

NAVIGATING THE DIGITAL FRONTIER: PROTECTING CHILDREN FROM HARMFUL CONTENT IN SOCIAL MEDIA THROUGH PROACTIVE LAWS, IS IT A PROGRESS OR AN OVERREACH?

Elmira Uysal Ljapina*

Abstract: *Given the vulnerability of children and their limited ability to recognize the threats, dangers, and harms of the internet - particularly on social media - as well as the consequences of their actions, and acknowledging the fact that parents or guardians are not always able to prevent potential damage, legislators in recent years have increasingly adopted a proactive approach to mitigate such harm for vulnerable groups. This approach is reflected in the recent implementation of proactive legal measures aimed at protecting minors from harmful online content. These include age barriers for social media registration in jurisdictions such as the USA, Australia, and the UK, higher requirements for digital platforms and intermediaries under frameworks, such as the Digital Services Act Package in the EU, and recent court decisions. By incorporating real-world cases and addressing emerging risks (such as generative AI), this article evaluates whether these measures effectively tackle the complexities of the digital era or inadvertently restrict minors' access to valuable online resources. Finally, it proposes recommendations to balance safety, innovation, and user rights.*

Keywords: *children's rights, online child protection, proactive law, child and technology, social media, children's digital rights*

INTRODUCTION

The role of social media in contemporary life is undeniably complex and controversial. On the one hand, social media function as a popular means of communication and education. On the other, it presents significant threats, including exposure to harmful content, participation in dangerous social media challenges, dissemination of misinformation, cyberbullying,¹ and sexual harassment. These issues often result in adverse negative consequences, particularly psychological effects such as depression and anxiety. Individuals may also fall victim to online scams,² and in extreme cases, these impacts can lead to loss of life.³

* Elmira Uysal Ljapina,, Ph.D., researcher and lecturer, School of Business and IT, University of New York in Prague, Prague, Czech Republic. E-mail: elyapina@unyp.cz. ORCID: <https://orcid.org/0000-0002-1399-5268>.

¹ PATCHIN, J.W., HINDUJA, S. Summary of Our Cyberbullying Research (2007-2023), Cyberbullying Research Center. 2023. In: *Cyberbullying Research Center* [online]. [2026-01-09]. Available at: <https://www.cyberbullying.org/summary-of-our-cyberbullying-research#foobox-1/0/Cyberbullying_Victimization_all_studies_2019.jpg>.

² Federal Bureau of Investigation, Internet Crime Report 2022, Internet Crime Complaint Center. 2022. In: *Federal Bureau of Investigation, Internet Crime Report 2022* [online]. [2026-01-09]. Available at: <https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf>; Report of the Office of the United Nations High Commissioner for Human Rights (2022) Human Rights Council. In: *United Nations General Assembly* [online]. [2026-01-09]. Available at: <<https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf>>.

³ See The U.S. Surgeon General's Advisory. Social Media and Youth Mental Health 2023. In: *Social Media and Youth Mental Health* [online]. [2024-11-01]. Available at: <<https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>>; Pew Research Center. Teens, Social Media & Technology 2022. In: *Pew Research Center* [online]. [2026-01-09]. Available at: <<https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022>>; LAHTI, H., KOKKONEN, M., HIETAJÄRVI, L. et al. Social media threats and health among adolescents: evidence from the health behaviour in school-aged children study. *Child Adolescent Psychiatry Mental Health*. 2024, Vol 18, Issue 62; KATELLA, K. How Social Me-

This controversy is especially pronounced for children, who lack the cognitive maturity to fully comprehend the content they engage with online and the potential consequences of their actions. These risks have led to growing public concern and calls for stricter regulation. Different actors have raised concerns about the dangers and threats posed by social media, urging legislators to adopt stricter age barriers for access. The scholars and activists have also proposed recommendations to safeguard children, including calls for parental intervention to limit social media usage.⁴ Moreover, long-standing discussions around incorporating social media literacy into education for minors and adolescents highlight the necessity for proactive measures, though practical implementation often lags behind.⁵

Recent statistics underscore the extensive reach of social media platforms. In 2022, over three billion individuals worldwide used social networking sites, with Facebook alone surpassing three billion active users by 2024. META's platforms, including Facebook, WhatsApp (with two billion active users), and Instagram (with two billion active users), dominate this digital landscape. Other platforms, such as TikTok (1.5 billion users), Telegram and Snapchat (one billion users each), and X (formerly Twitter, over 600 million users) further highlight the ubiquity of social media.⁶ Globally, individuals spend an average of more than two hours daily in social media.⁷ Furthermore, according to the U.S. Surgeon General, 40% of children aged 8 to 12 and 95% of those aged 13 to 17 use social media apps.⁸ In the UK, the Office of Communications (Ofcom) reported that a majority of children under 13 had profiles on at least one social media platform. Specifically, 33% of parents of children aged 5 to 7 reported their child having a profile, and 60% of children aged 8 to 11 claimed the same. However, only four in ten parents of children

dia Affects Your Teen's Mental Health: A Parent's Guide. Yale Medicine. In: *Yale Medicine* [online]. 17. 6. 2024 [2026-01-09]. Available at: <<https://www.yalemedicine.org/news/social-media-teen-mental-health-a-parents-guide>>; American Psychological Association. Potential risks of content, features, and functions: The science of how social media affects youth. In: *American Psychological Association* [online]. 2024 [2026-01-09]. Available at: <<https://www.apa.org/topics/social-media-internet/youth-social-media-2024>>.

⁴ The Office of the High Commissioner for Human Rights. Call on Empowering Inclusive and Safe Digital Environment for Children. In: *web.test.ohchr.un-icc.cloud* [online]. 2024 [2026-01-09]. Available at: <<https://web.test.ohchr.un-icc.cloud/en/special-procedures/sr-sale-of-children/call-empowering-inclusive-and-safe-digital-environment-children>>.

⁵ UN Committee on the Right of the Child, General comment No. 25 on Children's rights in relation to the digital environment. In: *docstore.ohchr.org* [online]. 2021 [2026-01-09]. Available at: <<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34g-C78FwvnmZXGFU9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMKZRZd37nLN1bFc2t>>.

⁶ Statista. Most popular social networks worldwide as of January 2024, ranked by number of monthly active users. In: *Statista* [online]. 2024 [2026-01-09]. Available at: <<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>>; Pew Research Center. Teens, Social Media & Technology. In: *Pew Research Center* [online]. 2022 [2026-01-09]. Available at: <<https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022>>.

⁷ DIXON, S. J. Daily time spent on social networking by internet users worldwide from 2012 to 2024. In: *Statista* [online]. 2024 [2026-01-09]. Available at: <<https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/>>.

⁸ The U.S. Surgeon General's Advisory. Social Media and Youth Mental Health. In: *Social Media and Youth Mental Health* [online]. 2023 [2026-01-09]. Available at: <<https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>>; Cleveland Clinic. How Social Media Can Negatively Affect Your Child. In: *Cleveland Clinic* [online]. [2026-01-09]. Available at: <<https://health.clevelandclinic.org/dangers-of-social-media-for-youth>>.

aged 3 to 17 were aware of the minimum age requirement social media use. Notably, 38% of parents of children aged 8 to 11 stated they would allow their child to use social media.⁹

Despite the well-documented consequences of harmful social media challenges, their prevalence continues to rise. For instance, the U.S. Third Circuit Court recently held TikTok accountable for promoting harmful content in the *Anderson v. TikTok Inc.*, which involved the tragic consequences of dangerous trends such as the Blackout Challenge.¹⁰ Similarly, the Czech Republic has recently witnessed incidents linked to the swallowing magnets challenge, which poses severe health risks to children.¹¹ Other infamous challenges, such as the Blue Whale and Momo challenges, involve tasks culminating in self-harm or suicide. The other hazardous challenges, where participants ingest laundry detergent pods, setting oneself on fire, choking games, or jumping out of moving vehicles, have led to significant injuries and fatalities.¹² These incidents highlight the profound risks that impressionable minors face when engaging with social media.

Children, as a particularly vulnerable demographic compared to adults, are more susceptible to psychological and physical harm from online interactions. Consequently, there is a widespread consensus that children require enhanced legal protection, even in the context of parental guidance. These protections include age restrictions for social media registration, as seen in jurisdictions such as the USA, as Australia, and the UK. Additional measures include increased responsibilities for digital platforms and intermediaries, as outlined in the European Union's Digital Services Act Package, as well as recent judicial decisions.

This article investigates whether existing legal frameworks and policies are sufficient to protect minors from harmful online content. By examining real-world cases and addressing challenges and emerging risks, the analysis evaluates whether these measures effectively address the complexities of the digital era or if they inadvertently restrict minors' access to valuable online resources.

The article also explores the contentious nature of these interventions. For instance, in cases where children benefit from stable family environments, educational opportunities, and safe spaces to discuss offline (or online) threats, overregulation may prove unnecessary. Moreover, critics contend that regulatory measures could infringe upon parental rights, privacy rights, freedom of expression, and access to information.

This article argues that while proactive laws mark meaningful progress in protecting children from online harm, certain legislative approaches risk overreach, particularly

⁹ UK's Office of Communications. Children and parents: Media use and attitudes report 2022. In: *Ofcom* [online]. [2026-01-09]. Available at: <<https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-use-and-attitudes-2022/childrens-media-use-and-attitudes-report-2022.pdf?v=327686>>.

¹⁰ Case of *Anderson v. TikTok Inc.*, No. 22-3061 (3d Cir. 2024). Justia Law. In: *JUSTIA U.S. Law* [online]. [2026-01-09]. Available at: <<https://law.justia.com/cases/federal/appellate-courts/ca3/22-3061/22-3061-2024-08-27.html>>.

¹¹ ČTK. Nebezpečná výzva z TikToku. Děti spolky magnety a uvízly jim v tělech. *Pražský deník*. In: *Pražský deník* [online]. 2024 [2026-01-09]. Available at: <https://prazsky.denik.cz/zpravy_region/magnet-dite-spoklnuti-piercing-vyzva-tiktok-fn-motol-praha.html>.

¹² CRUZ, B., TURNER, G. Top 10 Most Dangerous Online Challenges. Security.org. In: *security.org* [online]. 2023 [2026-01-09]. Available at: <<https://www.security.org/digital-safety/most-dangerous-online-challenges/>>.

where they restrict children’s autonomy or privacy. Through an analysis of selected policies, laws, practices, and research, this article aims to consider the challenges and solutions for the protection of minors in the digital age. The study seeks to ensure a balanced approach that considers safety and fundamental rights, framing the central debate: Do age restrictions and proactive laws represent meaningful progress or unintended overreach?

I. INTERNATIONAL LEGAL FRAMEWORKS FOR CHILD PROTECTION

The Convention on the Rights of the Child (CRC) (1990) serves as a fundamental framework for the protection of children’s rights, emphasizing their entitlement to access information, freedom of expression, privacy, and protection from harm.

In the context of the digital world, these rights translate into ensuring equitable and safe access to the internet and digital technologies while protecting children from harmful content, exploitation, and abuse. This interpretation is reinforced by various guidelines and documents issued by the UN Committee on the Rights of the Child, including its General Comments, which provide recommendations for the states on how to uphold children’s rights in relation to the digital environment. These documents highlight the importance of ensuring that all children have equal and meaningful access to the digital world.

Key principles underpinning the CRC include non-discrimination, which ensures that children are protected from harmful online content and digital access is inclusive and equitable. This principle extends to safeguarding children from hateful communication and discriminatory practices that could exclude them from the benefits of the digital environment.

Another crucial principle is the Best Interests of the Child, which obliges states to implement contextually appropriate measures that prioritize children’s well-being in digital contexts. The Right to Life, Survival, and Development further mandates states to protect children from risks to their physical and psychological well-being, addressing threats such as exposure to violent or sexual content, cyberaggression, harassment, exploitation and suicide-related activities. The Committee stresses the importance of listening to children’s perspectives on the risks they face online.¹³

The principle of Respect for the Views of the Child is also central, emphasizing that children’s voices should be heard and integrated into the design and implementation of digital policies. To foster this, promoting digital literacy is essential, enabling children to navigate the digital world safely and effectively.

The Committee also stresses that these principles and recommended state actions must align with fundamental rights and freedoms. These include the freedom of expression, freedom of thought, conscience, and religion, freedom of association and peaceful

¹³ Para 14, UN Committee on the Right of the Child, General comment No. 25 on children’s rights in relation to the digital environment. In: *docstore.ohchr.org* [online]. 2021 [2026-01-09]. Available at: <<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPrCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2B-cAAx34gC78FwvnmZGXFUlnJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMKZRZd37nLN1bFc2t>>.

assembly, as well as the right to access information, the right to privacy, and the right to identity.

II. VARIATIONS IN IMPLEMENTATION ACROSS COUNTRIES

While the CRC provides a comprehensive framework, however it provides more freedom of implementation to the decision makers in each country based on particular cases, thus its implementation varies significantly across countries. Even among nations that have ratified the CRC, differences arise due to varying interpretations and reservations regarding parental authority and the rights of parents to raise their children according to their beliefs. These disparities reflect the challenges of balancing internationally recognized fundamental human rights with the unique child protection needs within diverse legal and cultural contexts.

The increasing interchangeability between social media and the broader internet is a notable trend, particularly given the ways these platforms are utilized. Public officials increasingly rely on social media as a medium for sharing opinions, issuing statements, and disseminating important legal information. Similarly, mass media often use social media posts as sources for news reporting or as supporting materials. These practices have blurred the once-clear distinctions between public forums, the internet, and social media platforms. As a result, the conceptual and functional boundaries between these entities are eroding, complicating legal and regulatory approaches to digital governance.

Some countries have adopted stricter legislative measures aimed at protecting minors from digital harm, which sometimes intersect with or even overlap parental authority. These include measures that regulate online privacy, such as the EU General Data Protection Regulation (GDPR), and the U.S. Children’s Online Privacy Protection Act (COPPA), as well as laws prohibiting the spread of pornography and regulating hate speech and defamation online. Interestingly, the legislators are attempting to tackle any potential harm to the child, including their protection from the potential predators, as those accused in sexual abuse or assault. However, dimensions of that are not always clear, since the protection of the vulnerable minority can contradict the constitutional rights of even potential harmful person. In the following sections the paper provides the overview of some activities of particular developed countries, in order to follow their proactive measures to protect the child and child’s privacy in the digital sphere. The overview includes the United States (section III), United Kingdom and Australian approaches (section IV) due to their recent legislative amendments regarding the restriction of the minors under 13 years old in the social media space. Then, it provides the approach of the European Union, and particular case studies in some EU Member States (section V). It will help to understand the tendency of the legislators, but also to reflect on the contradictions between the particular rights of the actors in the digital sphere.

III. CHILD PROTECTION IN THE UNITED STATES

III.1 COPPA

The U.S. approach to online child protection is primarily driven by several legislative measures aimed at safeguarding minors. A key piece of legislation is the Children’s On-

line Privacy Protection Act (COPPA), enacted in 1998. COPPA regulates the collection of personal information from children under the age of 13, requiring websites and online services, operating within or under U.S. jurisdiction, to obtain verifiable parental consent before collecting data. However, COPPA has faced criticism for being outdated, as children often bypass age verification, undermining its effectiveness. Additionally, concerns have been raised about the law's potential conflict with the First Amendment, given the robust protections from free expression in the U.S. Critics argue that COPPA may not adequately address modern online risks.¹⁴ Another law, aimed to extend protections to children enhancing the online safety is proposed bill on Kids Online Safety Act (KOSA).¹⁵ It is important to mention that the Constitutional laws, such as the principles of the First Amendment (incl. on the freedom of expression), or the Fourth Amendment (on the privacy rights) are implemented by the Supreme Court widely on the internet, since it is considered to be a *public forum*.

III.2 Local attempts

In the United States, some states have attempted to regulate the internet through local legislation, though these efforts have not always been successful. The reason of it is the mentioned clash of the rights of the actors in the digital sphere, in the frame of the provided case – the rights of the users: the children and the registered sex offenders. Whereas the potential harm of the sex offender might be discussed and even foreseen, however the fundamental rights of the citizen (even the sex offender), in particular – right to freedom of expression, might overweight the right of the child for the safe use of the internet. This is the landmark case *Packingham v. North Carolina*, 582 U.S. (2017),¹⁶ where the state of North Carolina sought to protect minors by banning registered sex offenders from accessing social media platforms through the state law. However, the Supreme Court ruled this legislation unconstitutional, emphasizing that it infringed upon the First Amendment's protections of free speech. Thus, stating that the proactive approach in protection of the child on the internet must find the balance, and once it is tackling the rights and freedoms of the other users, it is a clear overreach. The Supreme Court stressed, that even “*convicted criminals – and in some instances especially convicted criminals – might receive legitimate benefits from these means for access to the world of ideas, in particular if they seek to reform and to pursue lawful and rewarding lives*” (pp. 6–8). Given that example, it is however important to mention the U.S. approaches to the states' legislative attempts, where it is required from them to make the laws narrowly tailored to particular circumstances, serve a significant governmental interest, and prove that the particular law is necessary to protect the vulnerable victims.

¹⁴ Children's Online Privacy Protection Rule ('COPPA'). Federal Trade Commission. In: *Federal Trade Commission* [online]. [2026-01-09]. Available at: <<https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>>.

¹⁵ UNICEF USA. Children's Right to Online Safety Must Be Protected. In: *Unicef USA* [online]. 2022 [2026-01-09]. Available at: <<https://www.unicefusa.org/stories/childrens-right-online-safety-must-be-protected>>.

¹⁶ *Packingham v. North Carolina*, 582 U.S. ____ (2017). Justia law. In: *JUSTIA U.S. Supreme Court* [online]. [2026-01-09]. Available at: <<https://supreme.justia.com/cases/federal/us/582/15-1194/>>.

In contrast, the California Consumer Privacy Act (CCPA)¹⁷ stands as an example of well-crafted legislation. The CCPA has been widely regarded as a model for balancing consumer privacy with practical regulatory frameworks, demonstrating how state-level initiatives can effectively address specific challenges in the digital age. Specifically, within a frame of the use, sale and share of the personal information of the child it is required from the businesses to get an affirmative authorization from the child aged 13-15 years old, and from the parents (or guardians) - for the children under 13. The businesses are encouraged to take measures verify the age of users, and in case they haven't received the necessary (above mentioned) consent – they are prohibited from selling the personal information of such a minor consumer (especially if they had been directed not to do so). Although, this law is considered to be a well-written to fulfil the requirements of the U.S. approach within Supreme Court's interpretations, however the subject-matter itself is debatable, whether it is sufficient for the protection of the child, given the minors' personal information being sold and/or shared, including the concerns about the obligations of the businesses, which seem to be easily bypassed, as well as the consent of the child/parent/guardian itself. Given this example, it can be discussed about the proactive steps, however are these steps sufficient to protect the vulnerable ones? That's and open question, considering which the scholars and politicians are trying to tackle the above-mentioned issue by the amendments to the federal laws.

III.3 COPPA 2.0.

One of the discussed amendments, which regards the protection of the child in the digital sphere is the Children and Teens' Online Privacy Protection Act (COPPA 2.0). It proposes to amend federal law by raising the age threshold for online privacy protections from 13 to 17. This amendment aims to enhance safeguards for older minors by introducing several key provisions. These include the concept of data minimization, the right to erasure for personal data, and the potential prohibition of targeted advertisements aimed at minors.¹⁸

However, these measures raise concerns about exceeding parental rights by limiting access to information about their child's social media activities. As it was mentioned in the previous section, the digital sphere provides not only harmful ideas, but also serves opportunities for growth and development of the child, not even mentioning the exchange of ideas between the same age users, but also it is a modern way of communication and sharing the information, even between the educational centers or schools and the students and/or their parents.

On the other side, given several issues highlighted by the documentaries about the “predators” in the social media, the sex offenders and persons convicted of pedophilia, including the harmful challenges, leading to fatal consequences for the minors, it is hard

¹⁷ State of California - Department of Justice - Office of the Attorney General. Protecting Your Child's Privacy Online. In: *State of California Department of Justice* [online]. 2012 [2026-01-09]. Available at: <<https://oag.ca.gov/privacy/facts/online-privacy/child-privacy>>.

¹⁸ SINGER, N. DeSantis Vetoes Blanket Social Media Ban for Youths Under 16. In: *The New York Times* [online]. 2014 [2026-01-09]. Available at: <<https://www.nytimes.com/2024/03/01/technology/desantis-florida-ban-tiktok-instagram.html>>.

to not recognize the importance of the social media illiteracy of the users, especially children. Given the fact, that the parents are not always able to follow what their children are doing in the internet, nor even check the respondent of the message, the issue seems important to be regulated “from above”.

Thus, the movement to raise the minimum age for social media registration reflects growing concerns about the safety and well-being of minors online. The rationale for this proposal extends beyond the previously discussed factors and includes several additional considerations. Psychological vulnerability is a primary concern, as adolescents are particularly susceptible to social pressures and negative online interactions, which can significantly affect their mental health.¹⁹ Another key factor is data privacy concerns, as minors often lack a full understanding of the implications of sharing personal information online. This lack of awareness increases their risk of data exploitation and related harms. Finally, the exposure to harmful or inappropriate content presents a developmental risk for minors, further underscoring the need for stricter age regulations.²⁰

III.4 Section 230 of CDA and the spread of harmful content

When discussed about the actors in the digital sphere – it is not only the users: children and the potential harmful persons. Most of the internet is run by the private companies, large corporations, as META, Google, etc. The question tackled by many countries, including the U.S. and the European Union, as a whole, as it will be discussed later, is whether and how to protect the vulnerable ones, by regulating not only those who are directly involved, but also those, who provide the possibilities, as for the exchange of the ideas, so for the harmful communication. Within the U.S. such proactive attempt is the controversial Section 230 of the Communications Decency Act (CDA), which however offers immunity to online platforms for content generated by users, while still requiring the removal of harmful material, violating federal or state laws, such as copyright infringement or human trafficking. This infamous Section 230 has been nevertheless criticized for fostering over-censorship and a lack of accountability and enabling the spread of harmful content.²¹

One of the cases highlighting this issue is in recent court decisions, such as *Anderson v. TikTok*. This case arose from the tragic consequences of the Blackout Challenge, which led to fatal consequences for the child attempting this “choking challenge”. The progress of the case consideration signal a significant shift in how courts are holding social media platforms accountable for their algorithm. While the Eastern District of Pennsylvania, as the court of first instance, dismissed the case, citing Section 230 immunity, the

¹⁹ American Psychological Association. Potential risks of content, features, and functions: The science of how social media affects youth. In: *American Psychological Association* [online]. 2024 [2026-01-09]. Available at: <<https://www.apa.org/topics/social-media-internet/youth-social-media-2024>>.

²⁰ NOMINET, T. B., Social media minimum age limits and experiences of distress for underage children online. Market Analyst at Digital Youth Index. In: *nominet* [online]. [2026-01-09]. Available at: <<https://digitalyouthindex.uk/social-media-age-limits/>>.

²¹ Harvard Law Review. Section 230 as First Amendment Rule. Harvard Law Review. In: *Harvard Law Review* [online]. [2026-01-09]. Available at: <<https://harvardlawreview.org/print/vol-131/section-230-as-first-amendment-rule/>>.

Third Circuit Court of Appeals partially overturned this ruling. The appellate court determined that TikTok’s algorithmic recommendations constituted first-party speech rather than third-party content, allowing the lawsuit to proceed.²²

By holding platforms accountable for the design and impact of their algorithms, the Third Circuit Court has set a precedent that could fundamentally reshape the responsibilities of social media companies. This decision emphasizes the need for platforms to consider the consequences of their algorithmic designs. Although, the case was also criticized for tackling the particular corporation (TikTok) due to political reasons, however the shift was clearly made, despite the protection under Section 230 CDA.

Although, considering the Court’s approach, it can be discussed about the proactive stance and even progress towards the protection of the minors, nevertheless, critics warn that such rulings could inadvertently create a chilling effect on innovation and free expression if platforms are excessively penalized for unintended outcomes of their algorithms.

III.5 Achieving balance reflecting international standards

From a critical thinking perspective, these developments raise important questions about achieving the right balance between safety, accountability, and fundamental freedoms in digital governance. While efforts, as COPPA and its proposed amendments (e.g. COPPA 2.0.) are commendable steps toward improving online protections for minors, critics argue that they may not fully address the rapidly evolving risks of the digital landscape.²³ For instance, while raising the age threshold, as proposed under COPPA 2.0, could enhance safeguards for older minors, it may also inadvertently limit teenagers’ access to valuable online resources and supportive communities. Additionally, such measures could introduce new challenges in protecting minors’ privacy, highlighting the need for a nuanced approach to regulation.

In this context, it is pertinent to highlight Article 16 of the UN CRC, which states:

1. *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation.*
2. *The child has the right to the protection of the law against such interference or attacks.*

²² FARRINGTON, B. Florida lawmakers pass ban on social media for kids under 16 despite constitutional concerns. [online] AP News. In: *AP News* [online]. [2026-01-09]. Available at: <<https://apnews.com/article/social-media-florida-government-2a11f9a4e9256eae341a3d54c439c5af>>.

²³ LEARY, G. The Indecency and Injustice of Section 230 of the Communications Decency Act. In: *ssrn.com* [online]. [2026-01-09]. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3160055>; Mercatus Center. Protecting Children Online: Evaluating Possible Reforms in the Law and the Application of COPPA. In: *Mercatus Center George Mason University* [online]. 2023 [2026-01-09]. Available at: <<https://www.mercatus.org/research/policy-briefs/protecting-children-online-evaluating-possible-reforms-law-and-application>>; NABIL, R. The Amended Children and Teens Online Privacy Protection Act (COPPA 2.0): Why This Well-Intentioned Legislation Could Disadvantage American Teens Relative to Their International Competition. National Taxpayers Union. In: *National Taxpayers Union* [online]. 2023 [2026-01-09]. Available at: <<https://www.ntu.org/publications/detail/the-amended-children-and-teens-online-privacy-protection-act-coppa-20-why-this-well-intentioned-legislation-could-disadvantage-american-teens-relative-to-their-international-competition>>.

This provision underscores the child's fundamental right to privacy, which extends protection against interference by parents, guardians, caretakers, or even public authorities, irrespective of the reasonableness of their interests. Such interventions, though potentially well-intentioned, may still infringe upon this essential right.

Similar protections are enshrined in other international conventions, including:

Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 22 of the Convention on the Rights of Persons with Disabilities, Article 11 of the American Convention on Human Rights, Article 10 of the African Charter on the Rights and Welfare of the Child, and Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

These provisions collectively reflect a global commitment to ensuring that the right to privacy remains a cornerstone of child protection, even in the face of competing interests from other stakeholders.

The U.S. approach shows both innovation and constitutional limits, demonstrating the tension between safeguarding children and preserving freedom of expression. The following section compares this with developments in the United Kingdom and Australia, where regulators have pursued more interventionist strategies that raise their own privacy concerns.

IV. CHILD PROTECTION IN THE UNITED KINGDOM AND AUSTRALIA

Both the United Kingdom (UK) and Australia have made significant strides towards raising the minimum age for social media access and implementing more stringent online safety laws. These efforts reflect a broader global trend toward enhancing the protection of minors in digital spaces.

As have been discussed in previous section, the enforcement of age verification measures poses several challenges. Concerns include the potential compromise of children's privacy and the risks of excluding minors from safe and beneficial online communities. Despite these issues the push for stricter age thresholds has gained traction worldwide.

IV.1 Legislative developments in Australia

In Australia, the Online Safety Amendment (Social Media Minimum Age) Bill was passed, and it prohibits adolescents under 16 from accessing social media platforms. Companies found in violation of this law face costly penalties.²⁴ Similarly, the Online Safety Act 2021, which includes the Basic Online Safety Expectations Determination 2022, aims to combat child exploitation and abuse online. However, these laws have faced criticism for potentially enabling excessive data surveillance, raising privacy concerns.²⁵

²⁴ Parliament of Australia. Online Safety Amendment (Social Media Minimum Age) Bill. In: *Parliament of Australia* [online]. [2026-01-09]. Available at: <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd39>.

²⁵ Online Safety Act (2022). (Basic Online Safety Expectations) Determination 2022. In: *Parliament of Australia* [online]. [2026-01-09]. Available at: <<https://www.legislation.gov.au/F2022L00062/latest/text>>.

investigations³⁴ into several services following evidence of harmful content and grooming. In this context, the reasoning of *Big Brother Watch and Others v. the UK* remains pertinent, as the ECtHR recognized that surveillance measures are often justified by serious threats such as child exploitation,³⁵ while requiring adequate safeguards to protect the right to privacy.

IV.3 Global implications and regulatory challenges

The debate over balancing child protection with privacy and freedom of expression is not unique to the UK and Australia. For instance, the EU Regulation 2021/1232, addressing child sexual exploitation and abuse, temporarily overrides certain provisions of Directive 2002/58/EC to allow providers to process data for combating online child sexual abuse. However, these measures are constrained by principles legality, necessity, and proportionality, as emphasized by the Committee on the Rights of the Child.³⁶

The Office of the United Nations High Commissioner for Human Rights (2022) has warned about growing use of digital surveillance technologies, highlighting the tension between the privacy rights and the need for effective regulation. Investigative reports have documented the increasing use of surveillance tools by governments worldwide, underscoring the risks these pose to individual freedoms.³⁷

Given these examples, the issue of the privacy of other users is an additional concern to the mentioned above freedom of expression. Although, the privacy in digital sphere, despite the existing legal frameworks, either national, international or regional, is usually not a central issue, while considering other “more important” human rights, and it might be neglected due to the given restrictions of such right (such as national security, criminal offence, public order, etc.), however it cannot be fully ignored given its recognition as a human right across the legislations. Thus, proactivity of the legislators is still somewhere on a border between the overreach and progress, once it lacks the systemic approach and cooperation of several involved actors.

While the UK and Australia have emphasized minimum ages and platform liability, these approaches risk intrusive surveillance. The next section will turn to the EU, where systemic regulation seeks to balance safety with children’s fundamental rights, though enforcement gaps remain, as well as the essential factor of harmonization across the Union.

³⁴ OFCOM. *Ofcom investigates Telegram and teen chat sites* [online]. London: Ofcom, 21. April 2026. [2026-05-01]. Available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/ofcom-investigates-telegram-and-teen-chat-sites>

³⁵ See paragraph 323 of the Judgement of the ECtHR, *Big Brother Watch and Others v. the United Kingdom* (App. nos. 58170/13, 62322/14, 24960/15). 25. May 2021 [2026-05-01]. Available at: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%7B%22001-210077%22%7D%7D>

³⁶ Para 70, UN Committee on the Right of the Child, General comment No. 25 on children’s rights in relation to the digital environment. In: *docstore.ohchr.org* [online]. 2021 [2026-01-09]. Available at: <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhskirKQZLK2M58RF%2F5F0vEG%2B-cAAx34gC78FwvnmZXGFU19nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMKZRZd37nLN1bFc2t>.

³⁷ FELDSTEIN, S. Governments Are Using Spyware on Citizens. Can They Be Stopped? In: *carnegieendowment.org* [online]. 2021 [2026-01-09]. Available at: <https://carnegieendowment.org/posts/2021/07/governments-are-using-spyware-on-citizens-can-they-be-stopped?lang=en>.

V. THE EUROPEAN UNION'S APPROACH

V.1 The contradiction between the protection of the child and the fundamental values of the EU

While discussing the protection of the child within the European Union, it is important to pay attention to the correlation between EU law and the laws of the EU Member States. While the Article 2 of the Treaty on European Union (TEU) promotes the fundamental values of the EU, Article 3 (paragraphs 3 and 5) aims at the specific protection of the right of the child, within the broader framework of human rights protection. This includes areas such as combatting social exclusion and discrimination, promotion of justice and protection, gender equality, solidarity between generations, peace, security, sustainable development, solidarity and mutual respect, free and fair trade, and the eradication of poverty, all in alignment with the principles of the UN Charter.

Thus, the main Treaties of the EU, including the mentioned TEU, or the Treaty on Functioning of the European Union, or the Charter of Fundamental Rights of the EU, establish the protection of the child as a principal objective, addressing related issues that require specific attention to the rights of the child, such as personal data protection, or prohibition of child labor. While providing a foundation and acknowledgment of the importance of the protecting the child both within the EU and beyond, the EU, while recognizing the primary responsibility of the EU Member States for protecting the rights of the child within their internal borders, nevertheless focuses on the harmonization and promotion of policies concerning the rights of the child. It complements the actions of the Member States by addressing areas that require inter-state cooperation, such as the cross-border issues, including the recognition of judgments.

When a Member State violates the fundamental values of the European Union, the infringement procedure serves to highlight and address such issues.

One of such cases where the European Commission had to involve in and start an infringement procedure, is the case of Hungary, which adopted a Law LXXIX of 2021, aimed at protecting minors, introducing stricter measures against individuals convicted of paedophilia and amending certain child protection laws. Certain amendments introduced by this law, however, in claim of the European Commission³⁸ and in the Opinion Advocate General Ćapeta³⁹ prohibit or restrict access to content that depicts or promotes “gender identities that do not correspond to the sex assigned at birth, sex reassignment, or homosexuality” (LGBTI content).⁴⁰

The European Commission determined that these amendments violated EU law on multiple levels, including the fundamental principles set out in Article 2 of the Treaty

³⁸ Case C-769/22, European Commission v. Hungary. In: *InfoCuria* [online]. [2026-01-09]. Available at: <<https://curia.europa.eu/juris/documents.jsf?num=C-769/22>>.

³⁹ Opinion of advocate general Ćapeta delivered on 5 June 2025 (1) Case C-769/22 European Commission v. Hungary. In: *InfoCuria* [online]. [2026-01-09]. Available at: <<https://curia.europa.eu/juris/documents.jsf?num=C-769/22>>.

⁴⁰ Para 2 Opinion of advocate general Ćapeta delivered on 5 June 2025 (1) Case C-769/22 European Commission v. Hungary. In: *InfoCuria* [online]. [2026-01-09]. Available at: <<https://curia.europa.eu/juris/documents.jsf?num=C-769/22>>.

In its judgment of 21 April 2026 in Case C-769/22 (Commission v Hungary), the Court of Justice of the European Union confirmed the findings of the Advocate General, and held that Hungary's child-protection legislation, although justified by reference to the best interests of the child, resulted in serious violations of fundamental rights. The Court found that restrictions on content portraying LGBTI identities were discriminatory and incompatible with the Charter, as they infringed dignity, privacy, and freedom of expression.

The Court further clarified that parental rights in education, under Article 14(3) of the Charter, must be interpreted in light of pluralism and do not entitle parents to shield children from differing views.⁴³ Crucially, the Court emphasized that neither child protection objectives nor parental rights can justify measures that undermine fundamental rights or discriminate on the basis of sexual orientation.

Thus, the CJEU in the case of Hungary confirmed that the proactive approach of the state in fact is an overreach. All this in recognition of the other cases resolved by the CJEU⁴⁴ on the margin of discretion that the choice of how to protect the physical, mental and moral development of minors, or how to safeguard parental rights is a matter for each EU Member State, however within particular limitations and within balancing the rights.

V.2 The GDPR' functional basis for the protection of minors

In the European Union (EU), discussions regarding the establishment of a minimum age for social media use are less prominent compared to broader debates on online safety and the protection of minors. Partially because they were already introduced earlier, including the General Data Protection Regulation (GDPR). However, individual cases and regulatory actions have highlighted the need for robust measures to protect vulnerable users.

Incidents such as the Blackout Challenge (similar case was discussed in section III, within the case *Anderson v. TikTok* in the U.S.), which led to the tragic death of a ten-year- in Palermo,⁴⁵ prompted significant regulatory responses. In 2021, the Italian Data Protection Authority (DPA) issued interim measures against TikTok, restricting its ability to process the data of users, residing in Italy, whose age could not be reliably verified.⁴⁶ These actions were grounded in the GDPR, which sets the age of consent for data pro-

⁴³ See paragraphs 149-152 of the Judgement of the CJEU. *Commission v Hungary* (C-769/22). 21. April 2026 [2026-05-01]. Available at: https://infocuria.curia.europa.eu/tabs/affair?lang=en&sort=AFF_NUM-DESC&searchTerm=%22C-769%2F22%22&publishedId=C-769%2F22&jurisdiction=C

⁴⁴ *Omega* (C-36/02) and *Booky.fi* (regarding labelling of audiovisual programs with the aim of the protection of children C-662/21).

⁴⁵ ROBERTS, H., LEALI, G. TikTok is the latest target in Italy's crusade against Big Tech. In: *Politico* [online]. 2021 [2026-01-09]. Available at: <<https://www.politico.eu/article/tiktok-latest-target-italy-privacy-regulator-crusade-against-big-tech/>>.

⁴⁶ Italian DPA imposes limitation on processing on TikTok after the death of a Girl from Palermo. European Data Protection Board. In: *European Data Protection Board* [online]. 2021 [2026-01-09]. Available at: <https://www.edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_it>; LETTIG, D. Italian DPA imposes TikTok ban for users unverifiable by age. In: *Euractiv* [online]. 2021 [2026-01-09]. Available at: <https://www.euractiv.com/section/politics/short_news/italian-dpa-imposes-ticktock-ban-for-users-unverifiable-by-age/>.

cessing at 16 [Article 6(1)(s)], but allows Member States to lower this threshold to 13 [Article 8(1)]. Italy’s national legislation sets the minimum age at 14, and TikTok’s non-compliance with these measures at its best consideration for the specific EU Member State – Italy – underscored the challenges of enforcing consistent standards across the EU.

The GDPR emphasizes in Recital No. 38, that “children merit specific protection” due to their limited awareness “of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data”. This protection applies particularly in contexts such as marketing, profiling, and the collection of personal data during the use of services offered directly to a child. The TikTok case established a persuasive precedent that has influenced the approach to age verification across the EU and accelerated the adoption of further EU legislation aimed at protecting minors, even indirectly, tackling the intermediaries, as discussed in the section III within U.S. Communication Decency Act, s. 230, and in the following paragraphs within the EU’s DSA.

V.3 Proactive attempts towards intermediary platforms via Digital Services Act

The Digital Services Act (DSA) represents the EU’s most comprehensive effort to regulate the digital environment, focusing on transparency, accountability, and user safety. Although the DSA does not explicitly mandate a minimum age for social media use, it requires platforms to implement age verification measures as part of broader obligations to protect users, particularly minors. These measures reflect the principles outlined in the UN Child Rights Committee’s guidance on safeguarding children’s rights in the digital environment⁴⁷ and the Charter of Fundamental Rights of the European Union,⁴⁸ which emphasizes the Child’s Best Interests.

The DSA, harmonizes different national laws in the European Union and incorporates several key provisions to protect minors, reflecting the fundamental rights and principles of children’s protection, including non-discrimination, freedom of expression, and privacy rights, obliging the online platforms to act in the “best interests of the child”.

It requires the Very Large Online Platforms and Very Large Online Search Engines to identify, assess and mitigate potential online risks for minors, including providing parental controls, age verification tools, and mechanisms for report abuse or get support by users. The Article 24 together with Article 45 require platforms to present terms of service in a manner understandable to children, and to introduce the age-appropriate design requirements. Further, the Article 28 prohibits targeted advertising directed at children. These measures aim to hold digital platforms to higher standards for protecting children.⁴⁹

The DSA further emphasizes algorithmic transparency and cooperation between national regulators and the European Commission, supported by the European Centre for

⁴⁷ OHCHR. Guidance establishes children’s rights carry into digital world. In: *OHCHR* [online]. 2021 [2026-01-09]. Available at: <<https://www.ohchr.org/en/stories/2021/03/guidance-establishes-childrens-rights-carry-digital-world>>.

⁴⁸ Article 24 (2).

⁴⁹ European Commission. The Digital Services Act package. Shaping Europe’s digital future. In: *European Commission* [online]. 2022 [2026-01-09]. Available at: <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>>.

Algorithmic Transparency (ECAT). Platforms are required to disclose their algorithms, advertising practices, and content moderation processes, enabling regulators to address potential issues proactively. This transparency is intended to empower users and foster trust by simplifying the reporting of illegal content and ensuring accessible mechanisms for appealing moderation decisions.

While legislators might see it as a progressive and proactive measure to tackle the digital corporations, the corporations themselves see it as an overreach. Thus, despite DSA's recent implementation (in 2024), it has already been subject to significant legal scrutiny.

The Amazon contested its classification as a Very Large Online Platform, arguing that certain transparency obligations imposed excessive burdens. Although the Court of Justice of the European Union (CJEU) dismissed Amazon's request for interim measures, emphasizing in para 164 the prevail of the EU law over "Amazon's material interests".⁵⁰

The digital corporations are reluctant to comply with the DSA, and often attempt to find the gaps in the legislation or challenge it, using different instruments to protect its interests, including the inefficient age-verification mechanisms or infamous use of algorithms and Artificial Intelligence.

Concerning the protection of minors online, the European Commission launched a probe into META's adherence to DSA obligations. Commission in its press-release mentioned the concerns "that the systems of both Facebook and Instagram, including their algorithms, may stimulate behavioral addictions in children, as well as create so-called 'rabbit-hole effects'. In addition, the Commission is also concerned about age-assurance and verification methods put in place by META".⁵¹

Although, in response to the DSA, META has introduced improved age verification processes to prevent underage users from accessing its platforms (including the use of artificial intelligence to detect age discrepancies and prompt users to provide age verification), however, Commission raised concerns about the reliability of Meta's age verification systems.⁵² Reports suggest that underage users can still access the platforms by providing false information, indicating a need for more robust verification methods. Investigations have found that minors are still exposed to harmful content, including material related to self-harm and eating disorders. This highlights potential shortcomings in content moderation practices and the algorithms used to recommend content.

The European Commission has noted that META's transparency reports lack detailed information on measures taken to protect minors. Additionally, there are

⁵⁰ Order of the Vice-President of the Court of 27 March 2024, *European Commission v Amazon Services Europe Sàrl.*, Case C-639/23 P(R). (2024). EUR-Lex - 62023CO0639(01) - EN - EUR-Lex. In: *EUR-Lex* [online]. [2026-01-09]. Available at: <[https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62023CO0639\(01\)](https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62023CO0639(01))>; CJEU Press Release. In: *Court of Justice of the European Union* [online]. 2024 [2026-01-09]. Available at: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp240060en.pdf>>.

⁵¹ European Commission – press release. In: *European Commission* [online]. 16. 5. 2024 [2026-01-09]. Available at: <https://ec.europa.eu/commission/presscorner/detail/hy/ip_24_2664>.

⁵² *Ibid.* In April 2026 Commission preliminary found META liable for non-compliance with DSA - for failing to diligently identify, assess and mitigate the risks of minors under 13 years old accessing their services, more: European Commission – press release. In: *European Commission* [online]. 26.4.2026 [2026-05-01]. Available at: <https://ec.europa.eu/commission/presscorner/detail/hy/ip_24_2664>.

concerns about the effectiveness of user reporting mechanisms and Meta's responsiveness to regulatory oversight. The non-compliance of META with EU law could entail the formal opening of proceedings pursuant to Article 66 of the DSA. Potential non-compliance, or incorrect, incomplete, or misleading information could result in significant fines imposed by Commission under the DSA framework, pursuant to Article 74 (2) of the DSA, including fines up to 6% of its global annual turnover. And potential further failure to reply by the deadline could lead to the imposition of periodic penalty payments.

Commission requested for information TikTok, Snapchat, YouTube regarding the design and functioning of its recommender systems in relation to elections,⁵³ in particular to provide detailed information on how it analyzed and mitigated the risk of inauthentic or automated exploitation of its service and the risks stemming from its recommender systems. The Commission is also asking information about TikTok's efforts to enable a wider range of third parties to conduct public scrutiny, as well as have access to publicly accessible data to detect, identify and understand systemic risks related to electoral processes in Romania, under DSA stressing the importance of a safe, predictable and trustworthy online environment.

Similarly to META, the Commission opened formal proceedings against Temu under the DSA in areas linked to the sale of illegal products, the potentially addictive design of the service, could have negative consequences to a person's physical and mental well-being, the systems used to recommend purchases to users, as well as data access for researchers.⁵⁴

This investigation is part of a wider effort by the European Union to enforce the DSA and ensure that large online platforms adhere to stringent standards for user safety, particularly concerning vulnerable groups, as minors.

The outcome of these requests and probes will likely have significant implications for how social media companies operate within the EU, potentially setting precedents for future regulatory actions aimed at safeguarding children in digital environments. With comprehensive approach it will potentially lead to improved online safety outcomes. Platforms have adopted stricter age verification processes and enhanced privacy settings, resulting in a safer online environment for young users.

While the DSA represents a proactive regulatory framework, it has faced criticism on several topics. Differing cultural norms and legal frameworks across EU Member States pose challenges in uniformly enforcing the DSA's provisions. For instance, the interpretation of what constitutes harmful content can vary, complicating consistent application of regulations. Thus, DSA was also criticized, due to the possibility of the authorities in

⁵³ European Commission. The Digital Services Act package | Shaping Europe's digital future. In: *European Commission* [online]. 2022 [2026-01-09]. Available at: <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>>; Shaping Europe's digital future. Commission sends additional request for information to TikTok under the Digital Services Act. In: *European Commission* [online]. [2026-01-09]. Available at: <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-additional-request-information-tiktok-under-digital-services-act>>.

⁵⁴ European Commission – European Commission- Commission opens formal proceedings against Temu under the Digital Services Act. In: *European Commission* [online]. 2024 [2026-01-09]. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5622>.

each EU Member State to decide whether the content displayed is illegal under the local legislation, with possibility to ban it.⁵⁵

Another limitation on the successful implementation of DSA, as on implementing effective age verification systems, technically challenges and raises concerns about user privacy. Methods such as biometric verification can be intrusive, and reliance on government-issued IDs may not be feasible for all users.⁵⁶ At the same time, collecting additional personal data for verification purposes heightens the risk of data breaches and misuse, as data exploitation risks, underscoring the challenge of balancing user privacy with regulatory requirements.

Besides, some tech companies argue that the DSA imposes excessive regulatory burdens, potentially stifling innovation and competitiveness.⁵⁷ They contend that the stringent requirements may hinder the growth of European tech firms in the global market. In addition, there are concerns that the DSA's provisions could lead to over-censorship, where platforms might excessively remove content to avoid penalties, thereby infringing on users' freedom of expression.⁵⁸ The broad definitions of harmful content may result in the suppression of legitimate speech.

Some U.S. senators has criticized the DSA, claiming it discriminates against American companies by imposing regulations that may not equally apply to European or other international firms. They argue that this could create an uneven playing field in the digital market.⁵⁹

Resuming, the EU's Digital Services Act represents a proactive, rights-based framework, yet concerns remain about its effectiveness and the risk of limiting children's freedom of expression, particularly in light of critiques from business and technology sectors. Italy's application of the GDPR illustrates the fragmented and inconsistent enforcement of harmful content rules across the EU, while Hungary's child-protection measures targeting LGBTQ content have sparked renewed debates over regulatory overreach. At the same time, questionable age-verification practices and corporate circumvention strategies (as it was shown in cases of Amazon and META) reveal persistent gaps in implementation. Against this backdrop, the following section examines the broader risks and challenges of restricting minors' access to social media.

⁵⁵ BREYER, P. Digital Services Act: Decision in part strengthens, in part threatens privacy, safety and free speech online. In: *breyer.de* [online]. 2022 [2026-01-09]. Available at: <<https://www.patrick-breyer.de/en/digital-services-act-decision-in-part-strengthens-in-part-threatens-privacy-safety-and-free-speech-online>>.

⁵⁶ Centre for Information Policy Leadership. Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable. In: *CIPL* [online]. 2023 [2026-01-09]. Available at: <<https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable>>.

⁵⁷ MEAKER, M. Meta Lobbyist Turned Regulator Says Europe's Big Tech Rules Have Gone Too Far. In: *WIRED* [online]. 2024 [2026-01-09]. Available at: <<https://www.wired.com/story/meta-lobbyist-eu-regulator-big-tech-rules-too-far/>>; BARRABI, T. Instagram parent Meta hit with online child safety probe in Europe. *New York Post*. In: *New York Post* [online]. 2024 [2026-01-09]. Available at: <<https://nypost.com/2024/05/16/business/instagram-parent-meta-hit-with-online-child-safety-probe-in-europe/>>.

⁵⁸ TURILLAZZI, A., CASOLARI, F., TADDEO, M., FLORIDI, L. The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications. In: *papers.ssrn.com* [online]. 2022 [2026-01-09]. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007389>.

⁵⁹ KELLEY, A. Lawmakers Argue Pending European Tech Laws Disadvantage American Firms – Nextgov/FCW. In: *nextgov.com* [online]. 2022 [2026-01-09]. Available at: <<https://www.nextgov.com/policy/2022/02/lawmakers-argue-pending-european-tech-laws-disadvantage-american-firms/361480/>>.

VI. RISKS AND CHALLENGES OF RESTRICTING MINORS FROM SOCIAL MEDIA USE

Efforts by legislators to proactively restrict minors' access to social media come with significant challenges and unintended consequences. One major concern is the risk of exclusion of certain groups of children from critical support systems. Platforms such as Reddit and Discord provide digital spaces for minors, particularly teenagers, to discuss mental health struggles.⁶⁰ These platforms often serve as safe havens for children in abusive households, offering them access to supportive communities without the need to disclose their struggles to their abuser. Social media can also bypass the fear of seeking help from social services, which, in many cases, are perceived as ineffective.⁶¹

The role of social media in education and self-expression is equally critical. Platforms, such as TikTok and YouTube serve as accessible and entertaining sources of learning, offering opportunities for informal education and skill development.⁶² Additionally, social media is a vital means of self-expression for many young people, particularly those in isolated or rural areas where these platforms act as lifelines for building friendships and maintaining social connections.⁶³

Nevertheless, the evolution of digital platforms introduces new risks that must be addressed alongside regulatory measures. AI-generated content poses unique challenges, as it can bypass age restrictions, target minors with harmful material, and spread disinformation.⁶⁴ The rise of generative AI exacerbates these risks, enabling the creation of deepfake content and AI-driven grooming tactics. Addressing these threats requires ongoing reassessment and the updating of legal definitions to encompass emerging forms of online abuse and exploitation.⁶⁵ In the EU, such regulatory efforts remain ongoing, in particular through the Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council), which seeks to establish a risk-based framework including safeguards for children, explicitly referring to it in Recital 48.

As it was discussed through the overview of the recent legislation and approaches of the legislators and judiciaries, the balanced approach that ensures all – respect of the fundamental rights of the involved parties, but also safety and innovation – is crucial. Proactive regulations must address the needs of all the actors, but also while tackling the intermediaries, as the large and small platforms to achieve compliance effectively. For instance, while very large platforms such as META or TikTok may have the resources to

⁶⁰ American Psychological Association. Potential risks of content, features, and functions: The science of how social media affects youth. In: *American Psychological Association* [online]. 2024 [2026-01-09]. Available at: <<https://www.apa.org/topics/social-media-internet/youth-social-media-2024>>.

⁶¹ UNICEF and VAN BERGEN, N. Essay collection children's rights in the digital world. In: *Unicef* [online]. [2026-01-09]. Available at: <<https://www.unicef.nl/files/UNICEF-Essay-collection-Childrens-rights-in-the-digital-world.pdf>>.

⁶² BOYD, D. *It's Complicated: The Social Lives of Networked Teens*. New Haven, London: Yale University Press, 2014.

⁶³ Pew Research Center. Teens, Social Media & Technology. In: *Pew Research Center* [online]. 2022 [2026-01-09]. Available at: <<https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/>>.

⁶⁴ NANNINI, L., BONEL, E., BASSI, D., MICHELE JOSHUA MAGGINI. *Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. AI and ethics*. New York: Springer, 2024.

⁶⁵ UNICEF. Generative AI: Risks and Opportunities for Children. Innocenti Global Office of Research and Foresight. In: *Unicef* [online]. [2026-01-09]. Available at: <<https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children>>.

implement advanced compliance mechanisms, smaller platforms may struggle to meet the same standards, even though, as it was discussed, the larger platforms are reluctant to comply with the requirements. Furthermore, as seen in the case of Amazon's contestation of the EU DSA, large corporations may attempt to circumvent or contest regulations by restructuring or subdividing their operations. Such developments underscore the need for robust systemic approaches.⁶⁶

Probably, in order to fulfil the aim of protection of minors in digital sphere more constructively and not to interfere with other fundamental rights, but also the benefits for the minors brought by the digital frontier, is to complement proactive laws by the complex approach. There must be a focus on media literacy, particularly social media literacy, among all stakeholders. This includes educating parents, educators, and civil society actors on the safe and responsible use of social media platforms.⁶⁷ Strengthening parental controls and embedding digital literacy programs in education systems is essential to preparing children for navigating the digital world safely.

Given the cross-border nature of social media, regulatory frameworks must also account for international cooperation and harmonization. The challenges highlighted in the cases above, for instance of the Italian Data Protection Authority (DPA) vs. TikTok, demonstrate the difficulties of implementing national regulations within broader regional frameworks, such as the EU. Establishing international guidelines to address disparities in enforcement and ensure consistency across jurisdictions is therefore critical. By proposing a comparative framework that integrates law, policy, and digital literacy, this article seeks to advance these ongoing debates. To situate this discussion within the broader academic context, it is essential to examine how scholars and legal commentators have conceptualized the challenges of regulating children's online safety.

VII. SCHOLARLY CRITIQUES OF CURRENT FRAMEWORKS

Legal scholarship has increasingly highlighted the limits of existing child protection laws in adapting to the dynamics of digital media. For instance, Livingstone, Nair, Stoilova, van der Hof, and Caglar (2024)⁶⁸ argue that age-assurance mechanisms often neglect children's rights to participation and self-expression. They also note that such verification measures are frequently ineffective in practice, underscoring the importance of developing ongoing processes and creating ecosystems that are genuinely inclusive for children.⁶⁹

Similar criticisms were directed at the U.S. COPPA more than a decade ago. In their researches⁷⁰ describe COPPA as outdated, emphasizing that its age-verification mech-

⁶⁶ CAUFFMAN, C., GOANTA, C. A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*. 2021, Vol. 12, No. 4, pp.758-774.

⁶⁷ HUSOVEC, M. *Principles of the Digital Services Act*. Oxford: Oxford University Press, 2024.

⁶⁸ LIVINGSTONE, S., NAIR, A., STOILOVA, M., VAN DER HOF, S., CAGLAR, C. Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*. 2024, Vol. 32, No. 3, pp. 721-747.

⁶⁹ *Ibid.*

⁷⁰ MONTGOMERY, K. Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy, Elsevier*. Vol. 39, No. 9, pp. 771-786. 2015; THIERER, A. Parental Controls & Online Child Protection: A Survey of Tools & Methods. In: *ssrn.com* [online]. 2009 [2026-01-09]. Available at: <<https://ssrn.com/abstract=1268433> or <http://dx.doi.org/10.2139/ssrn.1268433>>.

anisms are easily circumvented and fail to address risks beyond the narrow scope of data collection. Meanwhile, regulatory fragmentation remains a persistent challenge. A Brookings commentary⁷¹ characterizes the regulatory landscape as it lacks nuance and often overlooks the broader spectrum of children's rights analyzing different states' approach within the United States of America. Together, these critiques highlight the persistent gap between legislative intent and enforcement realities.

Comparative studies also reveal divergent normative approaches to regulating children's online activity. In the United States, free speech jurisprudence frequently constrains regulatory intervention. By contrast, the European Union has emphasized child-specific protections through a framework of platform accountability, systemic risk management, and algorithmic transparency⁷². However, as recent cases demonstrate, the implementation of such principles remains an evolving process, and their effectiveness is not yet fully established. In the recent briefing papers of the European Parliamentary Research Service,⁷³ the proactive measures of the EU (including legislative acts, initiatives, and awareness campaigns) are highlighted as notable progress in strengthening online child protection. Nevertheless, significant gaps in enforcement remain. Niestadt's analysis of EU, national, and regional measures underscores both the advances achieved and the ongoing difficulties in ensuring effective implementation.

A further strand of literature concerns the role of emerging technologies in amplifying risks. Scholars warn that algorithmic recommendation systems and generative AI can heighten children's exposure to harmful content and facilitate new forms of online manipulation. Despite this, legal scholarship on how regulatory frameworks should adapt to these novel risks (particularly in relation to AI-enhanced disinformation and deepfakes targeting minors) remains limited.

Finally, scholars increasingly call for holistic approaches that extend beyond regulation. Livingstone (2016),⁷⁴ Hanson (2014),⁷⁵ and Staksrud (2013)⁷⁶, O'Neill (2023)⁷⁷ stress the need for coordinated strategies that balance children's rights, such as freedom of expression and participation in digital life, against the imperative to protect them from online harm. These authors also caution that even well-intentioned interventions in the

⁷¹ JANG, K., PAN, L., TURNER, L. N. The fragmentation of online child safety regulations, Brookings. In: *Brookings* [online]. 14. 8. 2023 [2026-01-09]. Available at: <<https://www.brookings.edu/articles/patchwork-protection-of-minors/>>.

⁷² HELBERGER, N., JO PIERSON, POELL, T. Governing Online Platforms: From Contested to Cooperative Responsibility. *The Information Society*. 2017, Vol. 34, No. 1.

⁷³ NIESTADT, M. Protecting children online: Selected EU, national and regional laws and initiatives. EPRS | European Parliamentary Research Service. In: *European Parliament* [online]. April 2025 [2026-01-09]. Available at: <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI\(2025\)769570_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf)>.

⁷⁴ LIVINGSTONE, S. Reframing media effects in terms of children's rights in the digital age. *Journal of Children and Media*. 2016, Vol. 10, No. 1, pp. 4–12.

⁷⁵ HANSON, K. 'Killed by charity' – Towards interdisciplinary children's rights studies. *Childhood*, 21, pp. 441–446. In: *Sage Journals* [online]. 2014 [2026-01-09]. Available at: <<https://journals.sagepub.com/doi/full/10.1177/0907568214547453>>.

⁷⁶ STAKSRUD, E. *Children in the Online World. Risk, Regulation, Rights, 1st edition*. Abingdon on Thames: Routledge, 2013.

⁷⁷ O'NEILL, B. The influence of social media on the development of children and young people, Policy Department for Structural and Cohesion Policies, European Parliament. In: *European Parliament* [online]. 2023 [2026-01-09]. Available at: <[https://www.europarl.europa.eu/RegData/etudes/STUD/2023/733109/IPOL_STU\(2023\)733109_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/733109/IPOL_STU(2023)733109_EN.pdf)>.

name of children's rights can produce unintended, counterproductive effects. Nevertheless, empirical evaluations of such combined strategies remain scarce, especially in cross-jurisdictional contexts. Another issue arises when parents themselves share images of their children on social media. Under the GDPR, such practices may create what scholars have termed a "legislative paradox" (Lendvai, 2024).⁷⁸ Lendvai provides a comprehensive analysis of this phenomenon, conceptualizing sharenting as a regulatory paradox that complicates the balance between parental authority, children's privacy, and data protection obligations.

The literature demonstrates the limits of current frameworks and the need for balanced solutions, that effective regulation together with the researchers' recommendations must avoid overreach and respect children's rights to autonomy, privacy and expression, and provide a space for intersectional cooperation, not fully relying on sole regulatory attempt. The next section outlines concrete policy recommendations to strengthen child protection while respecting rights.

VIII. POLICY RECOMMENDATIONS

This article argues that while proactive laws represent meaningful progress in protecting children from online harm, certain legislative approaches risk overreach, particularly when they unduly restrict children's autonomy or privacy. Building on existing scholarly proposals, several additional recommendations can be made from a local and comparative perspective.

First, given the fragmented nature of current regulatory approaches, cross-border cooperation should be strengthened. Although the EU has advanced a relatively harmonized framework through instruments such as the GDPR, discrepancies remain due to the flexibility afforded to member states in implementing national solutions. Since the digital sphere transcends national borders, establishing joint task forces, enhanced data-sharing mechanisms, and coordinated enforcement strategies across jurisdictions (including beyond EU) is essential.

Second, while digital literacy programs and public awareness campaigns already exist, they are often insufficient. Embedding mandatory digital literacy education into school curricula, complemented by targeted parental education programs, would provide children and families with the skills needed to navigate online risks effectively.

Third, the persistent reluctance of large technology corporations to cooperate fully with regulators highlights the need for stronger, coordinated oversight. To address corporate circumvention strategies, regulators should require transparent algorithmic auditing and establish independent mechanisms to monitor compliance. Such measures would not only enhance accountability but also help align platform practices with the principles of children's rights and online safety.

These recommendations point to cooperation, education, and accountability as key strategies, thus highlighting the need for a coordinated, multi-layered approach to child

⁷⁸ LENDVAI, G. F. Sharenting as a regulatory paradox – a comprehensive overview of the conceptualization and regulation of sharenting. *International Journal of Law, Policy and the Family*. 2024, Vol. 38, No. 1.

protection in the digital environment - one that balances autonomy and privacy with the imperative of safeguarding a vulnerable group. The conclusion now returns to the central debate of whether proactive laws represent progress or overreach.

CONCLUSION

Creating safer digital environments for children requires a multidimensional approach that combines proactive legal measures, technological innovation, and educational initiatives. The frameworks, such as COPPA in the United States, or the recent ones, as the United Kingdom's Online Safety Act, Australia's Online Safety Amendment, and the EU's GDPR or DSA, represent important progress in recognizing and mitigating the risks that minors face online. Yet, as this article has demonstrated, these measures also reveal persistent shortcomings: regulatory fragmentation (even within one country), contrasting conceptions of digital child protection (in global context, for example, while U.S. courts have emphasized constitutional constraints, the EU's approach has centered on harmonization and algorithmic accountability), weak enforcement, corporate resistance, and the continued ability of children to circumvent restrictions.

As set out in the introduction, this study has examined selected policies, laws, practices, and scholarly debates to assess whether proactive approaches represent meaningful progress or whether they inadvertently cross into unintended overregulation. The analysis has shown that the reality lies in between: proactive regulation is indispensable, but its effectiveness depends on striking a careful balance between safety and fundamental rights.

The central argument advanced here is that proactive laws are both necessary progress and a source of potential overreach. They mark a significant step forward in protecting children from online harm, but when implemented without sufficient safeguards, they risk undermining children's autonomy, privacy, and rights to digital participation. Legal scholarship and case law reveal that effective protection cannot rely on regulation alone but must also preserve the balance between shielding vulnerable groups and empowering children as rights-bearing digital citizens.

To move toward this balance, three policy priorities are especially important. First, greater cross-border cooperation is needed to harmonize enforcement in a borderless digital environment. The EU's GDPR provides a valuable model of harmonization, but discrepancies in national implementation highlight the need for joint task forces and international (including beyond the EU) data-sharing mechanisms. Second, digital literacy must be embedded into school curricula and extended to parental education, equipping children and families with tools to manage risks responsibly. Third, regulators should mandate transparent algorithmic auditing and establish independent oversight mechanisms to hold technology corporations accountable and prevent regulatory circumvention.

In conclusion, safeguarding children in the digital era requires more than just legislative intervention. Proactive legal frameworks must be complemented by systemic solutions, international collaboration, and education. Only through such a holistic approach can societies strike the delicate balance between protection and empowerment, ensuring that children benefit from the opportunities of the digital age while being shielded from its most harmful consequences.