismes addictogènes mis en place par les intermédiaires numériques tendent à prolonger le temps passé en ligne (les mineurs restants parfois éveillés la nuit), avec des effets de bord sur d'autres activités indispensables au développement des enfants et adolescents, à commencer par le sommeil, l'activité physique et la vue. Toutefois, **le temps passé en ligne ne dit rien des pratiques et des contenus visionnés**[100]. **La responsabilité revient avant toute chose aux plateformes** et de telles mesures pointent surtout les usages des jeunes. D'autre part, les plateformes numériques sont aussi le support d'apprentissages et de découvertes offrant un accès à des ressources éducatives, culturelles et/ou créatives[101]. Il est donc essentiel de distinguer l'usage passif, souvent critiqué, de l'usage actif et constructif, qui peut enrichir les compétences et les connaissances des utilisateurs, à condition d'être accompagné et d'utiliser des outils adaptés à chaque âge.

(2) Les interfaces numériques sécurisées et paramétrables

La protection des mineurs peut également passer par des interfaces dédiées, adaptées à leur âge et moins addictogènes et sur le filtrage des contenus nocifs. Ces mesures revêtent une importance capitale pour garantir que les mineurs, lorsqu'ils accèdent à ces services, évoluent dans des environnements numériques sécurisés. Ces adaptations peuvent être mises en place soit volontairement par les plateformes, sans succès probant jusqu'à maintenant, soit sous l'impulsion du législateur. Les dispositifs de contrôle de l'âge analysés précédemment,

[98] Appeal from the United States District Court for the Northern District of California Edward J. Davila, District Judge, Presiding, 9 septembre 2025.
[99] Center for Democracy and Technology, « What Kids and Parents wants: Policy Insights for Social Media Safety Features », 19 novembre2025.
[100] Le Monde, « Usages du numérique : « La question du temps d'écran, c'est le degré zéro de l'analyse » », 9 février 2021.
[101] Dominique Pasquier, Quentin Gilliote, « Apprendre par la bande : que nous apprennent (vraiment) les youtubeurs ? », 19 octobre 2023.

constituent souvent une condition préalable à l'activation de ces fonctionnalités ou interfaces adaptées.

Les lignes directrices de la Commission européenne sur l'article 28 du RSN[102] prévoient des mesures destinées à encadrer les fonctionnalités addictogènes des plateformes, afin de limiter leurs effets sur les mineurs. Les notifications doivent être désactivées par défaut, en particulier pendant les plages horaires de sommeil. Les fonctionnalités d'IA, telles que les agents conversationnels intégrés aux plateformes, ne doivent pas être activées par défaut. Par ailleurs, les mineurs ne doivent faire l'objet d'aucune incitation à les utiliser. Il serait souhaitable que de telles mesures protectrices instaurées par défaut soient pensées pour l'ensemble des utilisateurs.

> Aux **Pays-Bas**, un tribunal a ordonné à Meta de proposer par défaut un **fil d'actualité chronologique**, c'est-à-dire avec la présentation des publications dans l'ordre où elles sont postées et non plus selon un classement algorithmique. L'obligation de proposer un fil alternatif figure dans le RSN. Cette décision vient la compléter pour demander de l'activer par défaut. Cette mesure concerne tous les comptes utilisateurs et pas seulement les mineurs. Meta a fait appel de cette décision qui est donc suspendue jusqu'au prochain jugement.

Chez Meta, les réseaux sociaux Instagram, Facebook et Messenger font l'expérience des ***« comptes adolescents »*** dédiés aux 13-17 ans qui comportent des paramètres de protection pour les jeunes utilisateurs, qui limitent notamment *« le contenu inapproprié et les contacts indésirables »*[103]. L'activation du compte en mode *« adolescent »* est automatique, les paramètres sont installés par défaut et ne sont modifiables qu'avec accord parental pour les moins de 16 ans. Après un essai aux États-Unis, au Royaume-Uni, en Australie et au Canada, l'entreprise va généraliser ce mode aux pays du monde entier.

Plusieurs facteurs doivent être pris en compte. Tout d'abord, s'il revient **aux plateformes elles-mêmes de mettre en place des mesures de modération, de filtrage des contenus ou de paramétrage**, ces objectifs peuvent entrer en contradiction avec leur modèle économique et conduire à des mesures déceptives. Les montants d'amendes auxquelles les très grandes plateformes s'exposent représentent souvent une part très faible de leur chiffre d'affaires, ce qui n'est pas toujours dissuasif pour qu'elles intègrent ces fonctionnalités. Aussi, l'application des mesures d'adaptation de contenu nécessite que les plateformes disposent – et consacrent – de capacités techniques et humaines suffisantes, notamment dans le cas de plus petits acteurs numériques. Enfin, si ces options de paramétrage ne sont pas activées par défaut, il peut être nécessaire pour les utilisateurs mineurs d'être accompagnés dans l'activation des options disponibles.

Au-delà des fonctionnalités pouvant exister sur les plateformes majoritairement utilisées, des services numériques alternatifs aux réseaux sociaux dominants existent comme Mastodon,

[102] 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.

[103] AFP, « Les "comptes adolescents" Facebook et Messenger déployés dans le monde entier », 29 septembre 2025.

réseau social décentralisé et fédéré, ou Bluesky, un réseau social offrant une expérience similaire mais fondé sur le paramétrage utilisateur et sur la modération humaine. Ces alternatives portent la promesse d'une expérience en ligne plus saine : des conceptions moins addictives et nocives pour l'utilisateur, davantage de capacités de modération humaine, un meilleur respect des données personnelles *etc*.

De façon plus prospective, W social[104], futur réseau social européen conçu par Anna Zeiter, ancienne vice-présidente en charge de la confidentialité, de l'intelligence artificielle et de la responsabilité des données chez eBay, promet une interface plus saine et moins toxique, le respect des données personnelles des utilisateurs, une stricte vérification de l'âge, de la modération humaine (et non algorithmique) et des algorithmes paramétrables pour échapper à l'enfermement.

Ces alternatives permettent de redonner à l'utilisateur le choix, à la fois dans le service numérique qu'il souhaite utiliser et dans les paramètres qu'il souhaite activer : contrôle des recommandations, protection de ses données etc.

Pourtant, la migration vers ces alternatives reste un parcours semé d'embûches. Tout d'abord, de nombreuses barrières techniques à la sortie, rendent la migration et l'effectivité du droit à la portabilité des données complexes, sans solution universalisée, contrairement aux télécoms par exemple (il est possible à chacun de conserver son numéro de téléphone lors d'un changement d'opérateur, opérateur qui assure l'intégralité de la migration). Aussi, l'effet de réseau est certain : les GAFAM ont construit des monopoles créant une dépendance systémique. Il peut paraître difficile de quitter un réseau social pour migrer vers un autre du fait de possibles perte d'audience, de communautés, de *« capital social numérique »*.

C'est ainsi que des outils et des mouvements émergent pour faciliter cette transition. Le mouvement HelloQuitteX a par exemple outillé 13,4 % des utilisateurs[105] de X qui ont migré en quelques mois vers Bluesky. OpenPortability[106] a été développé par le mouvement comme solution pour faciliter la migration, en s'appuyant sur le droit à la portabilité, permettant aux utilisateurs de récupérer leurs données et de les transférer vers Bluesky ou Mastodon.

Il est toutefois à noter que les alternatives vertueuses ne sont pas imperméables aux dérives structurelles. Bluesky a par exemple été critiqué pour ses *« listes de modération »*[107] qui permettent à un utilisateur de créer une liste dans laquelle il bloque ou masque certains comptes et aux autres utilisateurs de s'y abonner pour filtrer les contenus. Mastodon, malgré son modèle décentralisé, peine quant à lui à modérer efficacement les contenus haineux à grande échelle[108]. Ces solutions doivent davantage être vues comme des espaces de réappropriation. Elles montrent qu'il est possible de proposer des alternatives aux modèles dominants.

(c) Pistes de réflexions et chantiers prioritaires

Les réglementations fondées sur le contrôle de l'âge pour restreindre l'accès aux services numériques pour les mineurs ne règlent qu'une partie du problème, alors que **les causes**

[104] France Culture, « Le réseau européen "W social" pensé comme un "anti X" a-t-il une chance d'exister ? », 29 janvier 2026.
[105] HelloQuitteX : on fait le bilan.
[106] https://openportability.org/fr/auth/signin.
[107] France Inter, « Bluesky : les lites de modération font polémique », 2 décembre 2024.
[108] BFM, « Sécurité, modération, prise en main : ces points faibles de Mastodon, l'alternative à Twitter », 12 novembre 2022.

structurelles des risques engendrés par les réseaux sociaux, dans leur fonctionnement actuel, demeurent inchangées. Face aux angles morts des régulations actuelles, les chantiers prioritaires suivants visent à harmoniser le cadre de protection des mineurs en ligne au niveau européen, au risque – autrement – de rendre vains les efforts des États membres ; à porter des réformes structurantes sur le cadre de régulation européen des plateformes ; et à élargir le champ des réflexions sur les pratiques en ligne des plus jeunes et l'accompagnement à l'utilisation des services numériques pour permettre – sur le moyen terme – des usages plus sûrs et positifs.

*

Chantier n° 1 : Créer un standard européen de protection des mineurs en ligne

La protection des mineurs en ligne doit impérativement être portée à l'échelle européenne, marché de plus d'un demi-milliard d'utilisateurs de réseaux sociaux, pour des résultats probants.

Par son rôle pionnier, **la France pourrait jouer un rôle moteur à l'échelle européenne et œuvrer en faveur d'un standard partagé de protection des mineurs en ligne**, incluant des exigences harmonisées en matière de conception des services, de système de vérification de l'âge sécurisé et protecteur des données personnelles, de gouvernance des risques et associant les signaleurs de confiance désignés dont l'action est essentielle. Un tel cadre de référence sera enrichi dans les prochains mois par les travaux conduits en matière d'identité numérique européenne, gagnerait en pouvoir de prescription vis-à-vis des grandes plateformes numériques, afin de produire un effet structurel sur l'ensemble du marché.

Dans cette optique, la France pourrait utilement se rapprocher des autorités irlandaises et lituaniennes dans la perspective de leurs présidences respectives de l'Union Européenne, à compter du semestre prochain pour Dublin. L'Irlande a par ailleurs laissé entendre que le sujet de l'âge minimum requis pour accéder aux réseaux sociaux pourrait être inscrit à l'agenda de sa présidence européenne[109].

*

Chantier n° 2 : Ouvrir les fonctionnalités des plateformes, consacrer un droit au paramétrage et renforcer la transparence des algorithmes

Les mesures de protection renforcée ciblées sur les mineurs ne s'attaquent pas à la source des externalités sociales négatives induites par les plateformes, à savoir le modèle économique de ces acteurs. Une régulation systémique des plateformes apparaît aujourd'hui plus que nécessaire. Leur modèle économique repose sur la captation de l'attention des utilisateurs, un engagement permanent et une exposition constante – y compris aux contenus les plus toxiques[110] – afin de maximiser le temps d'écran et, *in fine*, les revenus publicitaires. Les

[109] Toute l'Europe.eu, « Mineurs et réseaux sociaux : quels pays européens comptent imposer un âge minimum ? », 26 février 2026.
[110] Voir à ce propos : CNNum, « Votre attention s'il vous plait ! Quels leviers face à l'économie de l'attention ? », janvier 2022.

plateformes exploitent les données personnelles des utilisateurs, intègrent des *dark patterns*[111] (interfaces trompeuses) dans leurs interfaces et déploient des algorithmes opaques et de plus en plus enfermant, malgré les obligations de transparence.

Comme le souligne l'Anses[112], ces algorithmes créent *« un "**effet spirale**", enfermant les jeunes dans des contenus de plus en plus ciblés, parfois extrêmes »*, en exploitant leurs biais cognitifs et leurs données comportementales. Parallèlement, les plateformes diversifient leurs sources de revenus : vente de données personnelles à des annonceurs, publicités ultraciblées, abonnements payants, monétisation des contenus générés par les utilisateurs, un modèle qui invite à la surenchère et favorise la production de contenus choquants ou clivants.

En Espagne par exemple, le Premier ministre Pedro Sanchez a annoncé vouloir s'attaquer à ces enjeux systémiques en allant au-delà de l'interdiction des réseaux sociaux envisagée pour les moins de 16 ans[113]. Parmi ses priorités : faire de *« la manipulation et (de) l'amplification algorithmique de contenus illégaux »* une *« infraction pénale »*.

Bien évidemment, ces risques ne concernent pas uniquement les mineurs, mais bien l'ensemble des utilisateurs de ces services numériques. Or, les mesures actuelles ciblées sur les mineurs présentent le risque, **par effet pervers, de débrider les espaces numériques**[114] **pour les autres utilisateurs**. Il est impératif d'éviter que la protection des mineurs ne serve de paravent à une dérégulation généralisée.

Indépendamment du contrôle de l'âge, des solutions complémentaires méritent d'être promues pour permettre à toutes et tous d'avoir davantage de choix et de contrôle sur son expérience en ligne, dans la continuité notamment des propositions formulées par les États généraux de l'information[115] et par la Commission d'enquête sur les effets psychologiques de TikTok sur les mineurs[116]. La priorité doit rester l'émergence de solutions en adéquation avec les valeurs européennes, la régulation et l'interdiction ne relevant que des mesures correctives. Parmi elles :

- Le **pluralisme algorithmique**, pour permettre aux utilisateurs de choisir comment les algorithmes sélectionnent et affichent les contenus et paramétrer leurs interfaces et ainsi de trouver davantage de diversité dans les contenus qui leur sont proposés tout en se prémunissant des contenus nocifs[117]. Par exemple, des options de filtrage renforcé, des algorithmes conçus par des tiers pour privilégier des contenus éducatifs ou adaptés à l'âge, ou encore des interfaces simplifiées et transparentes, pourraient limiter l'exposition à la désinformation, aux discours haineux ou aux contenus promotionnels de comportements à risque (comme les défis dangereux ou les troubles alimentaires). En outre, l'ouverture à des services tiers de modération, labellisés et

[111] Défini par Designers éthiques 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 ».
[112] Le Monde, « L'Anses alerte sur les risques des réseaux sociaux sur la santé des adolescents », 13 janvier 2026.
[113] Le Monde, « L'Espagne compte interdire à son tour les réseaux sociaux aux moins de 16 ans », 4 février 2026.
[114] Hubert Guillaud, « Vérification d'âge (2/4) : de l'impunité des géants à la criminalisation des usagers », 4 décembre 2025.
[115] Rapport des Etats généraux de l'information, Protéger et développer le droit à l'information : une urgence démocratique,12 septembre 2024. Recommandation n°1 du groupe de travail sur l'espace informationnel et les innovations technologiques.
[116] Assemblée nationale, Rapport fait au nom de la Commission d'enquête sur les effets psychologiques de TikTok sur les mineurs, septembre 2025. Recommandation n° 12.
[117] Le Monde, « Pour le pluralisme algorithmique ! », 25 septembre 2024.

contrôlés, permettrait de proposer des environnements numériques plus sûrs, où les règles de protection des mineurs seraient prioritaires et adaptables selon les besoins spécifiques de l'utilisateur. Certaines plateformes, comme Bluesky, expérimentent déjà des systèmes où les utilisateurs personnalisent leurs flux et leur modération. **Les pouvoirs publics pourraient encourager plus largement l'émergence d'offres algorithmiques alternatives**.

- Un **droit au paramétrage par défaut pour l'utilisateur mineur**, accompagné par un adulte, afin de définir conjointement les intérêts du mineur dans ses interactions sur les services numériques : *« Ce paramétrage pourrait concerner le niveau de notification, la détermination de la sphère d'émission des contenus qu'il publie ou encore sa sphère de réception donc ce qu'il verra apparaître comme contenus recommandés, comme ceci a été proposé dans le cadre des travaux de la CNCDH sur la haine en ligne. »*[118] Sans sur-responsabiliser l'utilisateur, *« le droit au paramétrage permettrait de penser une route alternative pour mettre les individus en posture de réflexion, favoriserait la prise de recul de l'utilisateur sur son comportement et ses usages et lui permettrait de réfléchir sur ses automatismes »*[119]. L'activation de ce paramétrage doit être pensée dans une interface simple d'accès et d'utilisation pour éviter toute fatigue décisionnelle face à la multiplicité de choix qui aboutirait systématiquement à conserver le paramétrage par défaut. En outre, par défaut, les fonctionnalités devraient être paramétrées de façon la plus neutre possible (désactivation des notifications, présentation des contenus par ordre chronologique etc.).

- Une **transparence renforcée des systèmes de recommandation et de modération** pour contraindre les plateformes à expliciter, de manière intelligible, leurs choix et critères de classement des contenus et à proposer des alternatives moins addictives. Le RSN impose déjà, via ses articles 14, 15 et 27, une information sur les outils de modération, la publication de rapports de transparence annuels et une explication des principaux paramètres des algorithmes de recommandation. Toutefois, ces obligations produisent aujourd'hui des rapports techniques, peu lisibles pour le grand public et ne permettent pas d'accéder à une compréhension fine des logiques économiques et attentionnelles qui structurent les systèmes. Il est donc nécessaire d'aller plus loin en exigeant des formats standardisés, intelligibles, synthétiques et comparables et en ouvrant davantage l'accès aux données pour les chercheurs et les autorités indépendantes.

- La promotion de **standards ouverts** dans les réseaux sociaux est un préalable indispensable au pluralisme algorithmique. Ce sont ces standards qui forment le socle rendant possible la portabilité des comptes (conservation de l'identité et contacts en changeant de plateformes), l'interopérabilité des solutions (échanger entre plusieurs réseaux, brancher des services tiers, choisir d'autres systèmes de recommandation) et la possibilité de proposer une pluralité d'options algorithmiques.

*

[118] Pour plus d'informations à ce propos voir CNNum, « Vers la consécration d'un droit au paramétrage ? Échange avec Célia Zolynski », 22 mai 2024.
[119] *Ibid.*

Chantier n° 3 : Repenser la dichotomie hébergeur/éditeur

Certains pays au sein de l'UE tendent à renforcer le régime de responsabilité s'appliquant aux plateformes en ligne s'agissant des mineurs. Par exemple, la proposition de loi française, telle qu'adoptée à l'Assemblée nationale, introduit un renversement majeur en proposant de redéfinir le statut des plateformes lorsqu'elles *« suggèrent ou hiérarchisent, au moyen d'un système de recommandation, des informations fournies par des destinataires du service »*[120]. Dans un tel cas et s'agissant de ces informations, les plateformes seraient considérées comme des éditeurs.

Traditionnellement, les réseaux sociaux bénéficient, au titre de la directive e-commerce, d'un régime de responsabilité allégée en tant qu'hébergeurs[121], n'étant tenus responsables des contenus publiés par leurs utilisateurs qu'à condition de ne pas en avoir eu une connaissance effective ou de ne pas avoir agi promptement pour les retirer. À l'inverse, l'éditeur, qui détermine et maîtrise les contenus est soumis à une responsabilité civile et pénale renforcée.

Toutefois, la montée en puissance des grandes plateformes qui organisent, recommandent et monétisent les contenus a révélé les limites de ce régime de responsabilité asymétrique. Selon l'Avocat général de l'affaire dite *« AGCOM »* de la Cour de justice de l'UE, « *la dichotomie du rôle passif ou actif semble insuffisante pour tenir compte des activités exercées par un tel prestataire, en particulier dans un domaine en constante évolution »*[122]. Des raisonnements similaires ont également été émis par l'Avocat général dans la récente décision *« Coyote System »*[123]. Il souligne que la plateforme d'aide à la conduite routière Coyote ne se contente pas de transmettre des informations fournies par ses utilisateurs, mais en exerce un contrôle actif. Il ne peut donc pas bénéficier du statut d'hébergeur, qui limite normalement la responsabilité des plateformes. Si la Cour de Justice valide cette analyse, cela pourrait marquer un tournant majeur dans la responsabilité des plateformes, en tant que concepteurs et programmeurs d'algorithmes.

Depuis une dizaine d'années, ces réflexions autour de la consécration d'un statut intermédiaire entre éditeur et hébergeur se multiplient face à l'inadaptation du critère de *« rôle techniquement neutre »*, retenu par la loi française de transposition[124], pour distinguer les hébergeurs des éditeurs.

Le Conseil d'État, dans son étude annuelle de 2014[125], recommandait déjà de dépasser la dualité éditeur/hébergeur pour consacrer un **statut de *« plateforme »***, assorti d'obligations renforcées. Une résolution du Sénat[126] en 2018 appelait également à définir au niveau européen un ***« troisième statut »***, *« une catégorie intermédiaire […] dite d'**« éditeur de services en ligne »** »*, s'alignant sur un rapport de 2014 du Conseil supérieur de la propriété littéraire et artistique. Ces anciennes propositions sont en partie relayées dans le RSN qui, sans créer formellement de troisième statut, distingue au sein des hébergeurs les plateformes en ligne et notamment

[120] Article 1er bis (nouveau), Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, adopté par l'Assemblée nationale en première lecture le 26 janvier 2026.
[121] Article 6-I-2 LCEN, loi qui transpose la directive e-commerce.
[122] Conclusions de l'avocat général SZPUNAR, présentées le 27 novembre 2025 dans l'affaire C-421/24 dite AGCOM.
[123] InfoCuria - Cour de justice de l'Union européenne
[124] Loi du 21 juin 2004 pour la confiance dans l'économie numérique.
[125] Conseil d'État, *Le numérique et les droits fondamentaux* , 8 septembre 2014.
[126] Sénat, *Proposition de résolution européenne n° 739*, 27 septembre 2018.

les très grandes plateformes et très grands moteurs de recherches pour leur imposer un régime de responsabilité plus exigent, notamment en termes de modération.

Repenser le statut de ces acteurs permettrait de passer à une logique de responsabilité partagée – par exemple en cas de diffusion de contenus illicites (cyberharcèlement, incitation à la haine etc.) – laquelle apparaît essentielle alors que les plateformes se rangent souvent derrière leur statut d'hébergeurs pour échapper aux obligations renforcées.

Une telle réforme ne peut être pensée qu'à l'échelle européenne. La révision du RSN prévue en 2027 pourrait constituer le moment opportun pour introduire cette modification. Dans cette perspective, la France peut être motrice de travaux préparatoires en coordination avec les États membres engagés dans des réflexions similaires comme l'Espagne, voire la Grèce, qui assurera la présidence de l'UE au second semestre 2027.

*

Chantier n° 4 : Considérer les usages pluriels des services numériques, en particulier ceux qui relèvent de l'IA générative

La protection des mineurs tend à se concentrer sur les réseaux sociaux. Or, les usages numériques se diversifient[127], en particulier chez les jeunes usagers : jeux en ligne, messageries privées, plateformes collaboratives, assistants vocaux *etc.* Ces usages sont également vecteurs de risques.

L'irruption de l'IA générative crée de nouvelles vulnérabilités. 59 % des 12–17 ans utilisent déjà une IA générative, un chiffre au-dessus de la moyenne de la population, qui atteint 48 %[128]. En juillet 2025, 206 applications de compagnonnage par IA étaient disponibles sur l'App Store et 253 sur Google Play – toutes comptabilisaient des centaines de millions de téléchargements. Replika, l'un des leaders de l'*« intimité artificielle »*, compte plus de 10 millions d'utilisateurs. Les fêtes de fin d'année 2025 ont vu fleurir des jouets intégrant de l'IA[129] et les compagnons IA sont de plus en plus intégrés aux réseaux sociaux (comme My AI sur Snapchat, Meta AI sur WhatsApp, Grok sur X etc.)

Ces outils, conçus pour maximiser l'engagement des utilisateurs, peuvent créer une dépendance affective et se substituer aux relations humaines essentielles à la construction psychique des plus jeunes, tout en captant leurs données personnelles à des fins commerciales. Les modèles sous-jacents, souvent opaques et non adaptés aux mineurs, risquent de manipuler leurs décisions, d'encourager des comportements dangereux[130] et de les exposer à des contenus inappropriés, voire illicites.

[127] Étude menée par l'Institut GWI pour le *Financial Times* dans plus de 50 pays auprès de 250 000 personnes.
[128] Arcom, Baromètre du numérique 2026.
[129] Voir à ce propos : CNNum, « Votre attention s'il vous plait ! Quels leviers face à l'économie de l'attention ? », janvier 2022.
[130] BBC, « 'A predator in your home': Mothers say chatbots encouraged their sons to kill themselves », 8 novembre 2025.

Afin de ne pas reproduire les erreurs commises vis-à-vis des réseaux sociaux, les pouvoirs publics doivent se saisir dès maintenant de la question de ces « nouveaux » usages et des vulnérabilités qu'ils pourraient générer chez les utilisateurs, en particulier chez les plus jeunes d'entre eux.

Dans ce cadre, **le Conseil de l'IA et du numérique pilotera la commission *« IA générative et vulnérabilités »*[131], à la demande de la ministre déléguée chargée de l'IA et du Numérique, dans le but de cibler les principaux risques afférents aux usages** et élaborer des recommandations concrètes à destination des pouvoirs publics. Les premières conclusions des travaux seront rendues publiques **d'ici la fin du mois de mai 2026**. Le rapport définitif sera remis au mois de septembre 2026.

*

Chantier n° 5 : Renforcer et structurer l'éducation au numérique, aux médias et à l'information

Face aux outils numériques pluriels et aux risques multiples auxquels ils exposent les mineurs, il est indispensable de renforcer l'esprit critique des utilisateurs, dès le plus jeune âge. Pour leur permettre de reprendre le contrôle sur leurs usages numériques **l'éducation au numérique, aux médias et à l'information (EMI) doit devenir un réel pilier des parcours scolaires**, à l'instar du modèle finlandais[132]. Il est également primordial de revaloriser les pratiques de socialisation en dehors de l'espace numérique.

Cette éducation au numérique doit être instaurée dès le plus jeune âge, du primaire aux études secondaires. Des dispositifs existent d'ores et déjà. On peut par exemple citer la Charte pour l'éducation à la culture et à la citoyenneté numériques[133] qui rappelle la nécessité d'une formation explicite aux droits et devoirs numériques, à la protection des données personnelles et à la lutte contre la désinformation. Le Cadre d'usage de l'IA en éducation recommande également de former à l'EMI dans les séquences pédagogiques intégrant l'IA générative[134]. Au niveau européen, les Lignes directrices pour les enseignants et les éducateurs en matière de lutte contre la désinformation et de promotion de la littératie numérique[135], mises à jour en 2026 dans la continuité du Plan d'action pour l'éducation numérique 2021-2027 préconisent de renforcer la place de la littératie numérique dans les curricula, la formation des enseignants et les projets d'établissement. L'UE insiste sur la nécessité de politiques scolaires pour soutenir les enseignants (temps, ressources, formation) et pour intégrer ces enjeux de manière cohérente dans l'ensemble de la vie scolaire. La circulaire française du 10 juillet 2025 visant à promouvoir un numérique raisonné à l'École[136] traduit ces orientations en mesures concrètes, via l'intégration évaluée de l'EMI dans les apprentissages. Sur la base du Cadre de référence des compétences numériques (CRCN), l'apprentissage de ces compétences doit être évalué

[131] CIANum, « Le Conseil de l'intelligence artificielle et du numérique chargé de constituer une commission « IA générative et vulnérabilités »», 27 février 2026.
[132] This is FINLAND, « La Finlande promeut l'éducation aux médias en tant que compétence civique », 2023.
[133] Ministère de l'Éducation nationale, « Charte pour l'éducation à la culture et à la citoyenneté numériques ».
[134] Ministère de l'Éducation nationale, « Cadre d'usage de l'IA en éducation », juin 2025.
[135] European Union, « Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training », 2026.
[136] Circulaire visant à promouvoir un numérique raisonné à l'École, 10 juillet 2025.

via la plateforme Pix. La circulaire souligne que dans le cadre de l'EMI *« les équipes éducatives contribuent à la formation des élèves aux droits et aux devoirs liés à l'usage d'Internet et des réseaux sociaux. Elles sensibilisent les élèves à un usage éthique et réfléchi des outils numériques et participent au développement de compétences numériques des élèves, en complément de la mise en œuvre des enseignements dédiés à la technologie et à l'informatique. »*

Malgré ces textes, l'EMI reste insuffisante en classe par manque de temps et de moyens. Celle-ci doit faire l'objet d'un programme scolaire structuré en adaptant les apprentissages à l'âge des élèves et leurs usages, sur le modèle du programme dédié à l'éducation à la vie affective, relationnelle et sexuelle paru en 2025[137]. À l'échelle européenne, un socle commun pourrait fixer des objectifs minimaux en termes de nombres d'heures, de compétences à acquérir, que chaque État membre intégrerait dans ses programmes scolaires. Ce programme doit s'accompagner d'un financement dédié pour garantir l'effectivité de la mesure.

Cette politique doit également aller de pair avec un plan de **formation des adultes entourant les jeunes** (familles, professionnels, enseignants, aidants etc.), via des outils pédagogiques adaptés, afin de favoriser un dialogue continu adulte-enfant sur les pratiques numériques. Plusieurs acteurs proposent déjà des outils en ce sens, comme les fiches dédiées aux parents et aux équipes pédagogiques produites par Internet Sans Crainte[138]. Ces enjeux s'inscrivent très directement en lien avec le **besoin d'accroître l'ampleur et la portée des initiatives en matière d'inclusion et de médiation numériques, en particulier dans les territoires**, à l'heure où les moyens alloués en la matière ne cessent d'être réduits.

Enfin, l'éducation doit être complétée par des politiques locales valorisant les espaces non numériques, comme des espaces de socialisation, des ateliers, de dialogue, d'information, des projets de participation civique, pour offrir aux jeunes des expériences collectives en dehors des plateformes en ligne. De nombreuses alternatives de politiques publiques sont d'ores et déjà proposées, il s'agit de les valoriser pour une meilleure diffusion auprès des publics concernés.

[137] Ministère de l'Education nationale, « Un programme ambitieux : éduquer à la vie affective et relationnelle et à la sexualité », février 2025.
[138] Pour plus d'informations : Internet Sans Crainte, « Vous êtes parents – Nos ressources et des événements pour accompagner les pratiques numériques de vos enfants ».