



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*

Conseil

de l'IA
et du Numérique

Note

Protecting Minors Online Through Age Verification: How Can We Go Further?

March 2026

Executive Summary

On the 26th of January 2026, the French National Assembly adopted at its first reading a bill aimed at protecting minors from the risks of social media use. The bill aligns with the government's priority to oversee minors' digital habits. France has thus joined the international momentum for the regulation of platform use by minors and is poised to become the first European Union (EU) Member State to implement a ban directly targeting minors' access to social media platforms, just weeks after the passage of the *Online Safety Amendment Act* in Australia.

Recent legislative initiatives follow years of relative political inertia, marked by a reluctance to confront the economic power of major platforms and the legal challenges surrounding the regulation of their business models. Fifteen years after the Arab Spring, during which social media platforms established themselves as genuine tools for democracy, the verdict is now clear: **the same networks are today highly mixed tools, far from the healthy spaces and vehicles of empowerment many hoped for. They expose users, particularly the youngest, to well-identified major risks.** Successive studies reveal an alarming situation with minors exposed daily to content which is violent, and which encourages self-harm, whilst being targeted by intrusive commercial practices and platform design mechanisms engineered to capture their attention. In France, 77% of minors aged between 11 and 17 years have already encountered harmful content, 48% of whom regularly, negatively impacting the wellbeing of 25% of them.

Lacking alternatives and pressed for time, legislators are preparing drastic measures intended to be symbolically strong: banning minors from platforms through the imposition of age verification. In the short term, it is necessary to acknowledge that this decision is a response to very real immediate needs; however, at the same time this approach offers only a partial response to the structural causes of the risks posed by online services. Whilst the banning of minors from social media platforms may seem a solution of last resort, it must not become a substitute for a profound overhaul of digital spaces for the benefit of all users.

This note provides an overview of the multifaceted risks encountered by minors online (I) and current/proposed regulations alongside their limits (II). It concludes with an analysis of the remaining issues in these provisions and provides several propositions for the rethinking of the regulation of digital services (III).

Regulations aiming to protect minors online face several conceptual questions:

- What is the scope of the law? The challenge lies in choosing between targeted regulations, at the risk of moving towards case-by-case oversight, and a global approach, which may encounter difficulties in enforcement.
- Which age verification method should be implemented, considering potential workarounds and wider effects? User age verification has commonly become the prerequisite for policies for the protection of minors online. However, critics increasingly point to the counterproductive

nature of age verification, which they argue merely postpones a sudden and unprepared introduction to complex digital environments. Verification methods are also susceptible to being bypassed, including with the use of VPNs, and they present risks to the most vulnerable minors in terms of inclusivity and accessibility.

- Which content should be subject to regulation? Certain texts target specific categories of content due to the risks they present to so-called “vulnerable” users, whilst others have a broader scope, encompassing various content categories and prioritising a risk-based approach.

Alternative methods for protecting minors are also being explored worldwide, further widening discussions, such as age verification at the device level, mandatory time-based restrictions, and modified digital interfaces.

However, whilst the risks for minors on social media platforms are real and present, age verification is not sufficient to address all the pitfalls or to guarantee a safer use of digital services for all users, an aspect which is now essential to democracy. Furthermore, it is vital to keep in mind that **minors must be able to find the tools and means to discover, learn, share, and empower themselves online in safety.** This was the initial promise of the digital age and remains a fundamental right for children.

Finally, **the debate on the protection of minors online must not eclipse the structural issues that many current regulations tend to neglect.** Faced with these challenges, France and Europe must, without further delay, accelerate progress on five priority areas:

1. **Create a European standard** for the protection of minors online.
2. **Open up platform functionalities,** establish a “right to customisation”, and strengthen algorithmic transparency.
3. **Rethink the division between “host” and “publisher”.**
4. **Consider the diverse usages of digital services,** particularly those involving generative AI.
5. **Strengthen and expand education** in digital literacy, media, and information.

Table of Contents

Executive Summary	1
Introduction.....	4
I. The Use of Social Media: Multifaceted Risks for Minors Online	5
II. Overview of Regulations on the Protection of Minors Online and Key Associated Questions... 6	6
(a) What is the scope of application?	11
(1) Regulations targeting specific categories of digital services	11
(2) Regulations creating new obligations for digital services based on the number of users	12
(b) Which age verification methods are possible and what workarounds or harmful effects are present?.....	13
(1) Different age verification methods and their applications	13
(2) Underlying issues with age verification.....	16
(3) The risk of bypassing age verification	17
(c) What content is targeted by the legislation?	18
(1) Regulations targeting specific categories of content	18
(2) Regulations adopting a risk-based approach	19
III. What Digital Future for Young People?	19
(a) How can we strengthen the fundamental rights of minors online?	20
(1) Investing in Online Empowerment.....	20
(2) Strengthening Personal Data Protection.....	21
(3) Consolidating and Diversifying the Education of Minors	22
(b) Alternative and Complementary Reflections	23
(1) Mandatory Time-based Restrictions.....	23
(2) Secure and Customisable Digital Interfaces.....	24
(c) Avenues for Reflection and Priority Areas	26
Priority 1: Create a European standard for the protection of minors online.....	26
Priority 2: Open up platform functionalities, establish a right to customisation, and strengthen algorithmic transparency	27
Priority 3: Rethink the division between “host” and “publisher”	29
Priority 4: Consider the diverse usages of digital services, particularly those involving generative AI.....	30
Priority 5: Strengthen and expand education in digital, media, and information literacy	31

Introduction

On the 26th January 2026, the French National Assembly adopted at its first reading a bill aimed at protecting minors from the risks of social media use.¹ The bill aligns with the government's priority to oversee the digital practices of minors. France has thus joined the international momentum for the regulation of platform use by underage users and is poised to become the first European Union (EU) Member State to implement a ban directly targeting minors' access to social media platforms.

Recent legislative initiatives follow years of relative political inertia, marked by a reluctance to confront the economic power of major platforms and the legal challenges surrounding the regulation of their business models, based on the capture of user attention and the monetisation of data. For example, the proposals of the French "Children and Screens" Commission (la Commission "Enfants et écrans") and the Estates General of Information (*États généraux de l'information*)², which evoked alternatives to current social media platforms, failed to find political momentum.

Fifteen years after the Arab Spring, the verdict is clear: social media platforms, as they function today, are highly mixed tools from a democratic standpoint. They have moved away from the healthy spaces and vehicles of empowerment many hoped for, and expose users—particularly the youngest—to major risks. Despite repeated warnings about the risks they generate and years of dialogue initiatives of all kinds, platforms have not integrated the necessary safeguards. Lacking alternatives, legislators are preparing drastic measures intended to be symbolically strong: banning minors from platforms through the imposition of age verification. It is necessary to acknowledge that this decision is a response to very real immediate needs, yet at the same time this approach is only a partial response to the structural causes of the risks posed by these online services.

This note is structured in three parts: a review of the multifaceted risks encountered by minors online (I), followed by an overview of current/proposed regulations and their limits (II). It concludes with an analysis of the remaining issues in these provisions and provides several propositions for the fundamental rethinking of the regulation of these digital services (III).

In short, whilst banning of minors from social media platforms may seem a solution of last resort, it must not become a substitute for a profound overhaul of digital spaces for the benefit of all users.

¹ Assemblée nationale, [Protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux](#), introduced on November 18, 2025.

² [Rapport des Etats généraux de l'information, Protéger et développer le droit à l'information : une urgence démocratique](#), September 18, 2025.

I. **The Use of Social Media: Multifaceted Risks for Minors Online**

The evidence is unequivocal: social media platforms, as they currently function, expose minors to harmful risks online due to both the content distributed and their specific functionalities, according to the French Agency for Food, Environmental and Occupational Health & Safety (Anses)³. These multifaceted risks were categorised into “5Cs” by the OECD in 2021⁴:

- Content risks: The exposure to inappropriate, violent, pornographic, or hateful content, or content likely to promote eating disorders, self-harm, or even suicidal behaviour.
- Contact risks: Interactions with malevolent adults (predation, grooming⁵) or with peers adopting toxic behaviours (cyberbullying, intimidation, sextortion⁶). Minors may be manipulated, harassed, or exposed to harmful influences.
- Conduct risks: The behaviours adopted by minors themselves, such as excessive sharing of personal information, participation in dangerous challenges (such as viral social media challenges), or engagement in illegal or harmful activities (cyberviolence, distribution of intimate content).
- Consumer risks: The excessive and compulsive consumption of content, capable of disrupting sleep, social relationships, academic performance, and the mental health of minors.
- Cross-cutting risks: This final point covers risks related to the uncontrolled collection, exploitation, and unregulated sharing of minors' personal data. Upon signature of terms of use, platforms can use this data for advertising, profiling, or monetisation, often without the awareness of minors or their parents.

Whilst these risks concern all social media users to some extent, they are particularly acute for minors and are exacerbated by several factors, as shown by multiple studies:

- Increasingly early access to digital services⁷: the average age for account creation in France is 8 years and a half⁸.
- Exposure to traumatic content: 77% of 11-17-year-olds have already encountered disturbing content, 48% of whom regularly, and for a quarter of whom with harmful consequences for their well-being.
- Increasing time spent online: 6-17-year-olds spend an average of 4 hours and 11 minutes per day in front of a screen (outside of school)⁹. Furthermore, 31% of 11-18-year-olds report staying awake or waking up at night to use a screen.
- Anxiety, experienced by 45% of adolescents after consulting social media¹⁰.

³ Anses, « [Usages des réseaux sociaux numériques et santé des adolescents - Connaître, évaluer, protéger](#) », Collective Expert Report, December 2025.

⁴ OECD, « [Children in the digital environment. Revised typology of risks](#) », OECD digital economy papers n° 302, January 2021.

⁵ Grooming refers to “actions taken by a person seeking to establish a relationship of trust with a child (with the aim of eventually arranging a meeting) for sexual purposes”, [Action Innocence](#).

⁶ Sextortion is defined by the French [Ministère de l'Intérieur](#) as the threat to show nude photos or sexual videos of a person to someone else if the person does not do as requested, in exchange for money or other photos or videos.

⁷ Defined by the [European Commission](#) as “intermediary services such as host providers, online marketplaces, and social media networks”.

⁸ Arcom, « [Protection des mineurs : quels risques ? Quelles protections ?](#) », September 25, 2025.

⁹ Report « [Enfants écrans : à la recherche du temps perdu](#) », April 2024.

¹⁰ Ipsos, « [Baromètre du moral des adolescents : un jeune sur quatre fait l'objet d'une suspicion d'un trouble anxieux généralisé](#) », March 14, 2025.

Whilst a causal link is difficult to prove, the KidsRights Index 2025 suggests a “disturbing correlation” between the degradation of minors’ mental health and the excessive and addictive use of social media. It should be noted that whilst video game (and gambling) disorders are internationally recognised as “addictions”, social media—despite featuring “addictive” design elements—are not currently recognised as addictive. The addictiveness of these services is, however, increasingly being considered. In 2023, an Amnesty International report already revealed that TikTok “relied on an addictive design to generate maximum engagement”¹¹. The Children and Screens Commission report argues in this regard for a recognition of social media addiction¹². The European Commission recently acknowledged that TikTok’s algorithm featured addictive characteristics¹³.

Recent judicial decisions in the United States, based on platform design and the role played by user interfaces (rather than content), pave the way for numerous future lawsuits, including in Europe, against platforms. On 24 March 2026, Meta was sanctioned by a civil court in Santa Fe (New Mexico)¹⁴ for violating the state’s consumer protection law by failing to disclose the risks its platforms posed to children. Furthermore, on 25 March 2026, a civil court in Los Angeles (California)¹⁵ found Meta and YouTube liable for negligence, for knowingly designing their products to be addictive to the detriment of the mental health of their young users.

In turn, Anses identifies harmful effects on the health of minors: disrupted sleep, low self-esteem, risky behaviours, and exposure to cyberviolence. The French Audiovisual and Digital Communication Regulatory Authority (Arcom)¹⁶ points to a higher exposure of girls to content promoting eating disorders. In conclusion, for Anses, the verdict is now clear: social media platforms as they exist today are not suitable for young users.

II. **Overview of Regulations on the Protection of Minors Online and Key Associated Questions**

Faced with this alarming verdict, France and a growing number of countries are acting to attempt to address the risks affecting digital platform users, particularly minors. These actions are primarily regulatory, with few structured initiatives offering social media platforms with alternative functioning models.

¹¹ Amnesty International, « ["Je me sens vulnérable" Pris-e au piège de la surveillance intrinsèque à TikTok](#) », 2023.

¹² Report « [Enfants écrans : à la recherche du temps perdu](#) », April 2024, page 46.

¹³ European Commission, « [La Commission conclut à titre préliminaire que la conception addictive de TikTok est contraire à la législation sur les services numériques](#) », February 6, 2026.

¹⁴ Le Monde, « [Meta reconnu coupable de mise en danger de mineurs sur ses plateformes par un tribunal du Nouveau-Mexique](#) », March 24, 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 »](#) », March 25, 2026.

¹⁶ Arcom, « [Protection des mineurs : quels risques ? Quelles protections ?](#) », September 25, 2025.

France:

The Bill Banning Social Media Access for Minors Under 15

The French National Assembly approved on 26 January, at its first reading, for a bill aimed at protecting minors from the risks of social media use, led by MP Laure Miller.

Legislative context of the initiative:

- **2023:** Adoption of the Marcangeli Law¹⁷ aiming to establish a digital age threshold of 15 years, which was not implemented due to non-compliance with European law¹⁸.
- **14 July 2025:** Publication of the guidelines for Article 28 of the Digital Services Act (DSA) on the protection of minors, allowing Member States to define a minimum age threshold for accessing social media platforms.
- **18 November 2025:** Introduction of the bill to Parliament.
- **26-27 January 2026:** Vote on the bill in the National Assembly under the accelerated procedure.

Content of the law:

Platforms concerned:

- The text targets social media platforms in a general sense, as “online social networking services”, as defined by the Digital Markets Act (DMA),¹⁹ and “online platforms” under the Digital Services Act (DSA)²⁰.
- **General exclusions:** Services which offer solely public social functionalities in an incidental manner. *Example:* Any video-sharing platform without public social functionalities. These platforms remain accessible by default.
- **Specific exclusions:** Online encyclopedias, educational or scientific repositories, and open-source software development and sharing platforms. These platforms remain accessible by default.

Mobile phone ban:

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

¹⁸ This law did not comply with the notification deadlines to the European Commission required for legislative proposals concerning “information society services” (platforms, social media) and therefore falls within the scope of Directive (EU) 2015/1535.

¹⁹ The Digital Markets Act “aims to tackle anti-competitive practices by internet giants and address the imbalances arising from their dominance of the European digital market”. For more information: [vie-publique.fr. Digital Market Act \(UE\) 2022/1925](#), article 2 7) “‘online social networking service’ means a platform that enables end users to connect and communicate with each other, share content and discover other users and content across multiple devices and, in particular, via chats, posts, videos and recommendations ”.

²⁰ [Digital Services Act \(UE\) 2022/206](#), article 3 (i) “ ‘online platform’ means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation ”.

- Extension of the mobile phone ban to lycées (schools for ages 15-18 years). It is up to each establishment to introduce the ban into its internal regulations and to adjust it according to the school's specific uses.

Relationship with EU law: The European Commission has confirmed France's competence to ban social media platforms for those under 15 years²¹, while specifying that solely the Commission can impose additional obligations on Very Large Online Platforms (VLOPs).

Oversight and monitoring: Arcom will be responsible for ensuring compliance with the ban and will have the role of:

- Monitoring compliance with the age threshold on social media platforms established in France or outside the EU;
- Referring cases to origin Member States for services established in the EU but outside France;
- Referring cases to the European Commission or competent national authorities in the event of failure by platforms to verify age, in accordance with the DSA.

Sanctions: In case of non-compliance, the European can impose sanctions of up to 6% of the annual global turnover of the previous financial year under the DSA.

Next steps:

- Notification procedure launched with the European Commission, the results of which are still pending; meanwhile the *status quo* for three months²².
- First reading by the Senate Culture Commission on 25 March 2026.
- Debate in the Senate²³ in a public session from 31 March, under the accelerated procedure.

At the European level, in November 2025 the Parliament adopted a calling for a minimum age of 16 for access to social media platforms, video-sharing platforms, and AI companions within the EU, whilst allowing access for 13–16-year-olds provided they have parental consent. Meanwhile the European Commission has convened a panel of experts²⁴ to assess ways to strengthen the legal protection of minors beyond the DSA.

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

²² In accordance with Directive (EU) 2015/1535, Member States must notify the Commission of any draft technical regulation prior to its adoption. From the date of notification of the draft, a three-month standstill period begins – during which the notifying Member State may not adopt the technical regulation in question – allowing the Commission and the other Member States to examine the notified text and respond appropriately. For more information: [website of the European Commission](#).

²³ Sénat, [Ordre du jour des prochaines séances du Sénat](#), February 18, 2026.

²⁴ European Commission, « [La Commission tient la première réunion du groupe spécial sur la sécurité des enfants en ligne](#) », March 5, 2026.

These initiatives are not isolated and form part of an international movement for the regulation of digital services with the aim of improving the protection of minors online. The Australian case, a pioneer in the matter, has been widely highlighted, but measures have also been taken in the United Kingdom, China, California, and are being defined elsewhere, such as in Spain²⁵, Portugal²⁶, Norway²⁷, Denmark²⁸, Austria²⁹, and Slovenia³⁰.

Australia: The Australian Online Safety Act³¹

Australia became the first country in the world to implement a ban on social media access for minors under 16 years. This measure was introduced in November 2024 via the Social Media Minimum Age amendment³², modifying the *Online Safety Act 2021*. The text entered into force on 10 December 2025.

The text requires social media platforms to “take reasonable steps” to ensure they are only accessible to users over the age of 16, whether they are new or already registered. Existing accounts belonging to those under 16 must therefore be deactivated or deleted. The ban does not specify which technical measures platforms should prioritise in order to comply with the law, thereby setting an objective of results rather than means.

Furthermore, and notably, the obligation applies to a restricted list of social media platforms officially designated in November 2025. The platforms concerned are Facebook, Instagram, Reddit, Snapchat, TikTok, Twitter, Threads, Twitch, Kick, and YouTube.

Platforms that do not comply with these obligations face fines of up to 50 million Australian dollars (approximately 30.7 million Euros) imposed by the eSafety Commissioner and the Office of the Australian Information Commissioner (OAIC).

Whilst long-term data is currently lacking, many accounts of users under 16 have been deleted. One month after the law came into force, Australia had already recorded 4.7 million accounts deactivated, restricted, or deleted by the 10 concerned platforms³³. However, this figure should be put into perspective: 2.5 million 8–15-year-olds each own several accounts on different platforms. Users under 16 can download and save the content of their accounts, which will be deactivated until they turn 16. They will then be able to retrieve it.

²⁵ Contexte, « [L’Espagne se lance à son tour dans l’interdiction des réseaux sociaux \(aux moins de 16 ans\)](#) », February 4, 2026.

²⁶ El País, « [Portugal avanza para controlar el acceso de los menores a las redes sociales](#) », February 2, 2026.

²⁷ 20minutes, « [La Norvège souhaite interdire les réseaux sociaux aux moins de 15 ans](#) », October 25, 2025.

²⁸ Contexte, « [Le Danemark aux avant-postes sur la majorité numérique](#) », October 9, 2025.

²⁹ France Info, « [L’Autriche va interdire les réseaux sociaux aux moins de 14 ans](#) », March 27, 2026.

³⁰ Contexte, « [La Slovénie, nouveau candidat à la majorité numérique](#) », February 6, 2026.

³¹ [Online Safety Act](#), 2021.

³² Australian Government, [Social Media Minimum Age](#).

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»](#) », January 25, 2026.

In case of error, users can challenge an account deactivation decision with the platform. For this, they must provide an official ID or a facial video to the social media platform in order to confirm their age.

The preliminary question facing the legislator is defining an age threshold below which the user cannot access certain digital services, a measure which generates significant debate.

The proposal for a “digital majority” in France follows this logic. As shown, an age threshold of 15 years was set in French law in 2023³⁴, but due to the lack of an implementing decree and European Commission approval regarding its compliance with EU law, it was not applied. The Commission's doctrine has evolved with the publication of its guidelines³⁵, which now allow Member States to set age thresholds. The French State Council (*Conseil d'État*) in its opinion³⁶ on the bill proposes a hybrid system where social media services remain accessible online for minors under 15 with parental authorisation.

In the **United States**, the Children's Online Privacy Protection Act (COPPA) sets the minimum age at 13 for the collection of personal data without parental consent. This threshold is widely adopted by international platforms as the limit for account creation.

Within the EU, the GDPR provides a minimum age of 16 for minors to consent to the processing of their personal data. However, Member States can adjust this threshold. Ireland has thus established it at 13 years and France at 15 years.

These differences of chosen age threshold testify to the complexity of defining a threshold and their variability according to the conditions in which they apply.

Beyond the choice of threshold, regulations aiming to protect minors online face several methodological questions:

- What is the legal scope of application? (a.)
- Which age verification method should be implemented, considering potential workarounds and harmful effects? (b.)
- Which content should be subject to regulation? (c.)

These different variables will now be analysed and illustrated by examples of regulations and initiatives implemented by the platforms.

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

³⁵ European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#).

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

(a) What is the scope of application?

When a scope is defined, the challenge lies in choosing between a targeted regulation—at the risk of drifting toward case-by-case oversight—and a global approach, which may encounter enforcement difficulties.

(1) Regulations targeting specific categories of digital services

Some countries have chosen to target specific platforms, such as **Australia**, where only platforms qualified as “social media platforms” and named specifically are subject to legislation. The inclusion of YouTube (and not YouTube Kids), for example, sparked numerous debates regarding the qualification of the service as a social media platform. The platform was ultimately included for its “inappropriate content” and “predatory algorithms,” according to the terms of the country’s minister for Communications, Anika Wells.

However, the restrictive delimitation of the scope raises questions regarding the objectives pursued by the text: many other digital services can present risks for under 16s, such as private messaging and online video games. To cite just one example, the network video game Roblox is not subject to this text. Yet, of its 111.8 million daily active users³⁷ worldwide, half are under 13. Furthermore, the platform features social functionalities similar to those of social media: personalised profiles, the construction of a friend network, a chat for communicating with other users, etc. Risks are equally present: the research firm Hindenburg Research qualified the platform as a “pedophile hellscape for children”³⁸ whilst demonstrating the presence of around fifty groups with more than 100,000 members exchanging child abuse content and soliciting sexual acts from minors.

Faced with this indicative list, there is a real risk of a shift to other more obscure platforms, or even to new platforms created following the entry into force of the law. Whilst it is still too early to measure these potential shifts, certain trends are revealing. Adolescents report spending more time playing video games or communicating with friends via other channels such as WhatsApp or Messenger³⁹ since the ban came into force. Other alternative platforms recorded an increase in downloads, particularly competitors with smaller audiences such as Bluesky, Yubo (a French community platform), and Lemon8, a video platform similar to TikTok and owned by the same parent company, ByteDance⁴⁰. This increase remains limited, however, as after recording a peak of 25,000 daily downloads in the days following the ban, downloads of banned social media platforms returned to their usual levels ten days later⁴¹.

³⁷ Statista, [Utilisateurs actifs quotidiens du jeu 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"](#) », October 14, 2024.

³⁹ BBC, “[Australia social media ban: Teens share their views one month on](#)”, January 9, 2026.

⁴⁰ Financial Times, “[Social media companies purge 4.7mn accounts after landmark Australia ban](#)”, January 16, 2026.

⁴¹ Apptopia, dans BBC, “[Australia social media ban: Teens share their views one month on](#)”, January 9, 2026.

On 6 March 2026, the eSafety Commissioner announced⁴² the launch of new online safety codes aimed at ensuring that children have age-appropriate online experiences and are not exposed to harmful content. This complementary step, targeting content this time rather than platforms, marks a new stage in the Australian framework. High-impact violent content, pornography, and content promoting suicide, self-harm, and eating disorders are targeted. These codes will also cover AI-powered companion chatbots to prevent them from engaging in sexually explicit conversations with minors or encouraging self-harm and suicide, app stores for preventing the download of applications categorised 18+, adult messaging services specialised in the distribution of targeted content, online games rated 18+, search engines when searches concern the targeted content, and social media services that allow access to targeted content.

Conversely, France targets “online social media services provided by an online platform”⁴³, without providing a restrictive list but discriminating according to their functionalities, i.e. when they allow communication between users.

Targeting only certain digital services, restrictively or otherwise, risks not being unable to monitor and sanction other platforms whose content may nevertheless be harmful because they do not fall within the scope of the law. The Australian example, which appeared ambitious at the time of the vote, now seems to show its limits as many other risky platforms remain accessible, rapidly making an expansion by content type necessary.

(2) Regulations creating new obligations for digital services based on the number of users

The scope of application can also vary based on the number of users, a distinction notably made by the DSA, which constitutes an “asymmetric” regulation the obligations of which vary according to the nature of the services and their size. The regulation distinguishes four categories of online platforms: (i) “Very Large Online Platforms” (VLOPs) with more than 45 million monthly users in the EU, (ii) internet service providers, (iii) cloud computing services, and (iv) online platforms such as marketplaces, social media platforms, content-sharing platforms, and travel and accommodation platforms.

Overall, all categories of platform must combat illegal content, be more transparent about content moderation and the functioning of their algorithms, and must not provide targeted advertising to minors. VLOPs are subject to other more restrictive measures to mitigate the risks they may generate.

Regardless of the chosen scope, criticisms emerge in their definition. Regulations may seem too restricted or too broad. Therefore, some highlight the need for a global regulation of digital services in all their diversity, as illustrated, for example, by the European Parliament's official position. The latter calls for regulating social media platforms, video platforms, and “AI

⁴² eSafety Commissioner, *Online safety codes introduce real-world protections for children online*, March 6, 2026.

⁴³ [Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux](#), adopted by the Assemblée Nationale at first reading on 26 January 2026.

companions” simultaneously. While this vision seems necessary at a time when usage is evolving and shifting, the challenge lies in formulating provisions that can apply to services as diverse as these, the functioning and uses of which can differ greatly. It now appears necessary to regulate digital uses beyond social media platforms, without waiting for uses to become too established and lead to a proliferation of unacceptable risks (see *supra* II, point 2).

(b) Which age verification methods are possible and what workarounds or harmful effects are present?

Protection measures often combine age verification, access bans, time limits, and adapted interfaces. Age verification frequently constitutes a prerequisite for implementing other complementary measures⁴⁴. In the DSA, age verification measures are deemed appropriate only when no other means can mitigate risks.

(1) Different age verification methods and their applications

User age verification has widely become the prerequisite for policies on the protection of minors in the digital space. It involves verifying, in a reliable and secure manner, that access to certain content, functionalities, services, or platforms is limited to authorised audiences based on their age.

The European Commission⁴⁵ distinguishes three methods of age verification:

- **Self-declaration:** The most widespread method, where the user indicates their age or confirms their age range, “either by voluntarily providing their date of birth or age, or by declaring that they are over a given age.” This method has proven ineffective and easy to bypass. A study conducted by Arcom⁴⁶ in 2025 reveals that nearly two-thirds of young people surveyed (62%) admit to having already lied about their age to register on a platform. The main reason cited was that they were not yet of the required minimum age (65%).
- **Age estimation:** Little used, it allows “a provider to determine that a user is likely to be a given age, to fall within a certain age range, or to be older or younger than the given age.” On a practical level, age can be estimated by facial recognition, which requires the collection of biometric data. Age can also be estimated by cross-referencing usage data (consumption habits, time spent on certain content, voter registration, purchases, etc.) with declared personal data (email address, full name, etc.). This method is considered the least reliable in an Australian government report⁴⁷.

Separately, YouTube has been testing an artificial intelligence (AI) tool since August 2025 to estimate its users' age in the United States, with the aim of protecting minors. This tool aims to deduce user age, without taking into account the date of birth declared during account

⁴⁴ This technique is recommended or implemented in many countries, including Australia, China, Malaysia, Turkey, Kenya, Pakistan, Papua New Guinea, New Zealand, Texas, Papua New Guinea, Kenya and Malaysia.

⁴⁵ European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#), paragraphs 28 et 29.

⁴⁶ Arcom, « [Protection des mineurs : quels risques ? Quelles protections ?](#) », September 25, 2025.

⁴⁷ Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, “[Age Assurance Technology Trial— Final Report](#)”, August 31, 2025.

setup, to offer “tailored experiences and protections”⁴⁸, according to the platform. As soon as the tool identifies a user as a minor, advertising will no longer be personalised, and restriction and safety measures will be implemented. If a user believes the age estimation is incorrect, they can provide an official ID to verify their age. If the experiment proves successful, the tool could be rolled out beyond the United States.

In **Australia**, the chosen threshold is 16 years for social media access, regardless of the method chosen by platforms to achieve this objective. This choice may implicitly reflect the observation that platforms already possess sufficient data to infer user age without needing to verify it precisely, even if this estimation may have limits (see *infra*).

Furthermore, the number of users who have bypassed the measure has not yet been reliably estimated. However, the eSafety Commissioner, Julie Inman Grant, told the BBC that a series of notices of concern regarding anomalies and weaknesses in the implementation of the ban is about to be sent to companies⁴⁹. Snapchat, many of whose users are minors, is notably targeted as the social media platform uses age estimation methods based on facial recognition without verifying that they are real images⁵⁰.

The new online safety codes announced in March 2025 specify, moreover, that age verification will be required, as self-declaration was deemed too ineffective⁵¹.

- **Age verification using “physical identifiers or verified identification sources”** is increasingly being discussed by legislators⁵². It relies on an item proving age which has been certified and issued with reference to official documents.

In France, the Law to Secure and Regulate the Digital Space (SREN)⁵³ of May 2024 requires services distributing pornographic content to implement a user age verification system. The text directs Arcom to “establish and publish [...], after an opinion from the National Commission for Information Technology and Civil Liberties (CNIL), a reference framework determining the minimum technical requirements for age verification systems. These requirements should relate to the reliability of user age verification and respect for their privacy”⁵⁴. Following work jointly conducted by the CNIL and the interministerial Centre of Expertise for Digital Platform Regulation (PEReN), a technical reference framework was published in October 2024. The framework does not aim to certify technical solutions but leaves “the regulated services distributing pornographic content [...] free to choose the

⁴⁸ AFP, « [YouTube va deviner l'âge des utilisateurs grâce à l'IA](#) », August 14, 2025.

⁴⁹ BBC, « [Social media firms have come to ban 'kicking and screaming', says Australia eSafety boss](#) », January 23, 2026.

⁵⁰ The Guardian, « [Snapchat blocks more than 400,000 Australian accounts but warns of 'significant gaps' in under-16s social media ban](#) », February 1st, 2026.

⁵¹ eSafety Commissioner, *Online safety codes introduce real-world protections for children online*, March 6, 2026.

⁵² In particular, in the United Kingdom, Australia, China, Malaysia, Turkey, Kenya, Pakistan, Papua New Guinea, New Zealand, as well as in certain states of the United States.

⁵³ [Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique](#), known as the « SREN » Act.

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](#), October 2024.

solutions for the protection of minors that they prefer, provided they respect the technical requirements of the reference framework”.

Today, seventeen pornographic sites have been specifically identified and obliged to immediately implement robust age verification systems that protect personal data whilst preventing minors from accessing targeted content. Several solutions have been implemented by these sites, such as the sending a photo or short video capture of the user’s face which is then analysed by AI, or the sending of a copy of an identity document. These solutions are inconsistent with the protection of personal data, which are collected by the platforms.

Other EU countries have implemented similar obligations, such as Spain, Germany, Denmark, and Italy. European Commission guidelines, taken in addition to Article 28 of the DSA⁵⁵, help strengthen this approach by imposing mandatory age verification for access to pornographic sites or platforms throughout the Union.

The **United Kingdom** Online Safety Act (OSA) requires services hosting content harmful to minors to implement age verification through the uploading of an identity document accompanied by a facial image of the user, the use of a digital wallet, or recourse to banking services, amongst other means.⁵⁶ The platform Pornhub subsequently announced, after having recorded a 70% drop in traffic in the UK, that it would prevent new users from accessing its site as a result of the OSA.⁵⁷

Digital wallets are also used in **Papua New Guinea** via the government application SevisPassWallet, where users store their digital credentials.⁵⁸ Designed as a Digital Public Infrastructure (DPI), this digital wallet allows users to log into online public services, open bank accounts, and register mobile SIM cards.

At the European level, further discussions are also underway on the European Digital Identity Wallet (EUDI Wallet). The objective is to provide every citizen and business with a means of digital identification recognised within the EU that is interoperable, secure, and respectful of the protection of personal data. Each Member State must offer at least one EUDI Wallet to citizens, residents, and businesses by the end of 2026. These tools will notably be able to be used to prove age. The European Commission has launched a pilot application using the wallet framework to verify users’ age for access to social media platforms in five Member States, including France.⁵⁹ The application is based on a European prototype that each of the five

⁵⁵ European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#).

⁵⁶ Ofcom, [“Age checks for online safety – what you need to know as a user”](#), June 2025.

⁵⁷ The Guardian, [“Pornhub to stop new UK users accessing site from next week”](#), January 27, 2026.

⁵⁸ Department of Information And Communications Technology, [“Presentation - PNG eGov Portal”](#), October 2024.

⁵⁹ Le Monde, [« Cinq pays européens, dont la France, vont tester une application pour vérifier l’âge des utilisateurs sur Internet »](#), July 14, 2025.

Member States can modify according to the rules in place on their territory, with the aim of proposing modified national versions within a few months.

(2) Underlying issues with age verification

Beyond the question of the minimum age threshold, it can also be questioned whether a single, uniform rule is appropriate. A multidisciplinary consensus⁶⁰ agrees that it is necessary to consider the needs of the child “in light of their age, level of development, and individual characteristics.” The need for protection therefore varies according to age, but also the degree of maturity, which is not necessarily correlated to age, as well as digital habits.

These questions reflect the debates in France on the definition of an age threshold. On one hand, some political groups have questioned the choice of a threshold at 15 years proposed by the bill, given that the current access threshold for social media platforms is 13 years (primarily set in General Terms of Use). Arcom monitors compliance with this threshold while noting that 44% of young people access social media before the age of 13.⁶¹

On the other hand, the choice of the threshold at 15 years in France is aligned with the age of sexual consent, the age at which it is possible to consent to personal data collection under the GDPR without parental input, in addition to the age for entry into an apprenticeship contract, to receive a salary, and to consult a doctor without parental authority, etc. Finally, experts from the Children and Screens Commission recommend banning social media for minors under 15 years, as it “most often corresponds to the transition to high school (lycée), which represents an important stage in adolescence and the young person's journey toward progressive autonomy”.⁶²

Others argue that banning access before a certain age may prove counterproductive by denying young people a progressive and supervised introduction to digital environments. Psychiatrist Serge Tisseron warns that the impact will be greater, as “discovering social media after 15 offers no protection”⁶³. The European youth-led digital rights movement “ctrl+alt+reclaim” also believes that “bans do not prevent the harms of social media platforms”⁶⁴. Postponing access could expose adolescents to a sudden and unprepared immersion in a complex environment where they must manage their online image, social interactions, and exposure to varied content without having benefited from a gradual experience to develop their critical thinking and their use of the tools and settings available.

⁶⁰ [Démarche de consensus sur les besoins fondamentaux de l'enfant en protection de l'enfance](#), Report submitted by Dr. Marie-Paule Martin-Blachais to Laurence Rossignol, Minister of Families, Children, and Women's Rights, February 28, 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](#) », September 25, 2025.

⁶² Report « [Enfants écrans : à la recherche du temps perdu](#) », April 2024.

⁶³ Le Monde, « [Serge Tisseron, psychiatre : « Découvrir les réseaux sociaux après 15 ans ne protège de rien »](#) », January 7, 2026.

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 »](#) », January 25, 2026.

Some platforms capitalise on this debate to evade their responsibilities, advocating device-level age verification⁶⁵ during app store account creation or via the operating system. Platforms present this solution as simpler for users and digital actors, less prone to circumvention, and more robust by harmonising the verification systems used, along with the associated guarantees in terms of reliability and the protection of personal data. However, this option appears too extensive given the small number of applications actually requiring age verification.⁶⁶ It could also lead to platforms and app developers shirking their obligations, when they must remain involved in risk reduction. Furthermore, this system is poorly compatible with shared digital devices used by multiple users of different ages within a household.

(3) The risk of bypassing age verification

- **Intentional Bypassing**

From a technical point of view, verification methods are susceptible to circumvention. The use of VPNs⁶⁷ is among the most widespread methods. For instance, downloads of Proton VPN saw a 1,000% increase in France⁶⁸ following the implementation of age verification on adult sites. However, this figure should be put into perspective, as the measure did lead one in four French people to reduce their consumption of pornographic content. 10% even claimed to have completely abandoned pornographic sites—a figure reaching 20% among 18-24-year-olds. Whilst the reduction in consumption appears to be a qualified success, VPN use remains the preferred means for 60% of those surveyed. Additionally, 30% of 18-24-year-olds have turned to other platforms outside the scope of the measure⁶⁹.

In the **United Kingdom**,⁷⁰ despite a profusion of press headlines regarding VPN usage, a direct link between the introduction of bans and increased VPN usage has not been proven. Ofcom observed that despite an initial peak of 1.5 million daily active users following the ban on pornography for minors and age verification devices for certain social media platforms in July 2025, usage quickly fell below 1 million by October.⁷¹ Furthermore, the UK Safer Internet Centre suggested that this increase was principally due to adults concerned about their online anonymity.⁷²

⁶⁵ Euractiv, « [Meta demande une réglementation européenne sur la vérification de l'âge pour l'utilisation des réseaux sociaux](#) », November 5, 2025 ; Next, « [Vérification d'âge : Pornhub appelle Apple, Google et Microsoft à l'intégrer aux appareils](#) », November 21, 2025.

⁶⁶ 01net, « [Tim Cook en croisade contre la vérification d'âge obligatoire sur l'App Store](#) », December 11, 2025 ; France 24, « [Vérification de l'âge en ligne : Google opposé à tout contrôle au niveau des boutiques d'applications](#) », June 13, 2025.

⁶⁷ A virtual private network (VPN) is an overlay network that uses network virtualization to extend a private network across a public network, such as the Internet, via the use of encryption and tunneling protocols. In a VPN, a tunneling protocol is used to transfer network messages from one network host to another.

⁶⁸ « [Les VPN contournent la nouvelle réglementation de l'Arcom sur les contenus pour adulte](#) », October 15, 2025.

⁶⁹ The Verge, « [The UK is slogging through an online age-gate apocalypse](#) », July 28, 2025.

⁷⁰ Ofcom, « [Online Safety in 2025](#) », December 4, 2025.

⁷¹ UK Safer Internet Centre, « [Young People's Use of VPNs](#) », December 1st, 2025.

⁷² UK Safer Internet Centre, « [Young People's Use of VPNs](#) », December 1st, 2025.

Beyond VPNs, some users turn to other methods, such as the black market for verified accounts,⁷³ where accounts verified as belonging to users over 16 years can be bought and sold.

Amongst other examples, a BBC article cites the case of an adolescent who used a photo of her mother to access Snapchat after the social media platform announced her account would be blocked upon the entry into force of the Australian law.⁷⁴

- **Difficulties of inclusivity and accessibility**

Age verification based on identity documents risks excluding the most vulnerable minors. UNICEF⁷⁵ warns that civil registration systems in many countries are incomplete or patchy. Millions of minors lack official proof of identity. These minors would thus be doubly penalised: victims of digital exclusion and deprived of protection measures which rely on the verification of age, reinforcing inequalities. In France, holding an identity document is not mandatory.

At the same time, age verification mechanisms must be accessible to people with disabilities, particularly those with impaired or weak vision, and comply with national accessibility standards,⁷⁶ ensuring compatibility with assistive technologies and providing alternatives to CAPTCHAs or other procedures depending solely on vision. Without such measures, these procedures would exacerbate the vulnerabilities of minors with disabilities, for whom the barriers of access to digital technologies would be reinforced under the guise of protection.

(c) What content is targeted by the legislation?

Some texts target specific categories of content due to the risks they pose to certain audiences deemed “vulnerable”, whilst others take a broader approach, encompassing various categories of content.

(1) Regulations targeting specific categories of content

Both French and British approaches have opted to target content deemed harmful. In France, the SREN Law aims, amongst other measures, to implement age verification for access to pornographic content.

In the **United Kingdom**, the OSA requires social media platforms and search engines to implement age verification measures to prevent minors from accessing content classified as “dangerous,” which includes pornographic content as well as material involving violence, self-harm, and eating disorders.

⁷³ Financial Times, “[The countdown to the world’s first social media ban for children](#)”, December 2025.

⁷⁴ BBC, “[Can you ban kids from social media? Australia is about to, but some teens are a step ahead](#)”, December 6, 2025.

⁷⁵ UNICEF, “Digital Age Verification: Risks and Opportunities for Children”, 2023.

⁷⁶ Center for Democracy and Technology, “[Mitigating risk to rights with age verification : Privacy-preserving guardrails that should accompany deployments of age verification approaches](#)”, October 10, 2025.

These regulations have the advantage of directly targeting certain risks to which minors are particularly exposed. However, their implementation can prove difficult as they require a high degree of adaptability in how they are implemented across different platforms and, crucially, significant resources for content moderation (see below), which still largely depends on the goodwill of the platforms themselves.

(2) Regulations adopting a risk-based approach

Other texts have a broader scope, such as the EU **Digital Services Act (DSA)** mentioned above, which adopts an approach based on the risks presented by digital platforms rather than the nature of the content itself. The protection of minors online is among the text's primary objectives and was specifically addressed in guidelines⁷⁷ published by the European Commission in July 2025. These establish a non-exhaustive list of proportionate and appropriate measures to protect minors against online risks such as grooming, exposure to harmful content, problematic and addictive behaviours, as well as cyberbullying and harmful commercial practices. They also recommend the use of age assurance methods, provided they are accurate, reliable, robust, non-intrusive, and non-discriminatory.

Trusted flaggers play a complementary role to that of regulators and platforms. Established by the **DSA**, this status includes associations, government agencies, and groups of experts tasked with detecting potentially illicit content. Their reports are treated with priority by platforms. These entities are designated by national Digital Services Coordinators, including **Arcom** in France. Some specifically target the protection of minors, such as the association *e-Enfance / 3018*⁷⁸, the first trusted flagger officially designated in France, which fights against harassment and digital violence targeting young people.

III. **What Digital Future for Young People?**

In the early 2010s, social media platforms were perceived as tools for democracy, freedom of expression, social bonding, and empowerment. Fifteen years later, it is clear that dominant social media platforms, with business models based on the capture of attention and the concentration of ownership, have mutated into spaces that promote the polarisation of ideas and toxic content, carrying major systemic risks, especially for young users.

This failure also extends to the regulation of these platforms. Having been searching for solutions for the past fifteen years, regulation has for too long focused on the legality of content while neglecting the role of algorithms. Regulation has been too heavily entrusted to the goodwill of the platforms through voluntary initiatives and "codes of conduct" with limited reach and effectiveness. It is also worth asking whether spaces that still respect the original promises are possible today, and how their development can be enabled.

Whilst regulatory efforts have intensified in Europe in recent years, online risks have not decreased, in particular for the youngest users who are now being barred from social media platforms.

⁷⁷ European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#).

⁷⁸ For more information: <https://e-enfance.org/>.

However, age verification alone is not enough to address all the challenges and risks related to the protection of minors, nor to guarantee a safer digital life for all users. Beyond the circumventions and technical questions detailed previously, it is important to remember that minors must be able to find the tools and means online to empower themselves safely (a). In addition to age verification, alternative methods for protecting minors deserve to be highlighted to enrich the debate (b). Finally, the debate on the protection of minors online must not overshadow the structural issues that most current regulations tend to neglect (c).

(a) How can we strengthen the fundamental rights of minors online?

The European Commission recalls in its guidelines on Article 28 of the DSA⁷⁹ that protection measures for minors on online platforms must be appropriate and proportionate to users' rights, meaning they must not infringe upon the exercise of minors' rights online.

(1) Investing in Online Empowerment

The UN Convention on the Rights of the Child (UNCRC) sets out the fundamental rights that minors enjoy and can exercise alone in the digital space. These rights are grouped into four categories by the Child Rights International Network⁸⁰: (i) the right to access information and the right to education, (ii) the right to privacy and the right to be forgotten, (iii) the right to freedom of expression and the right to be heard, and (iv) the right to be protected from abuse.

In **Australia**, for example, the measure banning access to under 16s has already been subject to a High Court challenge brought by minors, supported by the Digital Freedom Project, arguing a violation of their right to access political communications.⁸¹ This example shows that users' fundamental rights are (and must be) central and reaffirmed.

The right to information (Articles 17, 23, 24, and 28 of the UNCRC) is at the heart of the debate, as digital technology has fundamentally disrupted how information is consumed. 49% of minors say they use social media to stay informed.⁸² In France, for example, HugoDécrypte is the most cited information source amongst respondents in the 2024 Reuters Report⁸³, ahead of Le Monde, Le Figaro, and Libération combined, which is particularly the case amongst minors. The challenge is therefore to protect minors without cutting off their primary means of accessing information.

As it stands, the French bill allows minors under 15 years to continue accessing news applications and messaging services which include information channels, but without being able to interact with the general user base.

⁷⁹ European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#).

⁸⁰ Child Rights International Network, [Briefing : Children's rights in the digital age](#).

⁸¹ BBC, ["Teens launch High Court challenge to Australia's social media ban"](#), November 2025.

⁸² Fondation pour l'Enfance, [Baromètre « Enfance & Numérique »](#), February 16, 2026.

⁸³ Reuters, [Digital News Report](#), 2024.

Historically, social media has been a space for social interaction and socialisation in a context where a growing number of young people report suffering from loneliness and isolation. The WHO Commission on Social Connection shows that 13–29-year-olds are the most affected by loneliness, a percentage even higher amongst adolescents.⁸⁴

At first, digital spaces were primarily used as vehicles for the freedom of expression. Social media platforms have also served as political spaces for young people in the face of repression.⁸⁵ Their power was demonstrated notably during the “Arab Spring,” where these services, still in their infancy, played a role as amplifying echo chambers, bringing together protesters and spreading their messages beyond borders. These movements “marked the dramatic entry of politics into the digital age, revealing a disturbing truth: for every tool of empowerment, there is a counterpart of repression”.⁸⁶

Whilst the democratic promise of social media is now less perceptible due to the evolution of their business models, the banning of minors could push them towards other, less controllable digital services,⁸⁷ which are regulated to a lesser extent, or toward new platforms hosting illicit content. Generative AI, for instance, is being highly used amongst young people for personal use: 6% of young people use AI to confide in or to ask for personal advice⁸⁸. AI companions reinforce this phenomenon as they are designed to simulate interpersonal or emotional interaction, accelerating the trend toward the increased anthropomorphisation of chatbots.

The challenge is therefore twofold: firstly, to build healthier digital spaces for our children, and secondly, researchers like Serge Tisseron insist on the necessity of offering alternative social spaces to social media platforms, such as by opening school playgrounds or gymnasiums at weekends,⁸⁹ to allow adolescents to meet and extend their social interactions outside of school. This recommendation is equally shared by the Children and Screens Commission.

(2) Strengthening Personal Data Protection

Age verification methods can present risks in terms of personal data collection, depending on the method used.

The collection of personal data is particularly problematic if sensitive data, such as biometric data, is collected via age verification methods based on facial recognition, especially if the user's specific consent is not obtained. If age verification relies on the submission of an identity document, data other than the user's age such as their name and surname, sex, address, place of birth, etc. will be transmitted even though these are not necessary to ensure a user is above

⁸⁴ OMS, [De la solitude aux liens sociaux](#).

⁸⁵ Cohen Jared. *Children of Jihad: a young American's travels among the youth of the Middle East*. Penguin, 2007.

⁸⁶ Fondation Jean Jaurès, « [Entre rues et réseaux : les printemps arabes, laboratoire d'un numérique politique](#) », September 11, 2025.

⁸⁷ L'ADN, « [Anne Cordier : « Avec l'interdiction des réseaux sociaux, les jeunes deviennent une population à contrôler plutôt qu'à éduquer »](#) », November 13, 2025.

⁸⁸ Ifop, [Les jeunes et l'IA en 2025](#), November 2025.

⁸⁹ Le Monde, « [Serge Tisseron, psychiatre : « Découvrir les réseaux sociaux après 15 ans ne protège de rien »](#) », January 7, 2026.

a certain age. Furthermore, such a measure is often considered invasive and unreliable, as shown by a report from the *Center for Democracy and Technology*⁹⁰.

The European Commission is expected to release its conclusions shortly on the pilot scheme for age verification (without data transmission to the platform) for adult sites, thereby determining if personal data collection can be reduced and further secured using the European age control tool.

In this respect, France is aligned with the European protection strategy with the development of *France Identité*, which complies with the **EUDI Wallet** framework (mentioned above). This tool is secure because the site requiring age verification only receives a signal (positive or negative) indicating whether the user is above or below the required age threshold. No personal information is transmitted to the digital service.

(3) Consolidating and Diversifying the Education of Minors

For digital spaces to remain places of empowerment, socialisation, and information, it is essential to provide greater support for minors in their use of platforms and to raise awareness of the risks involved. Arcom's study on the risks to which minors are exposed shows that 11-17-year-olds are aware of the risks and welcome support in their use and better protection⁹¹.

The ctrl+alt+reclaim collective⁹² describes a “false dilemma” presented by the French bill to ban access to social media for under 15s, between “being deprived of digital spaces for exchange and learning or exposed to the devastating effects of algorithms.” These young people, who feel left out of debates that primarily concern them, believe that “education on the critical use of digital technology is a necessity, from childhood and throughout life.”

This education must first allow them to understand the functioning of platforms (algorithms, data collection, dark patterns, etc.) in order to utilise the settings and limit risks as much as possible. Secondly, it must equip them with the right instincts: to cross-reference information sources, to identify algorithmic biases, and to develop critical thinking towards content. It is also vital to better understand the configuration and personalisation options already available on these services to ensure a safer experience. However, studies show that while young people have a theoretical awareness of the dangers,⁹³ their actions remain poorly adapted to the risks (excessive sharing of personal data, unregulated screen time, resharing of misinformation, etc.).

As stated by the French National Advisory Ethics Council for Health and Life Sciences (CCNE) and the French National Advisory Council for Digital Ethics (CCNEN)⁹⁴: “the objective to be reached must therefore be to support them so that they develop their critical thinking and

⁹⁰ Center for Democracy and Technology, “[What Kids and Parents want: Policy Insights for Social Media Safety Features](#)”, November 19, 2025.

⁹¹ Arcom, « [Protection des mineurs : quels risques ? Quelles protections ?](#) », September 25, 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 »](#) », January 25, 2026.

⁹³ Arcom, « [Protection des mineurs : quels risques ? Quelles protections ?](#) », September 25, 2025.

⁹⁴ Joint statement by the CCNE and the CCNEN, « [Les jeunes face aux réseaux sociaux numériques : le questionnement éthique face à une menace confirmée](#) », February 2026.

progressive digital autonomy. Freedom does not mean the absence of rules, but the capacity to make informed choices concerning one's health, particularly mental health.”

Integrated public policy solutions are already in place, such as in Finland, where the Media Literacy for All program⁹⁵ trains students from the age of 7 to understand digital media, with measurable results on their resilience to disinformation. This initiative is coupled with wider work on developing critical thinking at primary and secondary school, where children learn about propaganda mechanisms and how statistics can be manipulated.

France is gradually moving in this direction. Media and Information Literacy forms part of the national school curriculum. The French Centre for Media and Information Literacy (CLEMI, Centre pour l'éducation aux médias et à l'information) is responsible in France for media and information training across the education system. However, these mechanisms alone are not enough to develop robust digital critical thinking and resilience.

(b) Alternative and Complementary Reflections

Some countries and platforms propose alternative methods to age verification: device-level verification (1), mandatory disconnection periods (2), and secure digital interfaces (3).

(1) Mandatory Time-based Restrictions

Some legislations provide for mandatory disconnection periods to reduce exposure and decrease addictive behaviours. Such measures require age verification, regardless of the method chosen.

This technique is not new; it was implemented in **South Korea**⁹⁶ between 2011 and 2021, from midnight to 6 a.m. The measure was lifted due to its narrow scope, targeting only online games. A similar measure is currently in force in China with a “minor mode”⁹⁷ blocking access between 10 p.m. and 6 a.m. and setting time limits based on age group.

In **California**, the Protecting Our Kids from Social Media Addiction Act (2024) prohibits “addictive feeds” by default for minors and sets a default time limit of

⁹⁵ This is Finland, “[Finland promoted media literacy as civic skill](#)”, 2023.

⁹⁶ [Youth Protection Revision Act](#), May 2011.

⁹⁷ For more information: France Inter, « ["Réduire la dépendance" aux écrans : la Chine veut drastiquement limiter l'accès des jeunes à Internet](#) », August 3, 2023.

one hour per day, modifiable by parents. These measures have been in effect since February 2025⁹⁸.

The French bill initially contained a digital curfew measure, but this provision was ultimately withdrawn before its examination by the National Assembly on 26 January 2026.

Examples show that limiting screen time for minors can be applied either strictly, through a complete ban during a state-defined time slot, or more flexibly, with protective default settings that can be adjusted by users or their parents. The aforementioned report by the **Center for Democracy and Technology**⁹⁹ considers strict curfew measures to be too intrusive and impractical, suggesting instead more flexibility in screen time functionalities. Indeed, interface design and the addictive mechanisms implemented by digital intermediaries tend to prolong time spent online (with minors sometimes staying awake at night), leading to knock-on effects on activities essential to the development of children and adolescents including sleep, physical activity, and eyesight. However, time spent online reveals nothing about actual practices or the content viewed.¹⁰⁰ Responsibility lies first and foremost with the platforms, yet such measures primarily target the habits of young people. Furthermore, digital platforms also serve to aid learning and discovery, offering access to educational, cultural, and creative resources.¹⁰¹ It is therefore essential to distinguish passive usage, which is often criticised, from active and constructive usage, which can enrich the skills and knowledge of users, provided it is supervised and involves tools adapted to each age group.

(2) Secure and Customisable Digital Interfaces

The protection of minors can also be achieved through dedicated interfaces that are age-appropriate, less addictive, and focused on filtering harmful content. These measures are of paramount importance to ensure that minors, when accessing these services, operate within secure digital environments. Such adaptations can be implemented either voluntarily by platforms, which has not seen significant success to date, or at the behest of the legislator. The age verification methods analysed previously often constitute a prerequisite for activating these adapted functionalities or interfaces.

The European Commission's guidelines on Article 28 of the DSA¹⁰² provide measures intended to supervise the addictive functionalities of platforms in order to limit their effects on minors. Notifications must be disabled by default, particularly during the night. AI functionalities, such as chatbots integrated into platforms, must not be activated by default. Furthermore, minors must not be subject to any incitement to use them. It would be desirable for such protective default measures to be considered for all users.

⁹⁸ [Appeal from the United States District Court for the Northern District of California Edward J. Davila, District Judge, Presiding](#), September 9, 2025.

⁹⁹ Center for Democracy and Technology, "[What Kids and Parents wants: Policy Insights for Social Media Safety Features](#)", November 19 2025.

¹⁰⁰ Le Monde, « [Usages du numérique : « La question du temps d'écran, c'est le degré zéro de l'analyse »](#) », February 9, 2021.

¹⁰¹ Dominique Pasquier, Quentin Gillote, « [Apprendre par la bande : que nous apprennent \(vraiment\) les youtubeurs ?](#) », October 19, 2023.

¹⁰² European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#).

In the **Netherlands**, a court ordered Meta to offer a chronological news feed by default, meaning posts are presented in the order they are published rather than according to an algorithmic ranking. The obligation to offer an alternative feed is included in the DSA. This decision complements it by requiring its activation by default. This measure concerns all user accounts, not just those of minors. Meta has appealed this decision, which has therefore been suspended until the next judgement.

At Meta, the social media platforms Instagram, Facebook, and Messenger are experimenting with “Teen Accounts” dedicated to 13–17-year-olds, which include protection settings for young users, notably limiting “inappropriate content and unwanted contacts”.¹⁰³ The activation of the account in “teen” mode is automatic; settings are installed by default and can only be modified with parental consent for those under 16. Following a trial in the United States, the United Kingdom, Australia, and Canada, the company is going to roll out this mode worldwide.

Several factors must be taken into account. First, whilst it is the responsibility of the platforms themselves to implement moderation, content filtering, and configuration measures, these objectives may conflict with their business model and lead to deceptive measures. The fines which very large platforms have received often represent a very small portion of their turnover, and are not always a deterrent to integrating these functionalities. Additionally, applying content adaptation measures requires platforms to possess—and dedicate—sufficient technical and human capacities, notable in the case of smaller digital actors. Finally, if these configuration options are not activated by default, it may be necessary for minor users to be supported in activating the available options.

Beyond functionalities that may exist on predominant platforms, alternative digital services to the dominant actors exist, such as Mastodon, a decentralised and federated social media platform, or Bluesky, a social media platform offering a similar experience but based on user customisation and human moderation. These alternatives carry the promise of a healthier online experience: less addictive and harmful designs for the user, greater human moderation capacities, better respect for personal data, etc.

With a view towards future developments, W social¹⁰⁴, a future European social media platform designed by Anna Zeiter, former Chief Privacy Officer and Vice President in charge of AI and Data Responsibility at eBay, promises a healthier and less toxic interface, respect for users' personal data, strict age verification, human (rather than algorithmic) moderation, and customisable algorithms to avoid algorithmic confinement. These alternatives restore choice to the user, both in terms of the digital service they wish to use and the settings they wish to activate.

¹⁰³ AFP, « [Les “comptes adolescents” Facebook et Messenger déployés dans le monde entier](#) », September 29, 2025.

¹⁰⁴ France Culture, « [Le réseau européen “W social” pensé comme un “anti X” a-t-il une chance d'exister ?](#) », January 29, 2026.

However, migrating to these alternatives remains a path fraught with obstacles. Firstly, numerous technical exit barriers make migration and the effectiveness of the right to data portability complex, without a universalised solution as seen in telecommunications, for example. Furthermore, the network effects are strong: major tech companies (the GAFAM) have built monopolies creating systemic dependence. It can seem difficult to leave one social media platform and to migrate to another due to the potential loss of audience, communities, and “digital social capital.” This is why tools and movements are emerging to facilitate this transition. The HelloQuitteX movement, for example, equipped 13.4% of users¹⁰⁵ who migrated from X to Bluesky in a few months. OpenPortability¹⁰⁶ was developed by the movement as a solution to facilitate migration, relying on the right to portability.

It should be noted, however, that virtuous alternatives are not immune to structural flaws. Bluesky has been criticised for its “moderation lists”,¹⁰⁷ and Mastodon, despite its decentralised model, struggles to effectively moderate hateful content at a large scale.¹⁰⁸ These solutions should rather be seen as spaces for re-appropriation. They demonstrate that it is possible to propose alternatives to dominant models.

(c) Avenues for Reflection and Priority Areas

Regulations based on age verification to restrict access for minors only solve part of the problem, as the structural causes of risks generated by social media remain unchanged. Faced with the issues remaining in current regulations, the following priority areas aim to harmonise the protection framework for minors at the European level, risking, however, to undermine the efforts of Member States; to carry out structural reforms on the European regulatory framework for platforms; and to broaden the scope of reflection on digital practices of the youngest users online and on support with the use of digital services to enable – in the foreseeable future – safer and more positive usage.

*

Priority 1: Create a European standard for the protection of minors online

The protection of minors online must imperatively be addressed at the European level, a market of over half a billion social media users, to achieve convincing results.

Through its pioneering role, France could act as a driving force within the European Union and advocate for a shared standard for the protection of minors online. This would include harmonised requirements for service design, secure age verification systems that protect personal data, and risk governance involving designated trusted flaggers whose work is essential. Such a framework of reference will be enriched in the coming months by work conducted on European digital identity solutions. It would gain prescriptive power over major digital platforms, thereby producing a structural effect across the entire market.

¹⁰⁵ [HelloQuitteX : on fait le bilan.](#)

¹⁰⁶ <https://openportability.org/fr/auth/signin>.

¹⁰⁷ France Inter, « [Bluesky : les lites de modération font polémique](#) », December 2, 2024.

¹⁰⁸ BFM, « [Sécurité, modération, prise en main : ces points faibles de Mastodon, l'alternative à Twitter](#) », November 12, 2022.

In this light, France could usefully collaborate with Irish and Lithuanian authorities ahead of their respective EU presidencies, starting with Dublin next semester. Indeed, Ireland has suggested that the issue of the minimum age required to access social media platforms could be included on its European presidency agenda.¹⁰⁹

*

Priority 2: Open up platform functionalities, establish a right to customisation, and strengthen algorithmic transparency

Reinforced protection measures targeting minors do not address the source of the negative social externalities induced by platforms: namely, the economic model of these actors. Systemic regulation of platforms now appears more than necessary. Their business model relies on the capture of user attention, permanent engagement, and constant exposure—including to the most toxic content¹¹⁰—in order to maximise screen time and, ultimately, advertising revenue. Platforms exploit users' personal data, integrate dark patterns¹¹¹ (deceptive interfaces) into their designs, and deploy algorithms that are opaque and increasingly restrictive, despite transparency obligations.

As highlighted by Anses¹¹², these algorithms create a “spiral effect,” trapping young people in increasingly targeted, and sometimes extreme, content by exploiting their cognitive biases and behavioural data. Simultaneously, platforms are diversifying their revenue sources: the sale of personal data to advertisers, ultra-targeted advertising, paid subscriptions, and the monetisation of user-generated content—a model that encourages escalation and favours the production of shocking or divisive content.

In Spain, for example, Prime Minister Pedro Sanchez announced his intention to tackle these systemic issues by going beyond the social media ban considered for those under 16.¹¹³ He stated making the “manipulation and algorithmic amplification of illegal content” a “criminal offence” amongst his priorities.

Clearly, these risks do not only concern minors, but all users of these digital services. However, current measures targeted at minors present a risk, through a perverse effect, of “unleashing” digital spaces¹¹⁴ for other users. It is imperative to prevent the protection of minors from serving as a screen for generalised deregulation.

Independently of age control, complementary solutions deserve to be promoted to allow everyone more choice and control over their online experience. This follows proposals made

¹⁰⁹ Toute l'Europe.eu, « [Mineurs et réseaux sociaux : quels pays européens comptent imposer un âge minimum ?](#) », February 26, 2026.

¹¹⁰ See also: CNum, « [Votre attention s'il vous plait ! Quels leviers face à l'économie de l'attention ?](#) », January 2022.

¹¹¹ Defined by [Designers éthiques](#) as “elements designed to push the user to do things that they would not necessarily have done initially”.

¹¹² Le Monde, « [L'Anses alerte sur les risques des réseaux sociaux sur la santé des adolescents](#) », January 13, 2026.

¹¹³ Le Monde, « [L'Espagne compte interdire à son tour les réseaux sociaux aux moins de 16 ans](#) », February 4, 2026.

¹¹⁴ Hubert Guillaud, « [Vérification d'âge \(2/4\) : de l'impunité des géants à la criminalisation des usagers](#) », December 4, 2025.

by the Estates General of Information¹¹⁵ and the Commission of Inquiry into the psychological effects of TikTok on minors.¹¹⁶ The priority must remain the emergence of solutions aligned with European values, with regulation and bans serving only as corrective measures.

Amongst these:

- **Algorithmic pluralism**, to allow users to choose how algorithms select and display content and to configure their interfaces. This enables users to find greater diversity in the content offered to them whilst protecting themselves from harmful content.¹¹⁷ For example, reinforced filtering options, algorithms designed by third parties to prioritise educational or age-appropriate content, or simplified and transparent interfaces could limit exposure to disinformation, hate speech, or content promoting risky behaviours (such as dangerous challenges or eating disorders). Furthermore, opening up to third-party moderation services—certified and monitored—would provide safer digital environments where minor protection rules are prioritised and adaptable to the user's specific needs. Certain platforms, like Bluesky, are already experimenting with systems where users can customise their feeds and moderation strategies. Public authorities could more broadly encourage the emergence of alternative algorithms.
- **A right to customisation by default for minor users, accompanied by an adult**, to jointly define the minor's interests in their interactions with digital services: "These settings could concern notification levels, the visibility of published content, or the type of content consumed—meaning what they see as recommended content—as proposed in the work of the CNCDH on online hate."¹¹⁸ Without placing too much responsibility on the user, "the right to customisation would allow an alternative path that puts individuals in a position of reflection, encouraging users to step back from their behaviour and usage, and allowing them to reflect on their automatic habits."¹¹⁹ The activation of these settings must be designed with a simple, accessible interface to avoid "decision fatigue," which systematically leads to users keeping default settings. Furthermore, by default, functionalities should be configured as neutrally as possible (disabling notifications, chronological presentation of content, etc.).
- **Reinforced transparency of recommendation and moderation systems** to compel platforms to explain, in an intelligible manner, their choices and criteria for ranking content and to offer alternatives which are less addictive. The DSA already imposes, in Articles 14, 15, and 27, the publication of information on moderation tools, annual transparency reports, and an explanation of the main parameters of recommendation algorithms. However, these obligations currently produce technical reports that are hardly readable for the general public and do not allow for a deep understanding of the economic and attentional logic structuring the systems. It is therefore necessary to go further by requiring standardised, intelligible, concise, and comparable formats, and by increasing data access for researchers and independent authorities.

¹¹⁵ [Rapport des Etats généraux de l'information, Protéger et développer le droit à l'information : une urgence démocratique](#), September 12, 2024. Proposal n° 1 Making critical thinking and media education in schools a priority.

¹¹⁶ Assemblée nationale, [Rapport fait au nom de la Commission d'enquête sur les effets psychologiques de TikTok sur les mineurs](#), September 2025. Proposal n° 12.

¹¹⁷ Le Monde, « [Pour le pluralisme algorithmique !](#) », September 25, 2024.

¹¹⁸ For more information: CNNum, « [Vers la consécration d'un droit au paramétrage ? Échange avec Célia Zolynski](#) », May 22, 2024.

¹¹⁹ *Ibid.*

- **The promotion of open standards** in social media platforms is an indispensable prerequisite for algorithmic pluralism. These standards form the foundation that makes possible account portability (keeping identity and contacts when changing platforms), interoperability (exchanging between networks, introducing third-party services, and choosing other recommendation systems), and an offer of a plurality of algorithmic options.

*

Priority 3: Rethink the division between “host” and “publisher”

Certain countries within the EU are moving toward strengthening the liability regime applicable to online platforms regarding minors. For instance, the French bill, as adopted by the National Assembly, introduces a major shift by proposing to redefine the status of platforms when they “suggest or prioritise, by means of a recommendation system, information provided by recipients of the service.”¹²⁰ In such cases, and regarding this information, platforms would be considered publishers.

Traditionally, social media platforms benefit, under the e-Commerce Directive, from a limited liability regime as hosts,¹²¹ being held responsible for content published by their users only if they had actual knowledge of it or failed to act promptly to remove it. Conversely, the publisher, who determines and controls content, is subject to reinforced civil and criminal liability.

However, the rise of major platforms that organise, recommend, and monetise content has revealed the limits of this asymmetrical liability regime. According to the Advocate General in the so-called “AGCOM” case of the Court of Justice of the EU, “the dichotomy of the passive or active role appears to be insufficient in addressing the activities conducted by a hosting service provider, especially in such an ever-changing field”¹²² Similar reasoning was also issued by the Advocate General in the recent “Coyote System” decision.¹²³ He emphasises that the driving assistance platform Coyote does not merely transmit information provided by its users but exercises active control over it. It cannot, therefore, benefit from the host status that normally limits platform liability. If the Court of Justice validates this analysis, it could mark a major turning point in the liability of platforms as designers and programmers of algorithms.

For a decade, reflections on establishing an intermediate status between publisher and host have increased due to the inadequacy of the “technically neutral role” criterion, adopted by the French transposition law¹²⁴, to distinguish hosts from publishers.

¹²⁰ Article 1 bis (new), [Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux](#), adopted at first reading on 26 January 2026.

¹²¹ Article 6-I-2 LCEN, the law transposing the E-Commerce Directive.

¹²² [Provisional text opinion of Advocate General Szpunar delivered on 27 November 2025, Case C-421/24 known as AGCOM.](#)

¹²³ [InfoCuria - Cour de justice de l'Union européenne.](#)

¹²⁴ [Loi du 21 juin 2004 pour la confiance dans l'économie numérique.](#)

The French State Council, in its 2014 annual study¹²⁵, recommended moving beyond the publisher/host duality to establish a “platform” status with reinforced obligations. A 2018 Senate resolution¹²⁶ also called for defining a “third status” at the European level—an intermediate category known as “online service publisher”—aligning with a 2014 report by the French Superior Council of Artistic and Literary Property (Conseil supérieur de la propriété littéraire et artistique). These proposals are partly visible in the DSA, which, without formally creating a third status, distinguishes online platforms—specifically Very Large Online Platforms and Search Engines—within the host category to impose a more demanding liability regime, particularly regarding moderation.

Rethinking the status of these actors would allow for a move toward a shared liability logic, for example, in cases of illegal content distribution (cyberbullying, incitement to hatred, etc.), which appears essential as platforms often hide behind their host status to escape reinforced obligations.

Such a reform can only be conceived at the European scale. The revision of the DSA planned for 2027 could constitute the opportune moment to introduce this modification. In this regard, France can drive preparatory work in coordination with Member States engaged in similar reflections, such as Spain or Greece, which will hold the EU presidency in the second half of 2027.

*

Priority 4: Consider the diverse usages of digital services, particularly those involving generative AI

The protection of minors tends to focus on social media. However, the way digital services are used is diversifying,¹²⁷ particularly amongst young users, on online games, private messaging, collaborative platforms, voice assistants, etc. These altered habits are also vectors for risks.

The emergence of generative AI creates new vulnerabilities. 59% of 12–17-year-olds already use generative AI, a figure above the population average of 48%.¹²⁸ In July 2025, 206 AI companionship applications were available on the App Store and 253 on Google Play—all with hundreds of millions of downloads. Replika, one of the leaders in “artificial intimacy”, has over 10 million users. The 2025 festive season saw a surge in toys integrating AI,¹²⁹ and AI companions are increasingly integrated into social media platforms (such as My AI on Snapchat, Meta AI on WhatsApp, Grok on X, etc.).

These tools, designed to maximise user engagement, can create emotional dependency and displace human relationships essential to the psychological development of the youngest users, while capturing their personal data for commercial purposes. The underlying models,

¹²⁵ Conseil d’État, [Le numérique et les droits fondamentaux](#), September 8, 2014.

¹²⁶ Sénat, [Proposition de résolution européenne n° 739](#), September 27, 2018.

¹²⁷ A survey conducted by the [Institut GWI](#) for the Financial Times in over 50 countries, involving 250,000 people.

¹²⁸ Arcom, [Baromètre du numérique 2026](#).

¹²⁹ See also: CNum, « [Votre attention s’il vous plaît ! Quels leviers face à l’économie de l’attention ?](#) », January 2022.

often opaque and not adapted for minors, risk manipulating their decisions, encouraging dangerous behaviours,¹³⁰ and exposing them to inappropriate or even illegal content.

To avoid repeating the errors made regarding social media, public authorities must address the issue of these “new” usages and the vulnerabilities they might generate for users, and especially for the youngest amongst them.

In this context, the French AI and Digital Council will launch a “Generative AI and Vulnerabilities” commission,¹³¹ at the request of the Minister Delegate for AI and Digital Affairs, with the aim of identifying the main risks related to these usages and developing concrete recommendations for public authorities. The first findings will be made public by the end of May 2026. The final report will be submitted in September 2026.

*

Priority 5: Strengthen and expand education in digital, media, and information literacy

Faced with diverse digital tools and the multiple risks to which they expose minors, it is essential to strengthen users' critical thinking from a young age. To enable them to regain control over their digital habits, media and information literacy must become a genuine pillar of school curricula, following the Finnish model.¹³² It is also vital to place importance on offline socialisation practices.

This digital education must be established from the earliest age, from primary to secondary school. Frameworks already exist. For example, the Charter for Education in Digital Culture and Citizenship¹³³ reiterates the need for explicit training on digital rights and duties, personal data protection, and the fight against disinformation. The Framework for AI Use in Education also recommends training in media and information literacy within classes integrating generative AI.¹³⁴ At the European level, the Guidelines for teachers and educators on tackling disinformation and promoting digital literacy,¹³⁵ updated in 2026 following the Digital Education Action Plan 2021-2027, advocate for strengthening the place of digital literacy in curricula, teacher training, and school projects. The EU emphasises the need for school policies to support teachers (with time, resources, and training) and to integrate these issues coherently across school life. The French circular of 10 July 2025, aimed at promoting reasoned digital habits in schools,¹³⁶ translates these orientations into concrete measures with the assessed integration of media and information literacy into learning. Based on the Digital Competence Reference Framework (CRCN), the learning of these skills must be evaluated via the Pix platform. The circular emphasizes that within the media and information literacy framework, “educational teams contribute to training students on the rights and duties related to the use

¹³⁰ BBC, “[‘A predator in your home’: Mothers say chatbots encouraged their sons to kill themselves](#)”, November 8, 2025.

¹³¹ CIANum, « [Le Conseil de l’intelligence artificielle et du numérique chargé de constituer une commission « IA générative et vulnérabilités](#) », February 27, 2026.

¹³² This is FINLAND, “[Finland promotes media literacy as a civic skill](#)”, 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](#) », June 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](#), July 10, 2025.

of the Internet and social media. They introduce students to an ethical and thoughtful use of digital tools and participate in the development of students' digital skills, complementing the implementation of lessons dedicated to technology and computer science.”

Despite these texts, media and information literacy remains insufficient in classrooms due to a lack of time and resources. It must be the subject of a structured school curriculum, adapting learning to the age and usage of students, following the model of the dedicated program for emotional, relational, and sexual education released in 2025.¹³⁷ At the European level, a common base could set minimum objectives in terms of hours and skills to be acquired, which each Member State would integrate into its school programs. This program must be accompanied by dedicated funding to guarantee the effectiveness of the measure.

This policy must also go hand in hand with a training plan for the adults surrounding young people (families, professionals, teachers, carers, etc.), with adapted pedagogical tools, to foster a continuous adult-child dialogue on digital practices. Several actors already offer tools to this end, such as the factsheets for parents and pedagogical teams produced by “Internet Without Fear” (Internet Sans Crainte) foundation¹³⁸. These issues are directly linked to the need to increase the scale and scope of initiatives regarding digital inclusion and mediation, particularly in local territories, at a time when resources allocated to this area are being continuously reduced.

Finally, education must be complemented by local policies that value non-digital spaces, such as spaces for socialising, workshops, in addition to dialogue, information, and civic participation projects, to offer young people collective experiences outside of online platforms. Many public policy alternatives are already proposed; it is important to promote them for better dissemination among the relevant audiences.

¹³⁷ Ministère de l'Éducation nationale, « [Un programme ambitieux : éduquer à la vie affective et relationnelle et à la sexualité](#) », February 2025.

¹³⁸ For more information: Internet Sans Crainte, « [Vous êtes parents – Nos ressources et des événements pour accompagner les pratiques numériques de vos enfants](#) ».