

La France vient de voter la fin de l'anonymat sur internet. Protéger nos enfants sur internet ? C'est un contrôle généralisé des français.

La France vient de voter une loi pour interdire les réseaux sociaux aux moins de 15 ans.

L'intention est juste, l'inquiétude des parents est réelle et personne ne peut contester qu'il faille protéger les enfants des contenus qui les blessent, les manipulent ou les exposent à des prédateurs.

Mais ce que personne ne dit clairement, c'est le prix que nous allons tous payer pour y parvenir. Car pour surveiller nos enfants, on va surveiller tout le monde. Sans exception, sans un retour en arrière possible.

Posons-nous une question simple, celle que les législateurs auraient dû poser avant de voter. Comment savoir qu'un utilisateur a moins de 15 ans ? Il faut vérifier son âge. Et pour vérifier l'âge de quelqu'un, il faut l'identifier. Pas seulement les enfants, pas seulement les adolescents, tout le monde, sans distinction. Vous. Moi. Le retraité qui lit ses nouvelles le matin sur son téléphone. La femme qui cherche en silence des informations médicales à trois heures du matin, des informations qu'elle n'oserait pas demander à son médecin. L'étudiant qui explore des idées politiques que sa famille ne partagerait peut-être pas. La victime de violence conjugale qui cherche de l'aide sans laisser de trace. Tous identifiés. Tous fichés. Définitivement.

Ce qui se passe ensuite est mécanique, inévitable, et connu de tous les spécialistes. Votre vrai nom est lié à votre compte. Chaque connexion est enregistrée avec l'heure, la durée, l'endroit depuis lequel vous vous connectez. Vos lectures, vos recherches, vos hésitations, les sujets sur lesquels vous revenez plusieurs fois, ceux que vous fuyez et tout cela compose un portrait de vous d'une précision que votre propre famille ne possède pas. C'est ce qu'on appelle le profilage. Ces profils valent des milliards de dollars. Ils sont au cœur du modèle économique des grandes plateformes numériques. Ils servent à vous vendre des produits au moment précis où vous êtes le plus vulnérable à les acheter, à influencer vos opinions politiques en vous montrant uniquement ce qui conforte vos peurs, à orienter progressivement ce que vous pensez sans que vous vous en rendiez compte. Et demain, si l'on ajoute la reconnaissance faciale à ce dispositif, le tableau sera complet. Votre visage dans l'espace public deviendra une donnée comme une autre, rattachée à votre profil numérique.

On nous rassure en nous parlant de "tiers de confiance", des applications officielles, qui seraient chargées d'effectuer ces vérifications d'identité sans transmettre les données personnelles aux plateformes. L'intention est louable. Mais en trente-cinq ans de carrière dans l'informatique et la cybersécurité, j'ai appris une vérité que l'histoire confirme sans cesse : rien n'est absolument sécurisé. Rien, sauf la mort après la vie. Chaque système peut être attaqué, contourné, compromis. Les plus grandes banques mondiales ont été hackées. Les services de renseignement américains ont été piratés. Les hôpitaux européens voient leurs données patients volées et revendues.

Confier à un tiers la clé de l'identité numérique de toute une population, c'est créer une cible d'une valeur inestimable, unique, centralisée, que toutes les formes de cybercriminalité et d'espionnage étatique vont s'employer à atteindre. Le jour où ce système sera compromis et ce jour viendra, c'est l'identité numérique de millions de citoyens qui sera exposée.

Il y a ensuite ce que la loi ne peut pas atteindre, et que personne n'évoque dans le débat public. Vos données ne restent pas en Europe. Elles traversent les frontières, elles sont traitées aux États-Unis, en Chine, dans des pays dont les lois sur la vie privée ne ressemblent en rien aux nôtres. Elles reviennent transformées en publicités ciblées, en contenus personnalisés, en profils commerciaux d'une précision redoutable. Le droit européen s'arrête aux frontières de l'Europe. Le règlement RGPD, pourtant le plus ambitieux du monde en matière de protection des données, ne peut pas s'appliquer à ce qui se passe à Singapour, à San Francisco ou à Pékin.

Or l'Europe ne représente que 5,5% de la population mondiale. Les 94,5% restants obéissent à d'autres règles, ou à aucune.

Quand les géants du numérique paient une amende record en Europe, ils la règlent comme une facture d'électricité et continuent leurs activités sans changer d'un iota leurs pratiques. Pour eux, l'amende est un coût opérationnel, intégré dans leurs prévisions budgétaires. Pas une sanction. Pas une dissuasion et c'est pour cela que Trump nous sanctionne avec des droits de douane à 100%.

L'Australie nous a précédés sur cette voie dès décembre 2025, devenant le premier pays au monde à interdire les réseaux sociaux aux moins de 16 ans. Six mois plus tard, le bilan est sévère et documenté. Le British Medical Journal confirme que l'impact sur la navigation des jeunes adolescents est resté marginal. Les adolescents ont conservé l'accès aux plateformes grâce à des VPN, à des faux comptes, aux erreurs des systèmes de reconnaissance faciale. N'importe quel lycéen sachant utiliser un moteur de recherche a trouvé comment contourner l'interdiction en quelques minutes. Le gouvernement australien vient de doubler les amendes imposables aux plateformes, avouant implicitement que la première version de la loi n'a pas fonctionné. L'infrastructure de contrôle, elle, est bien en place. Et elle ne disparaîtra pas, même si la loi était un jour abrogée. Les données collectées, elles, existent.

On nous propose de sacrifier la liberté de tous pour une efficacité incertaine. La méthode est contournable par

n'importe quel adolescent de 15 ans. Mais l'anonymat que vous pensiez avoir, lui, ne reviendra pas. Ce que l'on construit ici, sous couvert de protection de l'enfance, c'est l'infrastructure technique d'un contrôle généralisé de la population. Une infrastructure qui sera là demain, après-demain, quel que soit le gouvernement en place.

Il existe pourtant de meilleures voies, et elles n'impliquent pas de fichier l'ensemble de la population. La première est de responsabiliser les parents et d'éduquer aux usages du numérique, plutôt que de s'en remettre à de simples sanctions contre des plateformes qui ne les craignent guère. Pourtant, l'Europe représente 18 % du PIB mondial : c'est un marché que les géants de la Tech ne peuvent pas se permettre de perdre si l'on impose de véritables règles sur la conception même de leurs services. La deuxième est d'investir massivement dans l'éducation aux médias numériques, dès le plus jeune âge, dans les écoles, dans les familles. Xavier Degraux, spécialiste des réseaux sociaux, estime que les budgets consacrés à cette éducation devraient être dix à vingt fois plus importants qu'aujourd'hui. Il a raison. Et rien n'empêche d'exiger que ce soit les géants du numérique eux-mêmes qui financent cette éducation, puisque ce sont eux qui profitent de l'exposition de nos enfants à leurs plateformes.

Nos enfants méritent d'être protégés. Personne ne le conteste. Mais nos libertés fondamentales, la liberté d'expression, le droit à la vie privée, le droit à l'anonymat reconnu par la Cour européenne des droits de l'homme méritent elles aussi d'être défendues. Ces deux objectifs ne sont pas incompatibles. Ils exigent simplement que l'on choisisse les bons outils, plutôt que les plus simples à annoncer en conférence de presse.

Thierry MANSVELT

*Expert judiciaire en informatique, télécommunications
et propriété intellectuelle (n° Exp 2026892)
Enregistré au SPF Justice belge — www.baei.be*

L'auteur a formellement interpellé le Parlement belge sur cette problématique dès le 30 mars 2026, avant que la France légifère. Il a reçu des réponses officielles des ministres concernés. L'ensemble du dossier est disponible sur demande.

« Dès 2007, il alertait déjà sur les failles d'usurpation sur le GSM. Vingt ans plus tard, le législateur s'apprête à commettre exactement la même erreur de conception à l'échelle de toute la population française. »