Contribution relative à la notification 2026/0185/FR (France) - Proposition de loi visant à protéger les mineurs des risques liés à l'usage des réseaux sociaux

La proposition de loi notifiée sous la référence 2026/0185/FR soulève des difficultés substantielles au regard du droit primaire et dérivé de l'Union, mais aussi au regard de la trajectoire d'harmonisation technique actuellement engagée au niveau européen pour la protection des mineurs en ligne.

Au-delà de la seule question du seuil d'âge, le texte français repose sur un modèle de vérification d'âge et de contrôle de l'autorité parentale qui, en l'état des infrastructures disponibles, conduit à une collecte massive de données par des acteurs privés, sans solution publique européenne robuste et largement déployée, et sans examen sérieux des exigences de nécessité et de proportionnalité.

1. Nécessité d'un cadre technique européen harmonisé, piloté par les pouvoirs publics

Les travaux en cours au sein de l'Union sur la sécurité des enfants en ligne et l'harmonisation de la majorité numérique visent précisément à définir un socle commun de solutions techniques d'identification et d'authentification, compatible avec le DSA, le RGPD et le futur cadre européen d'identité numérique.

Dans ce contexte, la proposition française anticipe et contourne ces travaux en imposant, de manière unilatérale, des obligations de vérification d'âge dont la mise en œuvre pratique ne peut aujourd'hui reposer que sur des solutions privées, hétérogènes et difficilement auditables, faute d'un cadre européen opérationnel pour des « jetons » d'âge et d'autorité parentale délivrés et gouvernés par des entités publiques.

Les propres débats nationaux ont montré que ni l'autorité de régulation, ni les fournisseurs de services ne disposent, à ce stade, d'un dispositif de vérification d'âge fiable, interopérable et respectueux des droits fondamentaux, reposant sur une identité numérique publique largement diffusée au sein de la population.

Au contraire, le texte délègue de facto à chaque plateforme la charge de concevoir ou d'intégrer des solutions de vérification d'âge ad hoc, alors même qu'il serait plus conforme à l'intégrité du marché intérieur et à la logique d'harmonisation du DSA de développer, au niveau européen, une infrastructure technique commune, gérée par des autorités publiques (ou par des opérateurs agréés et strictement encadrés) et ensuite utilisable de manière uniforme par l'ensemble des services en ligne.

Une telle infrastructure harmonisée, adossée à des outils d'identité numérique et à des systèmes de « jetons » anonymisés, permettrait d'éviter la multiplication de dispositifs nationaux ou privés incompatibles, tout en limitant drastiquement la circulation et la duplication de données d'état civil entre les mains des plateformes.

2. Non-respect du principe de proportionnalité

Au plan des droits fondamentaux, la proposition de loi opère une restriction massive et indifférenciée de l'accès des mineurs à l'espace numérique, qui ne résiste pas à l'examen du triple test de proportionnalité (adéquation, nécessité, proportionnalité stricto sensu).

D'abord, l'adéquation de la mesure est discutable : le texte vise principalement l'accès des mineurs aux services, alors que les risques identifiés tiennent avant tout aux modèles économiques et à l'architecture algorithmique des plateformes, c'est-à-dire à la manière dont les contenus sont hiérarchisés, recommandés et rendus addictifs.

Ensuite, la nécessité n'est pas démontrée : des alternatives moins attentatoires aux droits fondamentaux existent, consistant à cibler les services effectivement « susceptibles de nuire » à l'épanouissement des mineurs (via une liste noire encadrée) et à imposer des obligations de « sûreté d'usage » (sécurité by design) sur les algorithmes de recommandation, plutôt qu'une interdiction générale et une obligation de filtrage à l'entrée pour tous.

Enfin, au stade de la proportionnalité stricto sensu, la proposition de loi ne tient pas compte de l'ampleur de l'ingérence dans la liberté d'expression, d'information et de participation sociale des jeunes, ni des effets d'exclusion numérique qu'elle entraînera pour des services non présumés dangereux (plateformes d'apprentissage, forums d'entraide, espaces associatifs ou citoyens).

Le projet substitue à une régulation par le design des services (recommandations, profilage, pression commerciale) une logique d'interdiction et de contrôle d'accès, qui transfère la charge des risques des plateformes vers les usagers mineurs et leurs familles.

3. Absence de cadre public robuste pour la vérification d'âge et risques pour les données personnelles

Le dispositif français repose sur une hypothèse implicite : il existerait déjà, ou il pourrait émerger spontanément, un écosystème de solutions de vérification d'âge et de consentement parental techniquement fiables, économiquement viables, et juridiquement compatibles avec le RGPD et le DSA.

Les analyses menées au niveau national montrent au contraire que ces solutions sont coûteuses, techniquement risquées, peu rentables, et qu'aucun acteur ne souhaite en assumer la responsabilité à grande échelle, ce qui a conduit le législateur à déléguer cette charge aux plateformes elles-mêmes.

En l'absence de service public d'authentification dédié et d'un recours généralisé à des outils d'identité numérique publics, la mise en œuvre de la loi aboutira très probablement à la numérisation et au stockage de documents d'identité, à la reconnaissance faciale ou à des procédés équivalents, par des entreprises privées dont le modèle économique repose précisément sur la collecte et la monétisation de données.

Une telle architecture est difficilement conciliable avec le principe de minimisation et avec la clause du DSA selon laquelle les obligations de protection des mineurs ne doivent pas obliger les fournisseurs de plateformes à traiter des données supplémentaires pour déterminer si un utilisateur est mineur.

En outre, cette exigence s'appliquerait aussi à des services qui ne figureraient pas sur une éventuelle liste de services « toxiques » et qui, à ce titre, seraient présumés ne pas présenter de risque significatif pour les mineurs : le niveau de contrainte en matière de données serait ainsi sans commune mesure avec le niveau de risque réel.

4. Fragmentation du marché intérieur et contournement de la logique du DSA

En imposant un schéma national de vérification d'âge et de contrôle parental, sans cadre technique européen unifié, la France impose de facto aux fournisseurs de services établis dans d'autres États membres une couche réglementaire supplémentaire, distincte des obligations de diligence prévues par le DSA.

Cette approche fragmente l'espace numérique européen en segmentant les conditions d'accès en fonction du pays de résidence des utilisateurs, ce qui renforce à la fois la complexité de conformité pour les entreprises et le risque de forum shopping réglementaire.

Surtout, elle détourne la logique du DSA, qui repose sur la responsabilisation des plateformes quant à la conception de leurs systèmes (évaluations de risques, atténuation des risques, transparence algorithmique, encadrement du profilage) plutôt que sur des interdictions brutales d'accès ou des dispositifs nationaux isolés.

Les propositions alternatives formulées au niveau national montrent pourtant qu'il existe des voies plus conformes au droit de l'Union pour protéger efficacement les mineurs : renforcement de la responsabilité éditoriale des systèmes de recommandation pour les contenus recommandés aux jeunes, indépendance des signaleurs de confiance, mécanismes de financement « pollueur-payeur » pour la prévention et l'accompagnement des victimes, renforcement des capacités des autorités publiques de signalement et de retrait des contenus manifestement illicites.

5. Demande à la Commission

Le cadre européen et national reconnaît désormais que l'accès à Internet est l'un des vecteurs essentiels de la liberté d'expression et de communication, ce qui emporte pour les États une double obligation :

- une obligation négative de ne pas interrompre arbitrairement cet accès ;

- une obligation positive de le garantir effectivement, en particulier pour les jeunes générations, dans des conditions sûres et non discriminatoires.

Par sa décision du 10 juin 2009 sur la « riposte graduée », le Conseil constitutionnel a expressément jugé que les atteintes à la liberté d'accéder à Internet s'analysent, en l'état du droit, comme des atteintes à la liberté de communication, en rappelant qu'une coupure de la connexion ne peut relever que de l'autorité judiciaire et non d'une décision automatisée ou administrative. La Cour européenne des droits de l'homme, dans l'arrêt *Cengiz et autres c. Turquie* du 1er décembre 2015, a de son côté considéré que le blocage global de YouTube, plateforme centrale pour l'information politique et le « journalisme citoyen », constituait une violation de l'article 10 CEDH, faute de base légale suffisante et en raison du caractère généralisé de la mesure.

Plus récemment, dans sa décision du 18 juin 2020 sur la loi dite « Avia », le Conseil constitutionnel a censuré des mécanismes de retrait accéléré et privatisé des contenus en ligne au motif qu'ils portaient une atteinte inadaptée, non nécessaire et non proportionnée à la liberté d'expression, en soulignant le risque d'un « effet de sur-censure » lorsqu'on transfère aux opérateurs privés la charge de filtrer préventivement les contenus.

La logique d'interdiction générale de l'accès aux réseaux sociaux pour les moins de 15 ans, combinée à une vérification d'âge massive confiée aux plateformes, s'inscrit à rebours de ces trois jalons jurisprudentiels :

- elle traite l'accès à une part substantielle de l'espace public numérique comme une variable d'ajustement, alors qu'il est reconnu comme une composante de la liberté de communication ;

- elle instaure, de facto, un blocage quasi total de services centraux pour l'expression et l'information des jeunes, comparable, dans son esprit, au blocage de YouTube sanctionné par la CEDH ;

- elle délègue à des acteurs privés la mise en œuvre d'un filtrage structurel de l'accès, reproduisant les travers de la loi « Avia » que le juge constitutionnel a jugés inadaptés et manifestement disproportionnés.

En d'autres termes, une politique fondée sur l'interdiction d'accès et le filtrage en amont se trouve en conflit frontal avec la conception européenne de la liberté d'expression en

ligne : il ne s'agit plus de corriger les abus de cette liberté, mais de retirer l'accès lui-même au support qui permet son exercice, ce que les décisions précitées encadrent très strictement.

Compte tenu :

- de l'absence d'infrastructure publique européenne opérationnelle pour une vérification d'âge et un contrôle de l'autorité parentale compatibles avec le RGPD, le DSA et la Charte ;

- du non-respect manifeste du principe de proportionnalité, au regard d'alternatives moins intrusives ciblant les services effectivement dangereux et l'architecture algorithmique plutôt que l'accès des usagers ;

- du risque élevé de fragmentation du marché intérieur et de contournement de la logique de régulation par le design portée par le DSA ;

- et des enseignements clairs tirés des décisions Hadopi (2009), CEDH YouTube (2015) et Avia (2020) sur l'interdiction des blocages généraux et des dispositifs privatisés de contrôle de l'accès à Internet ;

la proposition de loi notifiée sous la référence 2026/0185/FR apparaît incompatible avec le cadre juridique de l'Union et avec la jurisprudence européenne et constitutionnelle relative à la liberté d'expression en ligne.

Il est en conséquence demandé à la Commission européenne :

1. **De rejeter la proposition notifiée et d'inviter la France à y renoncer dans sa philosophie actuelle**, en rappelant que la protection des mineurs ne peut se traduire par une interdiction structurelle d'accès à l'espace numérique, mais doit viser prioritairement les modèles de conception et de recommandation des services, dans le cadre harmonisé du DSA.

2. **D'engager, dans les travaux européens en cours sur la sécurité des enfants en ligne, l'élaboration d'un cadre technique commun et public de vérification d'âge et d'autorité parentale**, fondé sur des outils d'identité numérique reconnus au niveau de l'Union (eIDAS, portefeuilles d'identité numérique), reposant sur des jetons anonymisés, interopérables et audités, de manière à limiter drastiquement la circulation de données d'état civil entre plateformes et à garantir un contrôle public sur ces fonctions sensibles.

3. **D'encourager les États membres à mettre en œuvre des politiques nationales qui combinent régulation « par le design » des plateformes (obligations renforcées sur les systèmes de recommandation, indépendance des signaleurs de confiance, mécanismes de « pollueur-payeur » pour financer prévention et accompagnement des**

victimes) et obligations positives d’inclusion numérique, afin de garantir concrètement l’accès des mineurs à un Internet sûr, éducatif et pluraliste plutôt que de les en exclure.

Une telle orientation permettrait de concilier la protection effective des mineurs avec le respect du droit d’accès à Internet, dans sa dimension à la fois négative (interdiction des coupures généralisées ou des blocages disproportionnés) et positive (obligation de créer les conditions d’un accès sûr et effectif), conformément aux lignes directrices tracées par la jurisprudence européenne et française.