

Social Media and Children's Mental Health

Taking stock and examining responses

Thematic Dialogue – CoE - Strasbourg, 4 June 2026

Manon Letouche' speaking notes.

Question

We have heard about standards and legislation, but laws only go so far if the platforms themselves are not designed with children in mind. What does actually mean in practice, and what needs to change in the way platforms are built to make safety the default rather than the exception ?

Presentation (10 minutes)

Introduction

Good afternoon, everyone.

Thank you for inviting me. I am delighted to represent 5Rights, alongside Julia and Rhythm who brilliantly shared their experiences and insights with us this morning.

(As was said), 5Rights Foundation is an international NGO dedicated to children's rights in the digital environment. We work on advocacy, compliance and research and we have a compelling youth engagement programme that helps us build our positioning on matters such as the one that we are discussing today.

And it is crucial to listen to children and young people. Their voices need to be heard, especially as we are now at a moment of deep collective anxiety, of moral panic, notably from parents and policy makers, on the topic of social media and children's mental health.

And the panic is understandable. The attention economy and persuasive design are worsening a profound mental health crisis marked by exploding rates of anxiety, depression and addiction.

While there is more and more awareness and consensus on the risks and harms children and young people face on those platforms, there is more debate on how to prevent them. At 5Rights, we advocate for regulations and standards that tackle the roots of the problem and focus on the design.

1,5 MINUTES

The law as a starting point :

So, to start responding to your question, *laws only go so far if the platforms themselves are not designed with children in mind* – I would like to first state that laws only go so far as properly enforced.

I focus on EU Affairs, and when we look at the EU legal landscape, I would not say that the problem lies first in the legislation.

After all, Europe has spent years constructing a good digital rulebook, with mostly :

- The **General Data Protection Regulation (GDPR)** to protect data and privacy.
- The **Digital Services Act (DSA)** to regulate online platforms and content moderation.
- The **Audiovisual Media Services Directive (AVMSD)** to regulate content itself and govern video-sharing platforms (which include social media)
- The **AI Act** to establish guardrails for artificial intelligence, with a risk based approach.

Yet, despite this regulatory armor, children are still falling prey to commercial exploitation on an unprecedented scale. Of course, there are gaps in these laws, but mostly, this framework suffers from massive enforcement and compliance deficit.

Looking at privacy for example, in April 2026, the [Global Privacy Enforcement Network \(GPEN\)](#) [published a report](#) that demonstrate that children today face much more pervasive privacy risks than they did ten years ago, including in the EU.

Take the **GDPR's age of consent**, which was designed to protect children from data-driven commercial exploitation. In reality, platforms have processed children's data on a massive scale, relying on other legislative grounds than consent, such as legitimate interest, and contract. Or look at the **AVMSD**, where late and fragmented implementation in some MS allowed video-sharing platforms and influencers to operate without effective oversight for far too long, leaving children and young exposed to tons of harmful content during critical developmental years.

Faced with this enforcement failure, we are witnessing a wave of panic. Governments all over the world are rushing to implement blanket social media bans, trying to pull children out of the machine. But panic rarely breeds sustainable solutions. And banning children from specific services while leaving the underlying system unchanged is not sustainable.

(It has been said before), but it could push children towards even more unregulated services (such as AI, gaming, or even education technologies) that are equally problematic. It could undermine existing protections for older teenagers. It doesn't tackle the persuasive and manipulative features and functionalities on the service and crucially, it shifts the burden away from tech companies and places it squarely on the shoulders of overstretched parents.

So instead, at 5Rights Foundation, we are pushing for a different approach. **An approach that respects and upholds children's rights, that is tech neutral and that place the responsibility on platforms to ensure that their services are safe, private and age-appropriate by design.**

5 MIN

What does age-appropriate design means in practice?

To answer this second part of the question, we must look to the core tenets of **safety-by design** and **age-appropriate design**.

Safety-by-design has emerged as a central principle in digital regulation, reflecting a shift toward tech accountability that requires digital services to assess and mitigate risks to users from the earliest stages of product development and throughout the entire lifecycle of the product or service.

(I put on the slide the references to our very recent Safety by design Code of Practice, that was written in the UK's context but which principles are very relevant in every contexts) :
<https://5rightsfoundation.com/resource/safety-by-design-code-of-practice/>

Age-appropriate design means moving away from a binary model of "presence or prohibition". It means building graduated digital environments that recognise children as distinct rights-holders and actively cater to their evolving capacities as they grow.

In practice, we need to take at least these 3 steps :

1. Recognising children online

We cannot protect children if we treat them as small adults or pretend that we don't know they are there.

Providers have two options : either they ensure that their services are safe and private and appropriate for all users, either they need to recognise children online and provide with specific safeguards for them. Age assurance can and must be performed using **privacy-preserving, proportionate, and secure methods**.

2. Differentiating the experience by age and development

Once we recognise a child's age, their digital experience must be tailored to their developmental milestones:

- **For children under 13:** they do not possess the cognitive maturity to critically engage with systems designed to manipulate their behavior. Therefore, personalised services driven by behavioral profiling and data-driven practices should not access this age group.
- **For teenagers (Up to 18),** it should not mean full exposure to the entire architecture of adult services. Instead, platforms must be reconfigured with **strong default protections**. Recommender systems must be strictly limited, and the most harmful design choices—like infinite scroll and push notifications designed to keep users hooked—must be deactivated by default.

3. Investing in alternatives

Access restrictions cannot work in isolation. Children don't only need protection from harm : they need access to better alternatives. Age-appropriate design requires public and corporate investment in rights-respecting services offline and online : digital services built to support child development, high-quality online cultural and information content, and safe civic spaces both online and offline.

And finally, on the last part of your question - what needs to change to make safety-by design the default setting ?

If this is what good looks like, how do we force a highly profitable technology market to change its core design models ? Fines are clearly not working; they are simply treated by multi-billion-dollar corporations as the cost of doing business.

We must apply the **precautionary principle** to the tech sector. In the physical world, a pharmaceutical company cannot release a new drug, nor can a toy manufacturer sell a new product, without proving it is safe for children first. Yet, in the digital sphere, tech companies regularly deploy highly addictive algorithms, generative AI companions, and invasive features directly to millions of children, treating them as live test subjects, and only attempting a recall after massive societal harm has occurred.

The EU framework should be updated to require all digital service providers—whether social media, gaming, EdTech, or AI chatbots—to undergo an **independent, ex-ante risk assessment and child-safety pre-certification** before their products or new features can be rolled out to minors.

If a platform cannot prove that its design model prioritizes the best interests of the child over its commercial profit margins, it must be denied access to the market. If children have to wait six or twelve months to access the latest tech feature while it undergoes independent safety auditing, that is a price well worth paying to preserve their mental well-being.

Furthermore, when platforms deliberately violate these design standards, the regulatory stick must be unyielding. We must move beyond financial penalties and introduce **strict market access restrictions** and **criminal director liability** for corporate executives who knowingly expose children to exploitative and dangerous designs. Children should not be banned from the digital world; companies that refuse to build safe products should be banned from accessing children.

Conclusion: creating spaces to grow and thrive

To conclude, the ultimate purpose of digital protection is to give children and young people the environment they need to learn, play, participate, and navigate the world with confidence.

What we need now is the political backbone to stop chasing short-term, ineffective bans and start doing the hard, structural work of enforcing tech accountability upstream.

What we want is to compel the technology sector to build a digital ecosystem that is truly worthy of children: one where their safety is guaranteed by default, and where they are fully empowered to thrive.

Thank you.