

Input by Simeon de Brouwer, on behalf of European Digital Rights ([EDRI](#)), for the the Independent Expert Commission on the Safety of Children and Young People in Digital Environments (4th hearing)

The EDRI network is a dynamic and resilient collective of NGOs, experts, advocates and academics working to defend and advance digital rights across the continent. For over two decades, it has served as the backbone of the digital rights movement in Europe.

I Principles and legal interests

1. Legal interests and guiding principles

In your opinion, which principles and legal interests are at the heart of digital child protection policy?

Child empowerment, and the principle of proportionality:

In line with the OECD [2025 report](#) and with the UN Committee on the Rights of the Child [General comment No. 25](#) (2021) on children's rights in relation to the digital environment, any measure to protect children should aim at maximising their ability to exercise and enjoy (all of) their rights, enabling them to participate, grow autonomous, confident and resilient. Any measure meant to ensure children's (right to) safety should be proportionate, so as not to be at the expense of their and others' ability to exercise their other rights. If measures less intrusive than censoring/surveillance/controlling access exist, the latter cannot be pursued.

Moreover, the analysis of child protection policy options must go beyond the interests of the average minor, and consider the risk of cutting marginalised groups off from crucial online communities and online safe spaces (think of LGBTQ young people, or young people living in isolated rural areas).

Further on proportionality, EDRI also underlines that a social media ban would not only negate children's rights, it would also negate the rights of all the adults who cannot fulfill the age verification process. This is the case for many already-marginalised demographics such as those with low digital literacy (e.g. the elderly), those who do not have the means or the desire to own a modern smartphone (but who still access social media via a computer), those who cannot submit valid ID documents (e.g. undocumented people), etc.

Finally, a key principle for meaningful, effective and sustainable child protection policy is to **aim for the root cause of harm**. The core of the problem lies in the business models of large technology platforms, and the practices they employ to keep people online. Banning vulnerable users from online spaces merely delay their exposure without equipping them with the needed skills/tools, but also removes any incentive platforms have to ensure safe spaces for young people. On top of that, it also implicitly legitimises the application of the platforms' harmful practices when they apply to adults.

2. Understanding of regulation

What role do the following play in your national model:

- the state's duty to protect,
- platform responsibility,
- empowerment of children and parents?

3. Protection, empowerment and participation

How is the balance between protective measures, empowerment and digital participation specifically structured in your country?

At EU level, the duty to protect is through the DSA, the enforcement of which befalls the EU Commission (for the biggest platforms only). The Commission notably recently issued [preliminary findings](#) against TikTok, based on the platform's addictive features and the impact it has on minors – thereby potentially setting a precedent for all other social media's similar design and features.

Under the DSA, platforms must ensure that minors are safe – but this does not mean that they need to check the age of every user. Instead, it means that when it knows, expects or suspects that a user is a minor, the platform needs to ensure them a safe, secure and privacy-preserving experience (and may take targeted measures to determine the age, if they have a doubt). Platforms are therefore held accountable for the risks and harms they create, and have incentives to mitigate these.

The DSA's spirit is to empower users, not by excluding vulnerable users from unsafe spaces but, to the contrary, by making these spaces safe so that all users can participate. The DSA aims at ensuring that all users can evolve in a safe online environment – where risks are acknowledged and addressed, where users can choose a feed that is not algorithmically-curated, where the reports they file are duly followed-up through an easily accessible and user-friendly notice and action mechanisms, etc.

II National regulation and implementation

III Experiences: What works – what doesn't?

1. Positive experiences

Which measures or instruments have proven particularly effective in your country?

Have there been measurable improvements?

2. Negative or unintended effects

Where have regulations proven problematic (e.g. circumvention, displacement effects, data protection conflicts, overblocking)?

We would like to note that experiences in the UK, Australia, China, Korea and the US all point toward the ineffectiveness of age-gates. Young people have every incentive to bypass any ban, because the targeted service is attractive/important for them, and will remain so. The available measures include having someone do the age-check for you (be it a parent, an other relative, an older friend, or someone who sells this as a service on the black market), circumventing national restrictions through VPNs or TOR.

Furthermore, children and young people who resort (like [in Australia](#)) to unregulated and unsafe platforms are exposed to unmoderated content, increased risks of fraud, malware, and data theft. Those who use free and unsafe VPNs to continue using their usual platform despite the ban face increased data protection risks as well, because their traffic data may get exposed to potentially malicious actors who monetise or abuse it.

Self-declaration is one form of age assurance which many consider insufficient because it can be abused, but EDRI considers it a useful and sufficient method in some cases: children indicating their true age should be sufficient where, upon being informed about the user's young age, the provider adapts its service to mitigate the specific risks young people are exposed to on the platform/tool - without excessively controlling/locking/monitoring their behaviour. If minors have the incentive to disclose their (average) age in good faith – because they know they'll be *offered* meaningful and tailored protection, instead of being *imposed* overly restrictive experiences (or banned) – then they can evolve in an environment meant to keep them safe, and in relation to which they can easily and safely seek help, training and support.

European Youth bodies call to not exclude young people from social media, and to instead mandate safety-by-design and fairness-by-design standards across all social media platforms. (see the European Youth Forum's position, as well as the position of Ctrl+alt+reclaim, Europe's First Youth-Led Tech Justice and Digital Rights Movement.)

Additional sources:

- Survey: 8000 young europeans from 13 Member States were polled at EDRi's initiative about their preferences on how they want to be protected online (specifically from Child Sexual Abuse online, but it extends *a fortiori* to 'lesser' harms). Here's the interactive poll + EDRi blog on it. The results overwhelmingly show that young people prefer being protected through empowerment rather than through intrusive or restrictive measures. Q7 indicates **56%** of the youth does not want to be blocked from installing apps/games. Q11: asked whether they would find an adult to help them circumventing an age-gate, **53%** of youth confidently respond 'yes' while **32%** respond 'maybe'. Thus, 85% of young people polled consider circumventing restrictions through an adult – and that is without even considering their ability to circumvent it on their own.
- Academic article: boyd, d., et al. (2011). *Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act*
 - Table 4: Among those parents who knew that their child joined below the age of 13 over two-thirds (68%) indicated that they helped their child create the account.
 - Table 7: 77% of parents declare willingness to allow their child to create an account in violation of the minimum age requirement.
 - Table 12: only 12% of parents think that "Restricting children's access to online services" should be the primary focus of efforts to keep children safe online.
- China
 - Article in Nature: *No evidence that Chinese playtime mandates reduced heavy gaming in one segment of the video games industry*
 - Article by Feng & Sion 2023: *A Study of China's Censorship and Its Evasion Through the Lens of Online Gaming*. It concludes that "anti-addiction policies do not work as designed against even very young gamers. [...] Somewhat counter-intuitively, [the bans aiming at preventing addiction] seem to act as a general censorship evasion training ground for tomorrow's adults, by familiarization with and normalization of general evasion techniques, and desensitization to their dangers."
 - A 2024 survey revealed that more than half (58.5%) of Chinese parents were willing to provide their identification information to help their children bypass the real-name authentication legal requirements in online games. The other children rely on other people: 77% of the minors surveyed used other people's identities to register for the games. (56.6% used their parents' IDs, 12.8% used their grandparents' IDs).

IV Political initiatives at national level

V European level

1. Expectations of the European Commission

What do you expect from the EU in terms of digital child and youth protection policy (e.g. new regulation, harmonisation, enforcement, guidelines, research, coordination)?

EDRi expects high fundamental rights standards at EU-level, but these expectations fail to materialise. The European Commission, for instance, is piloting a deregulation process

whereby the “red tape” protecting people’s rights and interests are watered-down, so as to serve ‘innovation’. 126 NGOs underlined the negative impact the digital and data omnibus risk having on fundamental rights, whereas the specific impact on children's protection was highlighted in a separate letter by child rights NGOs.

On child rights specifically, the Commission has already proposed blatantly disproportionate measures – the mass scanning of private conversations (Child Sexual Abuse Regulation proposal, or ‘chatcontrol’) – therefore it would not be surprising if, once again, it would support the populist call for banning young people from social media altogether.

The big issue with the Commission is the slow/lack of DSA enforcement with regard to the VLOPs it has competence on. The Commission is not an independent authority, and has been taking very timid steps amid a tense US geopolitical situation. (Note: every single national Digital Services Coordinator is working too slowly too, it’s not only the Commission’s fault.) As a result, the large majority of DSA infringement, even very obvious ones, remain to date unaddressed. This means that NGOs like us need to take the matter in our own hands and either document-and-complain to authorities, or litigate directly – see for instance the case of our Dutch member Bits of Freedom against Meta. However, we note the recent opening of Commission DSA preliminary findings against TikTok, which we hope will set the standard for what measures social media need to do / stop doing in the EU to prevent compulsive use/addiction and manipulation.

As to Guidelines, we underline the political nature of such soft law and of the fact that it merely reflects the Commission’s interpretation. In its first draft of the Art. 28 DSA Guidelines, the Commission was cautiously positive about the use of age assurance, including age verification, while warning against the risk of disproportionate reliance on it. However, although the Commission’s summary report states that “the overall trend [in the feedback received] leaned in favour of disagreeing with the appropriateness of age assurance measures,” the final version of the guidelines nonetheless further entrenched the widespread reliance on such tools – a 180-degree change that came as a big shock to us, but which was likely caused by the coordinated push from a few Member States who wanted bans. In its final version, the Commission stated that age verification is proportionate and appropriate where “due to identified risks to minors, the terms and conditions or any other contractual obligations of the service require users to be 18 years or older to access the service, even if there is no formal age requirement established by law.” This goes beyond (and also against) the text and spirit of the DSA, and we expect litigation from platforms, should the Commission try to enforce it as such. We also consider litigation ourselves, against national and EU laws which would impose a ban, for the reasons delineated in this document.

The EU eIDAS Regulation imposes each Member State to deploy an eID Wallet, which purports to enable anonymous age verification. We have concerns about the extent to which the Wallet will deliver on the Regulation's promises, and we and our members are scrutinising the Implementing Acts put forth by the Commission. In an open letter from 10/03/2026, we argue that the Wallet being designed still does not deserve users’ trust; it fails to empower users, it weakens the Regulation’s language on unlinkability/untraceability, it imposes unnecessary (and unforeseen) biometric facial data processing, etc. One thing to bear in mind is that no Wallet has been developed, nor deployed, nor stress-tested anywhere yet; if only for that, we therefore consider that it would be folly to make its use mandatory yet. We need to first make sure it delivers on its promises, and assess the impact on people who would be excluded.

2. Assessment of EU instruments

How do you assess existing EU regulations (e.g. DSA, AVMSD, Action Plan against Cyberbullying, BIK+, Guidelines on the Protection of Minors (C/2025/5519))? Where do you see strengths and where is there room for improvement?

Under the DSA, platforms must ensure that minors are safe – but this does not mean that they need to check the age of every user. Instead, it means that when it knows, expects or suspects that a user is a minor, the platform needs to ensure them a safe, secure and privacy-preserving experience (and may take targeted measures to determine the age, if they have a doubt). Platforms are therefore held accountable for the risks and harms they create, and have incentives to mitigate these. The framework is good but now needs to be enforced proactively.

On the guidelines, we welcome most of the measures except age verification, which the Commission put forward as ‘the way platforms need to ensure a safe and secure experience.’ We hope some of these measures will be incorporated in the upcoming Digital Fairness Act (DFA), though in a way which benefits all users, not only minors. Beyond that, on age verification, we repeat what we wrote above: *(As to Guidelines, we underline the political nature of such soft law and of the fact that it merely reflects the Commission’s interpretation. In its first draft of the Art. 28 DSA Guidelines, the Commission was cautiously positive about the use of age assurance, including age verification, while warning against the risk of disproportionate reliance on it. However, although the Commission’s summary report states that “the overall trend [in the feedback received] leaned in favour of disagreeing with the appropriateness of age assurance measures,” the final version of the guidelines nonetheless further entrenched the widespread reliance on such tools – a 180-degree change that came as a big shock to us, but which was likely caused by the coordinated push from a few Member States who wanted bans. In its final version, the Commission stated that age verification is proportionate and appropriate where “due to identified risks to minors, the terms and conditions or any other contractual obligations of the service require users to be 18 years or older to access the service, even if there is no formal age requirement established by law.” This goes beyond (and also against) the text and spirit of the DSA, and we expect litigation from platforms, should the Commission try to enforce it as such. We also consider litigation ourselves, against national and EU laws which would impose a ban, for the reasons delineated in this document.)*

The big issue with the Commission is the slow/lack of DSA enforcement with regard to the VLOPs it has competence on. The Commission is not an independent authority, and has been taking very timid steps amid a tense US geopolitical situation. (Note: every single national Digital Services Coordinator is working too slowly too, it’s not only the Commission’s fault.) As a result, the large majority of DSA infringement, even very obvious ones, remain to date unaddressed. This means that NGOs like us need to take the matter in our own hands and either document-and-complain to authorities, or litigate directly – see for instance the case of our Dutch member Bits of Freedom against Meta. However, we note the recent opening of Commission DSA preliminary findings against TikTok, which we hope will set the standard for what measures social media need to do / stop doing in the EU to prevent compulsive use/addiction and manipulation.

On the AVMSD, we note that age verification is (like in the DSA) optional rather than mandatory, which is best. Further, we note that not all Member States want to go down the path of age verification: when transposing the Directive into national law, Poland, Estonia, Finland, Latvia, the Netherlands and Slovenia decided not to include any reference to age verification and focused on parental control instead ([source](#), p12).

3. Enforcement at EU level

In your opinion, is European enforcement in terms of platform regulation consistent and efficient? Where are there practical shortcomings?

We repeat what we wrote about. (*The big issue with the Commission is the slow/lack of DSA enforcement with regard to the VLOPs it has competence on. The Commission is not an independent authority, and has been taking very timid steps amid a tense US geopolitical situation. (Note: every single national Digital Services Coordinator is working too slowly too, it's not only the Commission's fault.) As a result, the large majority of DSA infringement, even very obvious ones, remain to date unaddressed. This means that NGOs like us need to take the matter in our own hands and either document-and-complain to authorities, or litigate directly – see for instance the case of our Dutch member Bits of Freedom against Meta. However, we note the recent opening of Commission DSA preliminary findings against TikTok, which we hope will set the standard for what measures social media need to do / stop doing in the EU to prevent compulsive use/addiction and manipulation.*)

4. Relationship between national measures and European harmonisation

In which areas do you consider harmonised regulations within the EU to be necessary, and where would you like to see national regulatory powers?

We are wary of enforcement bottleneck (such as Ireland and Luxembourg when it comes to the GDPR), but also wary of centralising regulatory power into the EU Commission (which is not an independent authority, and faces geopolitical tensions when attempting to enforce the DSA onto US companies). Coordinated and proactive DSA enforcement would achieve much already in terms of child protection.

A harmonised regulation for a Digital Fairness Act (see our [position here](#)) is direly needed at EU level: Digital services influence how people act, make choices and relate to each other and the world. Many rely on design systems built to control and manipulate behaviour in line with commercial objectives to the detriment of fairness. Deceptive design, addictive architecture and unfair personalisation shape decisions before people make a choice. These are structural problems. They diminish autonomy and fundamental rights to access information, equality, and data protection, amongst others. The Digital Fairness Act framework should address these issues, in a way which benefits all people regardless of their age (but acknowledging that it would benefit greatly minors in particular). It should push for:

- Structural fairness as the core principle:
 - Shift the burden of proof to traders, requiring them to prove fairness by design and by default. This should be combined by clear prohibitions with a narrowly scoped grey list for context-dependent harms.
 - Modernise the definition of professional diligence to include a duty to avoid systems that exploit vulnerability. Require behavioural design impact assessments, design logs and experiment documentation.
- Addictive design and attention capture:
 - Treat addictive design as structurally manipulative and presumptively unfair when they removes disengagement cues or uses emotional profiling. Features incentivising time and/or money should be turned off by default in the baseline mode of use, and only activated following explicit user choice, with a single, clearly visible option to deactivate them.
 - Include in the UCPD Annex I a block list for tactics that always undermine autonomy and a grey list requiring strong justification for high-risk features.
- Deceptive design:

- Prohibit in the UCPD Annex I practices such as misleading consent interfaces, hidden opt-outs, fake scarcity and emotionally manipulative framing designed to pressure or distort decision-making.
 - Accountability should extend across the design chain. Consent Management Platforms (CMPs) CMP providers should be accountable for manipulative templates, and services should honour machine-readable consent signals.
- Unfair personalisation and profiling:
 - Prohibit the personalisation that exploits protected characteristics, inferred traits, distress, addiction or economic vulnerability, as part of consumer law
 - Guarantee a non-personalised default across digital services with full functionality and a right for users to access it in a non-personalised version.
 - Make personalisation opt-in, with unbundled consent. ensuring that the non-personalised version remains fully functional and free from service degradation.
 - Prohibit advertising models based on unlawful tracking or profiling as part of consumer law. Lawful contextual advertising that does not rely on personal data or profiling must be preserved and clearly distinguished
- Breaking the silos: Coordinated, cross-regulatory enforcement:
 - Introduce a legal duty of cooperation between consumers, data protection, competition, media and digital regulators.
 - Support coordinated investigations, evidence sharing and direct Commission enforcement for cross-border manipulation through the Consumer Protection Cooperation (CPC) framework. Regulators should run joint cases and use pattern-based detection to identify structural manipulation.