



Universiteit
Leiden
The Netherlands

The role of the law in regulating social media's impact on children

Hof, S. van der

Citation

Hof, S. van der. (2025). The role of the law in regulating social media's impact on children. *Media@Lse Blog*. Retrieved from <https://hdl.handle.net/1887/4273638>

Version: Publisher's Version

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/4273638>

Note: To cite this publication please use the final published version (if applicable).

Simone van der Hof

September 19th, 2025

The role of the law in regulating social media's impact on children

0 comments | 1 shares

Estimated reading time: 5 minutes

Simone van der Hof, Professor at Leiden Law School, Leiden University, details here some of the arguments she made during a hearing of the European Parliament's CULT Committee on the effects of social media and the online environment on children.

In 2019, during our university's anniversary event, I delivered a speech about the online economic exploitation of children. I pointed out that we already have legislation to protect children against such exploitation—and against other negative effects of social media—but that enforcement is lacking. At that time, the focus was mainly on the General Data Protection Regulation (GDPR).

Now, six years later, I could give the same speech again: we have laws, but enforcement remains insufficient. We are letting our children down, and in response, we now see **proposals for social media restrictions** that may further violate children's rights.

What's going wrong?

I understand the serious concerns of parents about healthy use of screens by their children. Children spend significant time on devices and in online spaces that are neither age-appropriate nor child-focused, despite existing legal frameworks that require just that. We need to understand why our laws are not having the intended effect: that calls for deeper research. But here, I would like to raise several key points for reflection related to the various legal frameworks in place.

GDPR – strong on paper, weak in practice

One example where we need to do better is the 'one-stop-shop' principle in the GDPR. This grants the power of lead supervisory authority to the authority in the place of establishment of a platform, even if they have an EU-wide reach. This means e.g. that the Data Protection Commission Ireland is the lead supervisor for some of the very large online platforms that children use, because these platforms have chosen to base their European headquarters in Ireland. However, the impact of digital services that reach across the EU is not effectively managed by individual Member States. Just as the Digital Services Act (DSA) provides central supervision by the **European Commission** over Very Large Online Platforms (VLOPs) in Brussels, the GDPR should follow suit.

The GDPR includes provisions to address behavioural profiling of children on online platforms. Yet, despite the clear legal foundation to address these concerns, enforcement remains fragmented and

inadequate and there has been little effort by national supervisory authorities to effectively curb commercial profiling. This is worrying: children are being targeted by commercial practices based on their online and offline behaviour. Parents, academics, and civil society are expressing growing concern over how children are targeted by these exploitative commercial tactics. This digital surveillance is unprecedented in scope and largely invisible. Apps deploy gambling-like mechanisms to trap children in endless loops, drain their attention, and pressure them into making purchases—often more than they intend.

Audio Visual Media Services Directive (AVMSD) – different principle, same problem

The AVMSD's country-of-origin principle means that audiovisual media services such as video sharing platforms are under the jurisdiction of the member state in which they are established (Article 2). While this principle works for national broadcasters, it fails when applied to video-sharing platforms that impact citizens throughout the EU—including millions of children. Although video sharing platforms have been subject to the Audio Visual Media Services Directive (AVMSD) regime since 2018, harmful content in all its forms is widespread. The nature and volume of such content that children can be confronted with online on a daily basis is alarming: they see images of war, suicide, animal cruelty and can end up in endless loops of unhealthy content or misinformation.

Here too, enforcement depends on individual Member States, and does not reflect the cross-border nature of these services. Supervision of platforms with EU-wide reach should be centralised. Country-of-origin and one-stop-shop principles should be limited to companies with a national scope and abandoned for those operating across the EU. A centralised approach would also offer opportunities for an EU system

for content rating on video sharing platforms, which could be linked to national age classification initiatives, similar to the approach of the [International Age Rating Coalition](#) (IARC) for apps and mobile games.

DSA – a big step forward, but not far enough

Interestingly, the Digital Services Act may avoid the enforcement problems of the GDPR and AVMSD. It centralises oversight of VLOPs in Brussels, setting an important precedent, and we can hope the DSA brings real protection for children and enforces obligations for online platforms in the DSA towards age-appropriate design.

Yet even the DSA has its blind spots. Despite regulating digital services, it barely touches the video game industry—a sector worth €455 billion, larger than many online platforms together. As many video and mobile games are not online platforms, they are not covered by the DSA nor the Audio Visual Media Services Directive, which regulates harmful content on video sharing platforms, yet not in games.

This is unfortunate. Children are just as susceptible to safety issues in digital games as on social media. Omitting this sector leaves a major gap in protection. Hopefully, the future [Digital Fairness Act](#) will remedy this to a certain extent, but players, including many children, would benefit from AVMSD- and DSA-specific obligations such as the obligation to protect the privacy, safety and security of minors in Article 28 of the DSA.

Looking forward: there is a role for more concrete guidelines to support enforcement

An important development is the [guidelines](#) under Article 28 of the DSA on proportionate and appropriate measures for child protection on online platforms. The guidelines are promising, and it's positive that the

guidelines were developed so quickly with the help of all stakeholders, including children.

Such guidelines should be mirrored across other EU digital laws. In the case of the GDPR, we've been waiting years for Guidelines on how to interpret the GDPR in relation to children. Further elaboration is needed for other legislation, such as the AVMSD and the AI Act. Such guidelines should go beyond what provisions mean for the rights and wellbeing of children, and provide actual guidance on what it means for apps, games, AI, etc to be truly age-appropriate and child-centred.

With AI, the stakes are especially high: we urgently need concrete guidelines for systems used by or affecting children, and we cannot afford delays like those we saw with online platforms. AI already has a huge impact on younger generations, and we see real harms happen because these systems are not made for children, but may still be attractive to them to experiment with. Like online platforms, AI systems are based on engagement by design and may therefore raise similar concerns in relation to pressure on time and attention, harmful information and unhealthy interactions. Precautionary measures are therefore essential to prevent further harm.

We need to build safer digital spaces and innovation that honours children

To offer children joyful, educational, and healthy online experiences, we need age-appropriate apps and games, we need age-appropriate features and functionalities in generic apps and games. To achieve that, we need to have robust, inclusive, and privacy-friendly age verification throughout the EU. And it's critical we avoid reliance on non-EU technologies—promising zero-knowledge systems developed within the EU, based on EU values, should be prioritised.

Some claim EU digital law holds back innovation. But there's nothing innovative about exploiting children to maximize profit. What's *truly* groundbreaking is designing apps and games that take children's rights and well-being seriously.

This post gives the views of the author and not the position of the Media@LSE blog, nor of the London School of Economics and Political Science.

Featured image: Photo by [Rendy Novantino](#) on [Unsplash](#)

About the author



Simone van der Hof

Simone van der Hof is a full Professor of Law and Digital Technology at the Center for Law and Digital Technology (eLaw) at Leiden Law School, Leiden University. Her research focuses on the intricate relationship between children's rights and digital technologies, with a particular emphasis on three vital dimensions: privacy and data protection, protection against economic exploitation, and the fundamental child right to play. She teaches courses on children's rights and digital technologies in the Advanced Master Law and Digital Technologies, the Advanced Master International Children's Rights and the Master Youth Law and holds various ancillary positions related to her area of expertise.

Posted In: Children and the Media