LIGUE DES DROITS HUMAINS

ANONYMAT EN LIGNE

/ Analyse de la Ligue des droits humains / Mars 2026

Commission Nouvelles Technologie LDH

INTRODUCTION

Des parlementaires fédéraux belges ont déposé des propositions visant à mettre fin à l'anonymat sur internet, dans le but de mieux lutter contre le cyberharcèlement et les discours de haine en ligne[1]. Le raisonnement est le suivant : si chaque compte sur un réseau social était obligatoirement lié à l'identité réelle de son titulaire, les autorités judiciaires pourraient plus facilement retrouver et poursuivre les personnes qui commettent des infractions en ligne. Cette traçabilité accrue aurait également un effet dissuasif : sachant qu'ils peuvent être identifiés, les internautes seraient moins enclins à adopter des comportements illicites.

Dans le même temps, une proposition vise à interdire l'accès aux réseaux sociaux aux personnes mineures. Elle imposerait aux internautes de vérifier leur âge avant de pouvoir créer un compte. L'idée sous-jacente est que, en excluant les jeunes de ces plateformes, la société les protégerait des effets néfastes descelles-ci. Cela permettrait de protéger leur développement et leur santé mentale.

La Chambre a invité la Ligue des Droits Humains à présenter sa position lors d'une des auditions organisées sur ces sujets[2]. La position de la Ligue, exposée dans le présent document, est fondée sur les droits humains.

PROPOSITION D'IDENTIFICATION DE TOUS LES UTILISATEURS ET UTILISATRICES DE RÉSEAUX SOCIAUX

La possibilité d'être anonyme en ligne, est cruciale dans une société démocratique moderne. Elle permet aux internautes de correspondre avec d'autres personnes ou d'accéder à des connaissances ou à du contenu.

Elle permet aux individus d'exercer leur liberté d'expression, d'information, de réunion. Elle est particulièrement précieuse pour les activistes, les défenseurs des droits humains et les journalistes d'investigation, dont le travail peut exposer à des représailles. De manière plus générale, les personnes exercent moins librement leurs libertés lorsqu'elles savent que leurs propos, leurs recherches en ligne et leurs choix sont susceptibles d'être surveillés et analysés — c'est ce que l'on appelle l'effet dissuasif ou « *chilling effect* ».

Il convient de distinguer deux notions souvent confondues :

- L'anonymat désigne la situation dans laquelle une personne ne peut être identifiée par personne.
- Le pseudonymat désigne la situation dans laquelle une personne utilise un nom

1 https://www.lachambre.be/flwb/pdf/56/1039/56K1039001.pdf
2 https://media.lachambre.be/meeting/56-019295-U1374

d'emprunt. Les autres internautes ne connaissent que ce pseudonyme et ne peuvent, au mieux, que supposer qui se cache derrière. En revanche, certains acteurs — comme le fournisseur de services (la plateforme ou l'opérateur télécom) — connaissent ou peuvent techniquement retrouver l'identité réelle. Ils sont donc en mesure d'établir le lien entre le pseudonyme et la personne.

Aujourd'hui, il est techniquement possible d'être anonyme en ligne, mais c'est difficile. Il est en particulier difficile de maintenir cet anonymat pendant une longue durée. L'autorité de la protection des données française souligne à ce propos que :

> « *Rester anonyme en ligne suppose [..] d'utiliser de nombreuses techniques, qui vont bien au-delà de la seule utilisation d'un nom d'emprunt ou d'un pseudonyme. La protection de l'anonymat en ligne nécessite, par exemple, d'utiliser un ordinateur dédié, des outils spécifiques masquant l'adresse IP de connexion, ainsi des comptes également dédiés et non reliables à la personne. Au quotidien, il est donc très difficile de se « cacher » en ligne, de ne pas être tracé ou de ne pas voir ses données être collectées.* » Et de rajouter : « L'« anonymat » sur internet est donc plutôt du pseudonymat et peut être levé, par exemple à la demande d'un juge. »[3]

Dans la suite de ce document, nous défendons les avantages du pseudonymat, mais aussi ceux, tout aussi importants, de l'anonymat.

L'anonymat est parfois présenté comme une des conditions favorisant des comportements en ligne néfastes ou illicites : diffamation, *revenge porn*, harcèlement, diffusion de contenus terroristes ou pédocriminels. Sur cette base, certains suggèrent que supprimer l'anonymat en ligne suffirait à résoudre ces problèmes.

Cette approche est ce qu'on appelle une vision technosolutionniste : elle présuppose qu'une mesure technique unique peut résoudre des phénomènes qui sont en réalité complexes et multifactoriels.

Elle sous-estime également la valeur propre du droit à l'anonymat, qui est une condition préalable à l'exercice effectif de la liberté d'expression, du droit à l'information et de la liberté de réunion. Elle ignore en outre le rôle protecteur que joue l'anonymat pour les communautés marginalisées, qui sont souvent les premières victimes des abus en ligne, et qui bénéficient précisément de la protection qu'offre l'anonymat pour s'exprimer sans crainte.

Possibilités actuelles d'identification

En Belgique, les services de police disposent déjà des moyens légaux nécessaires pour identifier des personnes suspectées de comportements illicites en ligne. Sur demande d'un juge d'instruction, ils peuvent obliger un fournisseur de services — site web, application, opérateur télécom — à communiquer les données permettant d'identifier un utilisateur : adresse IP, adresse MAC, géolocalisation, identifiant du routeur wifi, identité de l'abonné, etc[4]. La Circulaire COL 13/2025 *relative à la politique criminelle en matière de cyberviolence(s) contre les personnes* décrit en détail ces mesures.

3 https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf
4 C. FORGET, « La collecte de preuves informatiques en matière pénale », Pas de droit sans technologie, 2015, p. 265

Par ailleurs, depuis l'entrée en vigueur du Règlement sur les services numériques (Digital Services Act — DSA), les grandes plateformes ont une obligation harmonisée à l'échelle de l'Union européenne. Elles doivent signaler aux autorités judiciaires ou répressives les cas avérés ou soupçonnés de cyberharcèlement ou de menaces en ligne, et leur fournir toutes les informations disponibles permettant d'identifier l'auteur (article 18 DSA).

Des difficultés peuvent exister en Belgique, mais il est possible d'y remédier de manière moins attentatoire aux droits humains. Il n'est pas nécessaire de lier chaque compte de réseau social à l'identité légale de son propriétaire.

Il serait par exemple possible de faciliter les recours civils de victimes de harcèlement. Lorsque l'auteur des faits utilise un pseudonyme, son identité est inconnue. En droit belge, cela rend la voie civile impraticable : la victime est contrainte de déposer une plainte pénale pour qu'un juge d'instruction puisse ordonner à la plateforme de révéler l'identité de l'utilisateur. Lorsque le compte a été créé à l'étranger, la procédure est encore plus lente : la police doit solliciter la coopération volontaire de la plateforme étrangère, ce qui n'est pas garanti et s'avère chronophage. Ouvrir la voie civile à ce type de demandes permettrait d'alléger et d'accélérer considérablement le système — c'est précisément l'objet d'une proposition de loi déposée en 2025.[5]

Il serait par ailleurs possible de faciliter les poursuites pénales. L'article 150 de la Constitution belge prévoit que certains discours de haine doivent être jugés par une cour d'assises — c'est notamment le cas des délits de presse, même lorsqu'ils sont motivés par des critères discriminatoires (convictions religieuses ou philosophiques, orientation sexuelle, genre, identité de genre, expression de genre, handicap). Seuls les délits de presse inspirés par le racisme, la xénophobie ou le négationnisme peuvent être poursuivis devant les tribunaux correctionnels. Or, réunir un jury d'assises est une procédure longue et coûteuse, qui n'est en pratique pas prioritaire dans la politique pénale actuelle. Ce problème structurel empêche de fait la poursuite de nombreuses infractions — mais il peut être résolu par une réforme de l'article 150, que la Ligue des droits humains appelle de ses vœux depuis longtemps, en concertation avec de nombreuses autres organisations[6]. Ceci ne requiert pas de mettre fin à l'anonymat.

Une troisième difficulté structurelle est celle du sous-financement de la justice. Ce qui est illégal hors ligne est *déjà* illégal en ligne. La justice manque toutefois de moyens pour apporter une réponse adéquate à ces comportements. En Belgique, la Procureure fédérale Ann Fransen a récemment souligné le manque de *moyens humains* pour lutter contre la cybercriminalité[7]. Plus généralement, en Europe, il est fréquent que la police ne dispose pas des ressources suffisantes pour donner suite aux signalements de contenus illégaux qui lui sont transmis[8].

Le DSA contribuera à améliorer la situation en renforçant la coopération des plateformes avec les autorités — mais il ne résoudra pas le problème de fond. Pas plus, d'ailleurs, que ne le ferait l'obligation d'identifier chaque utilisateur de réseau social.

5 *Proposition de loi ouvrant la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet et modifiant l'article XII.20 du Code de droit économique*, document Chambre 56K0725001.
6 https://www.liguedh.be/article-150-mettons-fin-a-une-double-discrimination-dans-notre-constitution/
7 https://www.lesoir.be/677767/article/2025-05-26/ann-fransen-procureure-federale-nous-avons-reussi-eviter-plusieurs-
8 comme le reportait le journal allemand Tagesschau à propos de contenu pédopornographique signalé aux autorités, qui restait accessible en ligne des années durant. https://www.tagesschau.de/investigativ/panorama/kinderpornografie-loeschung-101.html

Inefficacité de l'identification

La mesure d'identification proposée serait inefficace. Elle n'atteindrait pas son objectif, pour deux raisons.

Premièrement, la corrélation entre anonymat et comportements problématiques en ligne est bien ancrée dans les esprits — mais elle n'est pas confirmée par les faits. Après les commentaires racistes qui ont suivi la finale de l'Euro 2020 de football, Twitter UK (aujourd'hui X) a relevé q 99 % des comptes suspendus pour propos injurieux n'étaient ni anonymes ni intraçables.[9] Ce constat est partagé par d'autres voix, notamment la journaliste antiraciste Rokhaya Diallo[10]. Il est également étayé par plusieurs études menées en Corée du Sud sur l'efficacité d'une mesure similaire[11]. Il existe certes des auteurs se cachant derrière un pseudonyme, mais ce n'est pas pour autant que l'identification obligatoire aurait l'impact majeur promis sur les discours de haine en ligne.

Deuxièmement, une telle mesure serait facilement contournable. Il suffit de quelques connaissances techniques pour créer un profil depuis un pays hors Union européenne, via un VPN ou le navigateur TOR, puis se connecter normalement depuis l'Europe sans être soumis à l'obligation d'identification. Ce phénomène de contournement a déjà été observé dans 19 États fédérés des États-Unis[12]. C'est également le constat qu'a dressé la Cour constitutionnelle sud-coréenne à propos d'une loi de 2007, qui imposait une vérification d'identité à toute personne souhaitant publier des commentaires sous pseudonyme sur les principales plateformes locales. Après en avoir examiné la proportionnalité, la Cour a invalidé cette loi en 2012 : la mesure était contournable et n'avait eu aucun effet sur les comportements visés. Elle était donc inefficace au regard de l'objectif poursuivi[13].

Le cyberharcèlement et les discours de haine ne prolifèrent pas parce que leurs auteurs sont intraçables. Ils prolifèrent parce que les moyens consacrés à leur répression effective sont insuffisants — ce qui peut effectivement donner aux auteurs un sentiment d'impunité. Une autre raison tient au modèle économique des plateformes elles-mêmes : leurs algorithmes favorisent les contenus choquants, provocateurs ou polarisants, qui génèrent davantage d'engagement et donc davantage de recettes publicitaires. Dans ce contexte, les plateformes acceptent parfois de suspendre un compte signalé, mais elles n'ont guère d'incitant à prévenir réellement la récidive et elles ne préviennent pas nécessairement la police. En effet, un utilisateur « problématique » se créant un nouveau compte continue de fréquenter la plateforme et de générer des revenus. Le DSA modifie cette donne, en imposant aux plateformes de nouvelles obligations en matière de signalement et de coopération avec les autorités.

9 https://blog.x.com/en_gb/topics/company/2020/combatting-online-racist-abuse-an-update-following-the-euros Autres sources: https://shs.cairn.info/la-france-tu-l-aimes-ou-tu-la-fermes--9782845977839-page-132?lang=fr ; https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0155923

10 https://shs.cairn.info/la-france-tu-l-aimes-ou-tu-la-fermes--9782845977839-page-132?lang=fr

11 Areum Kang, 2008, *Have Malicious Comments Really Decreased in the Aftermath of the Real Name Policy? Well…* http://news.sportsseoul.com/read/life/506278.htm (en Coréen).

12 https://www.eff.org/deeplinks/2025/01/vpns-are-not-solution-age-verification-laws

13 Ceci venait en sus des autres observations de la Cour, qui pointait le caractère indiscriminé de la loi, son impact sur la liberté d'expression et la liberté de la presse, son impact discriminatoire sur les résidents·es étrangers·ères (sans ID coréen), le risque de vol de données et d'usurpation d'identité, et le fait qu'elle n'était pas le mesure la moins restrictive/attentatoire. https://global-freedomofexpression.columbia.edu/wp-content/uploads/2017/08/Korea_internet_judgment.pdf

Dans ces conditions, les difficultés sont donc réelles, mais surmontables. Elles ne justifient pas d'imposer une identification généralisée de l'ensemble des utilisateurs en ligne.

Impact disproportionné sur les droits et libertés

Au-delà de son inefficacité, la mesure d'identification est également inadéquate parce que disproportionnée — à deux égards.

D'abord, par son étendue. Elle couvrirait la totalité de la population, sans distinction ni ciblage. Il s'agirait d'une forme de surveillance de masse préemptive.
Ensuite, par son impact sur les droits humains. Les réseaux sociaux permettent aujourd'hui à chacun de s'exprimer, de s'informer et de se rassembler à une échelle qui était auparavant réservée aux acteurs disposant d'un accès aux médias traditionnels — télévision, presse écrite. C'est un outil à fort potentiel d'émancipation. Si une infime minorité en fait un mauvais usage, il serait disproportionné d'en conditionner l'accès à une identification préalable généralisée.

L'impact d'une telle mesure serait immense. Il toucherait d'abord celles et ceux qui ne sont pas en mesure de s'identifier — parce qu'ils n'ont pas de smartphone, pas de document d'identité, ou parce qu'ils se heurtent à la fracture numérique. Il toucherait ensuite, plus largement, toutes les personnes qui préféreront se taire plutôt que de s'exprimer sous leur identité réelle. C'est ce que l'on appelle l'effet dissuasif ou *chilling effect* : la surveillance engendre l'autocensure.

Il existe également un risque sérieux de *function creep* — c'est-à-dire d'élargissement progressif et insidieux des finalités de la mesure. Une fois le système d'identification en place, rien n'empêcherait de l'utiliser à d'autres fins que celles initialement prévues : identifier les membres d'un groupe d'éco-activistes ou d'un collectif pro-Palestine, par exemple, sous prétexte de prévenir ou réprimer leurs actions.

La situation des droits humains en Belgique n'est pas comparable à celle de la Hongrie ou de la Chine. Mais le respect de l'Etat de droit y est en recul[14]. Les majorités politiques peuvent par ailleurs évoluer rapidement. On ne peut donc écarter la possibilité que l'Etat ait un jour recours à des formes de répression anti-démocratiques et que les outils d'identification mis en place aujourd'hui soient alors détournés à cette fin.

Les avantages du maintien de l'anonymat et du pseudonymat dépassent largement leurs inconvénients. L'absence d'identification systématique garantit la capacité de s'exprimer à l'abri de pressions extérieures ou de répressions. Elle protège celles et ceux qui sont déjà la cible de de l'oppression, de mauvais traitements ou de violences. Elle est indispensable pour toutes les personnes qui ont besoin de protéger leur identité pour débattre librement, consulter des informations sensibles, s'organiser collectivement — ou simplement exister en ligne sans crainte. Au-delà de la liberté d'expression et du droit à l'information, une telle mesure affecterait également le droit à la protection des données personnelles, la liberté de réunion et d'association, la liberté de la presse, et le droit au respect de la vie privée.

14 https://www.federalesinstitutmenschenrechte.be/fr/publications/rapport-sur-letat-de-droit-2025

VÉRIFICATION DE L'ÂGE ET CLOISONNEMENT DE L'ACCÈS AUX SERVICES

La deuxième mesure débattue est la restriction d'accès aux réseaux sociaux pour les personnes mineures, dans le but de protéger leur santé mentale[15]. La mesure est double : l'accès des moins de 18 ans serait rendu illégal, et cette interdiction serait mise en œuvre par un système de vérification de l'âge de chaque utilisateur.

La Ligue considère cette mesure disproportionnée, inefficace et dangereuse.

L'interdiction : effets défavorables sur les droits, le développement, l'éducation et l'épanouissement des jeunes

Limiter l'accès aux réseaux sociaux sur la base de l'âge n'élimine pas les risques que ces plateformes comportent. Les jeunes y seront simplement exposés sans préparation, le jour où ils atteindront l'âge requis[16]. Les représentants des droits de l'enfant s'opposent à cette approche. Ils prônent des mesures fondées sur l'émancipation et le soutien — pas sur la restriction et le contrôle[17]. Les jeunes eux-mêmes ne veulent pas d'une interdiction mais veulent être protégés d'une manière émancipatoire. Les jeunes eux-mêmes ne souhaitent pas une interdiction. Ils veulent être protégés, mais d'une manière qui respecte leur autonomie et leur volonté d'émancipation[18].

La Ligue ne défend pas les plateformes. Elle critique leur modèle économique, leurs algorithmes conçus pour capter l'attention, et les contenus toxiques qu'ils favorisent. Mais elle reconnaît aussi les bénéfices réels que ces espaces apportent à de nombreux jeunes — en particulier aux jeunes LGBTQIA+, aux jeunes marginalisés, aux jeunes isolés en milieu rural. Pour eux, les réseaux sociaux sont souvent des espaces essentiels de communauté, d'échange et d'expression. Les exclure de ces espaces n'est pas les protéger. C'est, au mieux, retarder le problème — tout en leur niant leurs droits fondamentaux.

La Ligue estime qu'il faut s'attaquer au problème à sa racine : rendre les plateformes plus saines et plus sûres pour l'ensemble des internautes. Dans ce cadre, il faut mieux outiller les jeunes pour faire face aux risques qu'ils et elles rencontrent encore — en favorisant leur autonomie, leur résilience, et les canaux de confiance auxquels ils peuvent recourir en cas de problème : parents, personnel scolaire, mécanismes de signalement en ligne.

Exclure n'est pas protéger, cela revient au mieux à retarder le problème, tout en niant aux jeunes leurs droits fondamentaux.

15 Proposition de résolution visant à mettre fin à l'anonymat en ligne et à instaurer un contrôle effectif de l'âge pour l'accès aux réseaux sociaux. Document parlementaire 56K1039. https://www.dekamer.be/kvvcr/showpage.cfm?section=flwb&language=fr&cfm=flwbn.cfm?lang=N&dossierID=1039&legislat=56

16 https://eprints.lse.ac.uk/112559/

17 https://home.crin.org/issues-droits-dans-espace-numerique; https://www.standaard.be/opinies/ook-online-verdienen-kinderen-een-veilige-wereld/74702800.html; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines/F3496535_en; https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/65dcb5321b1c1630bd619a95/1708963144372/Access%2BDenied_access_to_information.pdf ; https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf

18 https://www.youthforum.org/policy-library/on-guaranteeing-youth-safety-and-rights-in-the-digital-world-a-call-for-a-balanced-approach ; https://www.lemonde.fr/idees/article/2026/01/25/interdiction-des-reseaux-sociaux-aux-moins-de-15-ans-la-voix-des-jeunes-est-absente-du-debat-sur-la-regulation-du-numerique_6664036_3232.html ; https://www.euroconsumers.org/wp-content/uploads/2025/09/Growing-up-online-Building-a-digital-future-for-minors-by-minors-1-.pdf ; https://fosi.org/wp-content/uploads/2025/12/Children-Parents-Perceptions-of-Social-Media-and-Classroom-Smartphone-Bans-in-the-U.S.-and-Australia.pdf ; https://www.bbc.com/audio/play/p0mlv779

L'OCDE a publié le 15 mai 2025 un rapport qui rejette l'idée d'interdire aux jeunes les appareils numériques ou les réseaux sociaux. Les enfants ont besoin d'acquérir des compétences numériques indispensables à leur vie personnelle et professionnelle future. Une interdiction ne répond pas non plus au besoin de protection exprimé par les enfants et les adolescents eux-mêmes[19]. Le rapport souligne que les plateformes numériques offrent aux jeunes de nombreux moyens de s'informer, de s'amuser et d'obtenir du soutien — y compris un soutien qui n'est pas disponible hors ligne. Dans les pays de l'OCDE, 40 % en moyenne des adolescents de 11 à 15 ans sont en contact régulier avec des amis rencontrés en ligne. Plutôt qu'une interdiction, l'OCDE recommande de renforcer l'éducation aux médias à l'école, de mieux informer les parents, et d'intégrer la parole des enfants dans l'élaboration des politiques publiques[20]..

Le monde numérique fait désormais partie intégrante de la vie quotidienne. Ce qui était optionnel il y a dix ans est devenu essentiel — pour communiquer, s'informer, apprendre, travailler. Les enfants ne sont pas des objets passifs de protection : ce sont des sujets de droits, qui doivent être progressivement accompagnés vers l'autonomie[21]. La Convention des Nations Unies relative aux droits de l'enfant le dit clairement : les capacités des enfants sont évolutives (articles 5 et 14(2)). Ils ne peuvent pas être jugés incapables d'exercer les droits qui leur sont reconnus — liberté d'expression, droit à l'information, droit d'être entendu. Le droit des enfants à être protégé ne peut pas primer et écarter leurs autres droits. Une interdiction stricte fondée sur l'âge est incompatible avec l'obligation d'accompagner progressivement les enfants vers l'exercice autonome de leurs droits[22].

La Ligue défend donc une approche émancipatoire, fondée sur le droit existant. La vérification de l'âge figure déjà dans de nombreux textes — le DSA (article 35), la Directive sur les services audiovisuels (articles 6bis et 28ter), le RGPD (article 8). Elle constitue toutefois toujours une mesure optionnelle et proportionnée. La rendre obligatoire et systématique aurait l'effet inverse : elle fragiliserait les mécanismes de protection déjà en place. Le DSA impose aux plateformes d'identifier et de limiter les risques systémiques qu'elles créent, en particulier pour les mineurs, sans pour autant traiter davantage de données personnelles. Bannir les jeunes enverrait un double mauvais signal. D'une part, ce serait dire aux plateformes qu'elles n'ont plus rien à faire pour protéger les mineurs (puisqu'ils ne sont pas censés être sur la plateforme. D'autre part, cela reviendrait à admettre que les pratiques toxiques des plateformes sont acceptables dès lors qu'elles ne touchent que des adultes.

3.2. La méthode : contournement inévitable, et exclusion corollaire d'autres publics marginalisés

La proposition envisage l'utilisation de l'application itsme, ou à terme du portefeuille numérique européen eID, pour confirmer qu'un internaute a atteint l'âge requis, sans divulguer d'autres informations[23]. Cette approche est préférable à ce qui se pratique

19 https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.html
20 https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.htm
21 https://www.tandfonline.com/doi/full/10.1080/17482798.2024.2435015
22 https://digitallibrary.un.org/record/3906061?v=pdf#files
23 Malheureusement, ce portefeuille numérique, encore en développement ne délivre pas toutes les promesses faites envers la possibilité de l'utiliser sans être tracé à travers le web. Les spécificités techniques de l'outil sont encore en cours de négociation. https://edri.org/our-work/the-eid-wallet-still-doesnt-deserve-your-full-trust/ https://edri.org/our-work/showing-

au Royaume-Uni ou aux États-Unis, où les utilisateurs sont contraints de partager des documents d'identité sans garantie qu'ils soient ensuite supprimés — avec les risques que cela implique en matière de fuite de données, de fraude et d'usurpation d'identité[24].

Cependant, cette méthode sera contournée. Les jeunes qui souhaitent accéder aux plateformes trouveront rapidement comment le faire. Le recours à un VPN permet de s'enregistrer comme utilisateur relevant d'une juridiction étrangère, non soumise à l'obligation de vérification[25]. La promesse de ne vérifier que l'âge — sans traiter d'autres données — signifie qu'un seul jeune majeur pourra valider l'accès de tous ses amis mineurs. Et la méthode de contournement la plus répandue reste tout simplement de passer par ses parents : 58,5 % des parents en Chine, et entre 68 et 77 % aux États-Unis, aident activement leurs enfants à franchir ces vérifications.[26].

Si la mesure était efficace, elle poserait un autre problème : la discrimination. Conditionner l'accès à un réseau social à l'utilisation d'itsme — ou de tout autre outil accessible uniquement via un smartphone récent — exclurait de fait de nombreuses personnes déjà marginalisées : celles qui n'ont pas de smartphone, celles qui n'ont pas de document d'identité (comme les personnes sans papiers), ou celles qui manquent de compétences numériques — soit environ 40 % de la population belge[27].

Si elle était efficace, cette vérification obligatoire pourrait aussi être instrumentalisée par des États comme la Hongrie, qui utilisent déjà la protection des enfants comme prétexte pour bloquer tout contenu à caractère LGBTQIA+[28].

CONCLUSION

La Ligue des droits humains appelle à s'attaquer aux causes réelles du cyberharcèlement et des effets néfastes des réseaux sociaux sur la santé mentale — plutôt que d'adopter des mesures qui portent une atteinte disproportionnée aux droits fondamentaux de l'ensemble des utilisateurs. Elle invite les responsables politiques à privilégier des mesures proportionnées : des mesures qui outillent les victimes, favorisent leur protection et leur inclusion, et contribuent à rendre l'environnement en ligne plus sain et plus sûr pour tous et toutes.

---

your-id-to-get-online-might-become-a-reality-a-closer-look-at-the-eus-new-age-verification-app/; https://edri.org/our-work/civil-society-demands-european-commission-must-close-e-id-loopholes/; https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet; https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet ; https://epicenter.works/content/eidas-ein-schritt-vor-zwei-zurueck

24 https://www.researchgate.net/publication/221305493_Empirical_analysis_of_internet_identity_misuse_case_study_of_south_Korean_real_name_system ; Dans les autres cas, leur visage est scanné afin d'estimer leur âge (et là aussi, sans garantie que leurs données biométriques soient effacées après), ou alors les utilisateurs voient leur comportement traqué, analysé et profilé afin d'estimer leur âge.

25 https://www.eff.org/deeplinks/2025/01/vpns-are-not-solution-age-verification-laws; https://www.bbc.com/news/articles/cn72ydj70g5o

26 https://global.chinadaily.com.cn/a/202408/20/WS66c3e9a1a31060630b923e74.html ; https://www.ftc.gov/sites/default/files/documents/public_comments/massachusetts-00243%C2%A0/00243-82161.pdf; https://www.bbc.com/news/articles/cwyp9d3ddqyo

27 Fondation Roi Baudouin, baromètre de l'inclusion numérique 2024, https://www.calameo.com/read/001774295f8190a0f968e?authid=GjXuHcs7LcLj

28 https://socialbites.ca/news/hungarian-regulator-reviews-netflix-episode-over-lgbtq-content