Protecting Minors in the Digital Environment: Integrating Legal and Technical Perspectives

Mashal Afzal Memon, Lisandra Suárez Fernández and Marco Autili

University of L'Aquila, Italy

Abstract

Modern society is undergoing a profound transformation in how people interact, learn, and socialize through digital platforms, devices, services, and AI systems. While this transformation offers opportunities for well-being and education, it also introduces risks that are particularly significant for children, who are especially vulnerable and require specific protection in the digital environment. Hence, effective protection of children requires addressing issues related to the digital identification of minors, safeguarding their rights and interests that may be affected by digital technologies, and further adapting protective measures to their age, capacity, and autonomy. In this regard, this paper proposes three research directions that structure the analysis of the protection of minors in the digital environment from both legal and technical perspectives. The main objective of this study is to organize and synthesize this complex landscape through an interdisciplinary approach that integrates both dimensions, supporting the development of practices and solutions aimed at strengthening the protection of minors.

Keywords

Minors, Digital Environment, Privacy, Protection, Age Verification, Socio-Technical Systems.

1. Introduction

A minor is generally understood as any person under the age of eighteen, unless, by virtue of the law applicable to them, they have reached the age of majority earlier [1]. Their protection has long been recognised as a universal principle incorporated in international legal frameworks and expanded upon by national legal systems [2, 3]. According to the United Nations Universal Declaration of Human Rights [4], *"motherhood and childhood are entitled to special care and assistance"*, which recognizes the need to provide children with special protection due to their physical and mental immaturity.

The modern society has shifted a significant portion of social interactions and processes to the digital environment, facilitated by communication networks, electronic devices, online services, Artificial Intelligence (AI) enabled systems, and digital platforms. In this context, minors are often considered "digital natives" due to their familiarity with technology. Various studies and surveys have reported high levels of internet usage among minors [5, 6, 7], indicating that a

The 12th International Conference on Socio-Technical Perspectives in IS (STPIS'26), September 16–17, 2026, L'Aquila, Italy.

mashalafzal.memon@univaq.it (M. A. Memon); lisandra.suarezfernandez@univaq.it (L. Suárez Fernández); marco.autili@univaq.it (M. Autili)

0000-0003-3556-9144 (M. A. Memon); 0000-0002-3772-9749 (L. Suárez Fernández); 0000-0001-5951-1567 (M. Autili)



CC-BY logo & © 2026 Copyright for this paper by its author(s). Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-4334/paper29.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-19

significant portion of teens engage with the internet on a daily basis, with a few being online almost constantly. However, due to their stage of psychological and physical development, minors often struggle to recognize the risks posed by digital environments [8, 9, 10], making them particularly vulnerable.

Adapting the principle of minor protection to the digital environment requires assessing emerging risks for this age group and the characteristics of the technologies they interact with. This further reveals the risks related to access, inappropriate content [11], interactions with other users and AI enabled systems, and the prolonged use of digital platforms and devices [12, 13, 14]. Therefore, it requires establishing legal provisions and developing technical solutions that contribute to ensuring safe and transparent interaction with the digital environment, adapted to the specific needs and vulnerabilities related to minors and respectful of their fundamental rights, fostering the development of socio-technical systems capable of responding to the protection requirements of user groups with specific needs [15].

This requires addressing significant challenges widely recognised in the literature [15], including determining whether users are children for the purposes of regulating access to digital services, protecting privacy and personal data, ensuring system transparency, governing digital content, and respecting children's evolving autonomy. Furthermore, the rapid evolution of digital technologies, together with the still-developing international, regional, and national regulatory frameworks, complicates these efforts [16]. In light of these considerations, this study organises and synthesises the complex landscape of minors' protection in the digital environment from a socio-technical and interdisciplinary perspective, integrating legal and technical dimensions to support the development of effective practices and solutions. To structure this analysis, the study identifies three research directions addressing particularly relevant areas of minors' protection in which legal and technical considerations need to be addressed jointly:

RD1 Adoption of age-assurance mechanisms in digital services to identify minors and grant or deny access accordingly, while ensuring compliance with data-protection and privacy requirements.

RD2 Promoting the design and development of such solutions that allow effective parental control and adapt the content based on the progressive development of the minor's capacity and autonomy.

RD3 Promoting transparent and explainable AI systems by disclosing AI-driven functionalities and other mechanisms in digital services to increase minors' awareness of their usage.

Taking these research directions as a basis, the remainder of the paper is structured as follows.

Section 2 presents the background knowledge and related work. Section 3 presents the methodology used to develop the research agenda. Section 4 introduces the research directions along with their technical and legal analysis. Section 5 discusses the risks and challenges, and Section 6 concludes the paper.

2. Background & Related Work

Recent studies indicate that minors are among the most frequent users of the digital environment, which significantly increases their exposure to potentially harmful. According to the survey by

the Spanish National Statistics Institute [5], 93.1% of children between the ages of 10 and 15 use a computer while 94.7% browse the internet, and 70.6% use a mobile phone. According to the Pew Research Center's Teens, Social Media, and Technology 2024 report [6], 95% of American teens have access to a smartphone, 88% use a desktop or laptop computer, 83% use video game consoles, and 70% use a tablet at home. Moreover, a significant portion of teens engages with the internet daily, with a few being online almost constantly. A 2025 press release from Save the Children Italy [7] revealed that regardless of the age established for processing minors' data, 62.3% of pre-adolescents between the ages of 11 and 13 have at least one social media account.

Based on this reality, the literature has identified several dimensions that affect the protection of minors in the digital environment[17]. A primary aspect concerns access to digital services, identified as a necessary prerequisite for activating protection mechanisms. In this regard, age verification allows for the deployment of successive, differentiated protection measures and the regulation of access to certain services or content. However, mechanisms designed to verify or estimate users' ages pose significant challenges regarding respect for children's fundamental rights [18]. Moreover, the literature also highlights the need to reconcile child protection with privacy and the protection of personal data through proportionate, transparent solutions that respect the principle of data minimization, ensuring that protective measures do not involve disproportionate forms of identification or processing of personal information. Consequently, the Convention on the Rights of the Child provides in Article 17 [1] and United Nations human rights Council General Comment No. 25 [19] urge the digital service providers to support children's development and protect them from harmful content and follow ethical, privacy, and security standards through appropriate regulations, industry codes, and terms of service across all stages of their products and services. The Organisation for Economic Co-operation and Development (OECD) [20] furthermore provides a comprehensive overview of age assurance legislation across member countries for child safety. It highlights that the laws introducing age assurance requirements are being enacted at a fast pace, particularly regarding social media and online pornography.

Furthermore, the physical, psychological, and cognitive development of children requires that the principle of progressive autonomy guide their participation and decision-making capacity in the digital environment. Hence, both the literature and regulatory instruments agree that digital services should foster a progressive interaction with technology, taking into account the child's developmental capacities and the guidance and representational role of parents or legal guardians. Consequently, adequate governance is necessary to ensure children's access to age-appro priatecontent. Likewise, the increasing use of AI based systems has highlighted the need to incorporate transparency measures that allow children to identify and understand when they are interacting with an intelligent system.

These issues have been better addressed into technical and regulatory frameworks. In the European Union (EU) the General Data Protection Regulation (GDPR) [21], the Digital Services Act (DSA) [22], and the Artificial Intelligence Act (AI Act) stand out [23]; together with the recent proposal for the EU KIDS Act, specifically aimed at strengthening the protection of minors in the digital environment [24]. Meanwhile, instruments such as Children's Online Privacy Protection Rule (COPPA) [25] in the United States demonstrate a growing interest in developing mechanisms to guarantee and protect minors.

Growing regulatory and technical attention has contributed to strengthening the protection of

minors in the digital environment. Nevertheless, several important concerns remain unresolved. On the one hand, certain measures aimed at ensuring more effective protection can create significant tensions with privacy and personal data protection. On the other hand, current regulatory initiatives and technical solutions still provide only partial coverage of the diverse risks, needs, and specific characteristics of minors, particularly regarding their evolving autonomy, access to age-appropriate content, and the adaptation of digital tools and environments to their capabilities and needs. In this context, this study highlights the potential, and limitations associated with existing solutions, outline relevant courses of action for technical professionals, and identify areas requiring further research and development.

3. Methodology

In this section, we provide an overview of the methodology used to develop the research agenda.

This study adopts an interdisciplinary socio-technical perspective to examine the protection of minors in the digital environment, considering digital technologies in relation to the needs, risks, and vulnerabilities of those who interact with them, with particular attention to minors as a group requiring specific attention [26]. Accordingly, the analysis integrates legal and technical perspectives, considering legal provisions as the basis for defining rights, safeguards, and responsibilities, and technical solutions as a means of translating protection needs into system capabilities and mechanisms.

The three research directions are formulated to guide the analysis, based on three critical elements of minors' protection in the digital environment: (i) identification, (ii) adaptation, and (iii) interaction. Each dimension is addressed through the combined analysis of its legal and technical dimensions.

The study draws on academic literature and empirical studies, relevant legislation and regulatory initiatives from different jurisdictions, and guidelines, recommendations, and reports from national and international institutions and regulatory bodies.

Source selection is guided by relevance to the issues under examination, considering each source's contribution to identifying challenges, risks, and protection needs, documenting technical or regulatory responses, and, for institutional sources, the relevance and competence of the issuing body.

The study gives particular attention to the EU legal framework, which addresses different aspects of digital technologies and the protection of minors through an evolving set of regulatory instruments, while legal developments in other jurisdictions are considered where they provide relevant approaches to the specific protection issues under examination.

4. Research Direction

In this section, we introduce the three proposed research directions along with their legal and technical analyses.

Figure 1 illustrates how the proposed research line would contribute to the protection of minors in the digital environment.

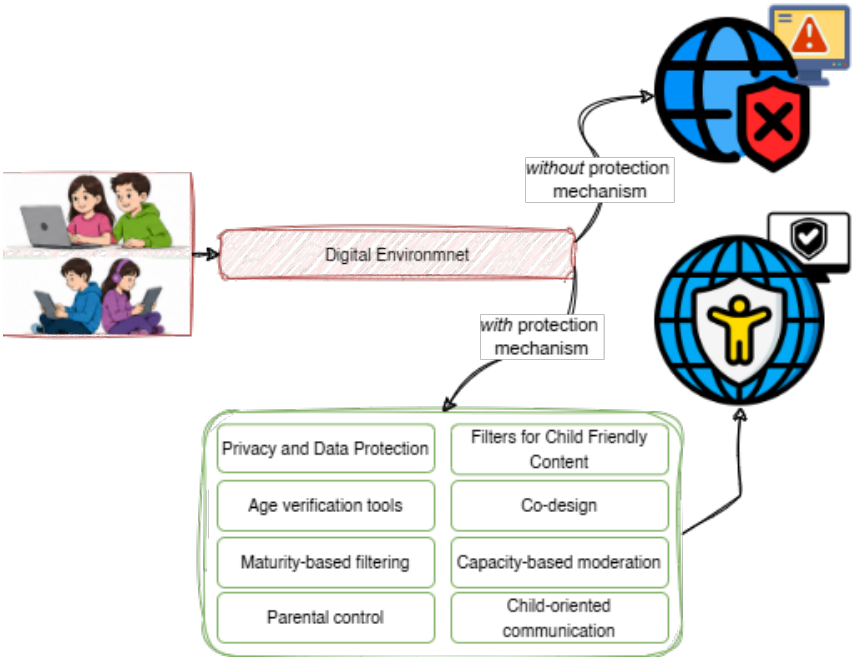


Figure 1: Vision of the proposed approach. Without protection mechanisms (upper path), children are exposed to various online risks, including inappropriate content, privacy violations, etc. With the proposed protection mechanisms (lower path), the digital environment becomes safer and more suitable for children.

To provide a safe digital environment as shown in lower path of Figure 1, we propose the three research directions as detailed below.

> *RD1# Adopting the use of age-assurance mechanisms while ensuring data-protection and privacy*

Legal Analysis: Age verification is an increasing requirement in various regulatory frameworks [27]. However, legislation has not established a uniform, mandatory model for age assurance or age verification, resulting in a fragmented and evolving digital landscape. At EU level, Article 35.1 (j) of DSA [28], expressly mentions this process. Within the framework of the systemic risk mitigation obligations imposed on providers of very large online platforms and very large search engines, the provision states that such measures may include the adoption of specific mechanisms to protect the rights of minors, including the implementation of age verification tools [22]. Similarly, the UK Online Safety Act 2023 [29] establishes a general obligation for providers of digital services likely to be accessed by children to adopt proportionate measures to prevent and mitigate the risks posed by harmful content. Specifically, where a service hosts categories of content classified by law as primary priority content harmful to children, the Act requires to use highly effective age verification, age estimation, or both to determine whether a user is a child and to prevent access to such content.

At the same time, however, it emerges that some systems implemented for age verification purposes may interfere with fundamental rights, particularly minors' rights to privacy and the protection of personal data [30]. In this regard, the GDPR establishes the legal framework for the

processing of personal data. Therefore, age verification solutions that involve the processing of personal data must be designed and implemented in accordance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, integrity and confidentiality and storage limitation, as well as with data protection obligations by design and by default [31]. In more detail, Article 8 of the GDPR establishes specific conditions for children's consent in relation to the direct provision of information society services. In such cases, the child's consent, and consequently the processing of their personal data, is lawful only if the child is at least 16 years old, unless a Member State has established a lower age, which may not be below 13 years, or where consent is given or authorised by the holder of parental responsibility over the child [21]. In parallel, Article 28 of DSA requires online platforms accessible to minors to implement appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors when using their services. To facilitate the implementation of these obligations, the European Commission has recently adopted Guidelines that provide practical guidance on the protection of minors online [32].

Currently, the European Union's regulatory framework addresses the protection of minors by imposing obligations to ensure a high level of privacy, security, and protection in digital services, as well as by progressively recognising age verification as a tool to strengthen this protection. However, it has not established a general minimum age for accessing digital platforms, products, or services, opting instead for a model based on protection and risk management obligations. In this perspective, Australian legislation takes a more direct approach by establishing a minimum age for accessing certain social media services and requiring providers to take reasonable measures to prevent minors who have not reached that age from maintaining an account. To ensure compliance with this obligation, the law regulates the use of identification materials and services designed to determine or verify users' ages [33].

This approach reflects a regulatory trend in which age determination is increasingly used to apply rules and restrictions on access to certain digital services. Age determination is configured as a tool for protecting minors by regulating access to certain digital services. However, its implementation must respect fundamental rights, particularly the right to privacy and the protection of personal data, in accordance with the applicable legal framework.

Technical Analysis: From a technical perspective, digital platforms need to be accurate at identifying age, secure, have parental control, respect privacy, and be resistant to manipulation. They must be capable of verifying users' age without collecting excessive personal data.

Traditional approaches to age verification, such as self-declaration, credit card verification, and biometric-based age estimation, are commonly used [34]. However, these methods present several issues, as they can be easily bypassed, biometric accuracy decreases significantly for children, and they raise privacy concerns regarding the handling of sensitive data.

Platforms like Meta have begun implementing automated age verification systems such as AI-based facial analysis and behavioral inference models to more accurately assess user age and comply with child protection regulations. However, the challenge remains regarding the accuracy of these systems and whether they consistently meet the legal and ethical standards required across different jurisdictions. Different perspectives on personal data protection regulations, age thresholds, and enforcement frameworks mean that a one-size-fits-all solution is often insufficient. As such, age verification technologies must be carefully designed to ensure

regional compliance, privacy preservation, and fairness, while minimizing the risk of exclusion or misuse.

Developing age verification solutions that comply with current regulatory frameworks requires careful consideration of data minimization, purpose limitation, and privacy by design principles. Current age verification approaches often rely on collecting and storing biometric data (e.g., facial images) or personal information such as credit card details and government-issued IDs. These approaches raise concerns about privacy and data protection, especially when not strictly limited to verifying age. To address these concerns, platforms must design systems that verify age only for the specific and limited purpose of access control, without misusing personal data. Moreover, the proposed approaches need to respect the regulations like the GDPR and the DSA, which emphasize minimal data processing and high standards of security and transparency.

In this context, transparency in communication is essential, i.e., users should be clearly informed about what data is processed, for which purpose, for how long, and under which safeguards. Equally important is the adoption of co-design approaches involving relevant stakeholders, including users, child protection experts, civil society organizations, regulators, and technology providers, to ensure that age verification systems are not only legally compliant, but also socially acceptable, trustworthy, and aligned with users' rights and expectations.

A key technical premise, therefore, is the need to decouple age verification from full identity verification, ensuring that platforms fulfill their duty to protect minors without undermining user anonymity or privacy. The development of such solutions should incorporate privacy-enhancing technologies (PETs), such as zero-knowledge proofs, on-device processing, and ephemeral data handling, to strike a balance between regulatory compliance and user trust.

RD2# Promoting the design and development of solutions that allow parental control and support age-flexible content

Legal Analysis: Cyber parental control is a manifestation of parents' legal responsibility to care in the digital environment [35]. Although neither EU legal framework nor the general approach of national family law establishes a specific legal framework governing parental control, recent regulatory developments increasingly require providers of digital devices and online services likely to be used by minors to incorporate, at no additional cost, parental control functionalities. These functionalities enable parents or legal guardians to supervise, configure, and, where appropriate, manage access to digital services, specific functionalities, and online content [28, 36].

Regarding the adjustment of content according to the progressive development of the child's capacity and autonomy, automated systems face the challenge of implementing the General Comment No. 25 [19], which establishes that digital service providers must offer environments appropriate to the evolving capacities of children. Although EU regulations have not addressed this topic in depth, its practical application requires the development of automated systems that adapt to the child's actual capacities or to average development levels according to their age. In this regard, the European Commission Guidelines on measures to ensure a high level of privacy, safety and security for minors online, adopted pursuant to Article 28(4) of the DSA, expressly recognise the relevance of age-appropriate design and the need to take into account the stage

of development, and evolving capacities. This approach can be strengthened by adopting an age-appropriate design perspective that adapts digital products and services to the specific characteristics, needs, and vulnerabilities of children. This encourages the adoption of enhanced privacy settings, as well as the use of transparent, understandable communication mechanisms for children [37]. This highlights that the protection of children extends beyond issues of access and identification, encompassing the creation of digital environments that support their development, well-being, dignity, and progressive autonomy [38].

Technical Analysis: Developing automated solutions for protecting minors requires a multi-layered approach. Such a system must include age estimation, content personalization, and parental oversight. The age estimation module would trigger the adaptation of content control pipelines, where content will be filtered according to age-appropriate guidelines. Moreover, it is important to develope solutions aimed at adapting content based on the progressive development of minors' capacities and autonomy, including co-design approaches and child-friendly content filtering mechanisms to address inappropriate or potentially harmful content[39]. Such adaptive approaches should also incorporate age-appropriate design principles, ensuring that interfaces, privacy notices, and platform functionalities remain understandable and accessible to children of different ages.

To reinforce children's safety, parental control should function as a configurable supervisory layer rather than a purely restrictive mechanism. Parental control or legal guardian modules should be able to review activity, set content boundaries, enforce screen time limits, and receive alerts. Such solutions must also be designed for adaptability and modularity, allowing them to evolve in response to content trends and user behavior without compromising performance or user experience. At the same time, these controls should remain flexible, allowing supervision to evolve as children mature and progressively exercise greater autonomy.

Another important technical challenge is ensuring that content adaptation and parental supervision respect children's privacy and fundamental rights. Privacy-enhancing technologies, explainable AI, and user-controlled privacy settings can help balance effective protection with children's evolving autonomy and their right to participate safely in digital environments.

RD3# Promoting transparent and explainable AI systems to increase minors' awareness

Legal Analysis: In the field of AI , the EU has implemented the AI Act, structuring its regulatory framework around the level of risk associated with AI systems and imposing prohibitions, requirements, and obligations proportionate to that risk [23]. It can be observed that, although the legislation does not establish a specific and independent regime for the protection of minors, it incorporates age and minor status as relevant elements in the application of various regulatory provisions, expressly recognizing that minors constitute a vulnerable group.

This consideration is reflected, first, in the regime of prohibited practices set out in Article 5 of AI Act [23], which takes into account age-related vulnerabilities by prohibiting certain uses of AI systems that exploit such vulnerabilities to cause significant harm to individuals or third parties. Likewise, regarding high-risk AI systems, age-related vulnerability is a relevant factor in assessing the risks that these systems may pose. Once classified as high-risk, providers must also consider, within their risk management systems, whether these systems are likely to adversely affect persons under the age of eighteen.

Furthermore, minors benefit from the general transparency obligations set out in Article 50 for certain AI systems. These obligations, aimed at ensuring that individuals are informed when interacting with AI systems or when certain content has been generated or manipulated using these technologies, indirectly help protect minors from deception, manipulation, or misperceptions about the nature of the content or the interaction. Consequently, although the AI Act does not establish a separate regime for the protection of minors, it incorporates safeguards that account for their status as a vulnerable group within its risk-based regulatory framework [23].

Technical Analysis: From a technical perspective, digital platforms should implement mechanisms that clearly disclose when minors are interacting with AI systems or consuming AI-generated content. Such disclosures should be designed not only for children but also for parents or legal guardians, enabling them to understand when AI technologies influence their children's digital experiences. This may include visual indicators, child-friendly explanations, parental notifications, and activity summaries that identify AI-driven interactions, recommendations, or automated decisions.

Providing transparency alone, however, is insufficient to ensure children's safety. Although modern AI systems incorporate safety mechanisms designed to reduce the generation of harmful content, they may still produce responses that are age-inappropriate, difficult for children to interpret, or unsuitable for their developmental stage. Therefore, AI systems must also be capable of recognizing age-related vulnerabilities and adjust the complexity and tone of their responses, avoid presenting content that may be inappropriate for a child's age or maturity level, and recognize situations where human intervention or parental supervision may be necessary. These capabilities require the integration of age-aware AI models, safety guardrails, risk detection mechanisms, and continuous content moderation.

5. Discussion

In this section, we discuss the broader implications of our findings and the key challenges that emerge for the design and governance of systems aimed at protecting minors in digital environments.

Access, Age-Appropriate Content, and Evolving Capabilities, Risk: Socio-technical systems designed for the protection of minors must overcome different types of risk [10]. The nature and impact of these risks vary with a child's age, cognitive development, and digital literacy, requiring age-appropriate safeguards. However, the evolution of maturity and capabilities throughout childhood makes the definition of technical solutions for adapting digital content and implementing appropriate protective measures complex. Moreover, regulatory frameworks typically set age limits for specific purposes, such as consent to personal data processing, without explicitly addressing related issues, such as the minimum age required to open an account or access other digital services and functionalities. This leaves uncertainty for those responsible for designing and technically managing these environments when defining and implementing age-related requirements. The current relevance of this issue is also reflected in the recent proposal for an EU KIDS Act [24], which seeks to address some of these aspects through specific age-related requirements for certain online services. Furthermore, exercising parental

responsibilities in the digital environment requires greater clarity regarding the requirements for implementing technical parental control mechanisms, as well as the limits of such control in relation to the minor's privacy, autonomy, and evolving capacities.

Balancing Technical Solutions with Data Protection and Privacy: The discussion of age verification technologies inevitably highlights the tension between protecting minors and preserving user privacy, data protection and autonomy. While regulations such as the GDPR and DSA mandate stronger protections for children online, they do not prescribe specific technologies, leaving platforms with the flexibility to explore a range of solutions. However, this flexibility requires to develop solutions that respect fundamental rights and meet legal requirements without creating surveillance-heavy or exclusionary systems, particularly for marginalized or vulnerable users.

Interdisciplinary and Inclusive Approaches to Child Protection: The development of socio-technical systems cannot be treated as purely technical. Designing systems that are both effective and respectful of children's rights requires collaboration among experts from multiple disciplines, including computer science, cybersecurity, law, child psychology, education, ethics, and human-computer interaction, as well as policymakers, civil society organizations, parents, and children themselves. Such collaboration is essential to balance competing objectives, including security, privacy, transparency, accessibility, and regulatory compliance. Furthermore, child-friendly design principles should guide the development process to ensure that systems account for children's cognitive, emotional, and social development. Inclusive design should also consider the diverse needs of children across different ages, abilities, cultural backgrounds, and socioeconomic contexts, ensuring equitable access to digital services while maintaining appropriate levels of protection. In this context, co-design approaches can offer a practical mechanism for involving diverse stakeholders, such as children and parents, in the early stages of system design and development. However, their implementation is not typically supported by explicit, binding legal requirements.

Effective Transparency in AI Interactions: The transparency requirements for AI systems highlight specific challenges in effectively protecting minors. On the one hand, we note that merely disclosing the presence of an AI system or explaining how it works does not guarantee that minors truly understand it. On the other hand, the information provided may not necessarily be sufficient to protect them. Consequently, this points to the need to determine how to adapt transparency mechanisms to minors' evolving capacities and when to complement them with additional protective measures.

Challenges of Global Compliance: While the protection of minors is a universal objective shared across jurisdictions, the national legal norms, age thresholds, consent requirements, and regulatory obligations vary significantly between countries and service providers. As a result, digital platforms face the challenge of developing solutions that can adapt to diverse legal and policy frameworks while maintaining a consistent level of compliance. This increases the complexity of system design and highlights the need for interoperable, modular, and policy-aware solutions, as well as greater international alignment on core principles for protecting children in digital environments.

6. Conclusion

The protection of minors in the digital environment is becoming increasingly important as children interact with digital platforms, AI systems, and online services from an early age. Exposure to inappropriate content, privacy risks, and other online threats highlights the need for automated yet rights-respecting protection mechanisms. In this paper, we identified key challenges affecting minors' digital safety and proposed three research directions, analyzed from both legal and technical perspectives, as the foundation of a socio-technical perspective for strengthening child protection in digital environments to support the development of practices and solutions for strengthening child protection in digital environments. Our analysis emphasizes that effective solutions require balancing child safety with privacy, transparency, data protection, and children's evolving autonomy, while ensuring compliance with emerging regulatory frameworks.

Declaration on Generative AI

During the preparation of this work, the author(s) used ChatGPT in order to check grammar and spelling.

References

[1] J. Tobin, The UN Convention on the Rights of the Child: A commentary, OUP Oxford, 2019.

[2] G. Van Bueren, The international law on the rights of the child, volume 35, Martinus Nijhoff Publishers, 2021.

[3] N. Ashurova, The legal status of minors and international legal protection mechanisms, Akademicheskie issledovaniya v sovremennoj nauke 4 (2025) 49–55.

[4] United Nations, Universal declaration of human rights, 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights, accessed: 2025-08-08.

[5] Instituto Nacional de Estadística (INE), Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. año 2023, 2023. URL: https://www.ine.es/prensa/tich_2023.pdf, accessed: 2025-08-08.

[6] Pew Research Center, Teens, social media and technology 2024, 2024. URL: https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/, accessed: 2025-08-08.

[7] Save the Children, Infanzia e digitale: circa un bambino su 3, tra i 6 e i 10 anni, usa lo smartphone tutti i giorni, 2025. URL: https://www.savethechildren.it/press/infanzia-e-digitale-circa-un-bambino-su-3-tra-i-6-e-i-10-anni-usa-lo-smartphone-tutti-i, accessed: 2025-08-08.

[8] A. Tsirtsis, N. Tsapatsoulis, M. Stamatelatos, K. Papadamou, M. Sirivianos, Cyber security risks for minors: A taxonomy and a software architecture, in: 2016 11th international workshop on semantic and social media adaptation and personalization (SMAP), IEEE, 2016, pp. 93–99.

[9] S. D. M. Katili, D. S. Pongoh, D. D. Matu, I. G. Rumantir, D. BlessTindas, C. H. Tumuwo,

The impact of social media technology development on minors, Jurnal Syntax Admiration 5 (2024) 5183–5190.
[10] oecd, Children in the digital environment: Revised typology of risks (oecd digital economy papers, no. 302), 2021.
[11] C. Marsden, Age-verification laws in the era of digital privacy, Nat'l Sec. LJ 10 (2023) 210.
[12] C. Costanza, L. Vetri, M. Carotenuto, M. Roccella, Use and abuse of digital devices: influencing factors of child and adolescent neuropsychology, 2023.
[13] V. Notara, E. Vagka, C. Gnardellis, A. Lagiou, The emerging phenomenon of nomophobia in young adults: a systematic review study, Addiction & health 13 (2021) 120.
[14] N. Jacob, R. Evans, J. Scourfield, The influence of online images on self-harm: A qualitative study of young people aged 16–24, Journal of adolescence 60 (2017) 140–147.
[15] M. Guštin, Challenges of protecting children's rights in the digital environment, EU and comparative law issues and challenges series (ECLIC) 6 (2022) 453–486.
[16] I. A. Caggiano, Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law, Eur. J. Privacy L. & Tech. (2022) 27.
[17] W. Said Almamari, M. M. K. Elsherbiny, Protecting children in digital environments: Identifying new forms of risk and neglect, in: Children and Family Social Work, Springer, 2026, pp. 1–19.
[18] F. Köhler-Dauner, L. Peter, E. Sitarski, K. Chauviré-Geib, A.-C. Haag, J. M. Fegert, Digital child protection in social networks: age verification and age-tiered regulation in europe, Child and Adolescent Psychiatry and Mental Health 19 (2025) 143.
[19] UN Committee on the Rights of the Child, General comment no. 25 (2021) on children's rights in relation to the digital environment, 2021. URL: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, accessed: 2025-08-08.
[20] Organisation for Economic Co-operation and Development (OECD), The legal and policy landscape of age assurance online for child safety and well-being, 2025. doi:10.1787/4a1878aa-en, accessed: 2025-08-08.
[21] European Union, Regulation (eu) 2016/679: General data protection regulation (gdpr), 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, accessed: 2025-08-08.
[22] European Parliament and the Council of the European Union, Regulation (eu) 2022/2065 on a single market for digital services (digital services act), 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065, accessed: 2025-08-08.
[23] E. U. Commission, Artificial intelligence act, 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.
[24] R. O. T. E. PARLIAMENT, O. T. COUNCIL, EU KIDS ACT - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0681, 2026. [Accessed 04-10-2026].
[25] F. T. Commission, Children's Online Privacy Protection Rule ("COPPA") — ftc.gov, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa, 2025. [Accessed 04-10-2026].
[26] E. L. Trist, et al., The evolution of socio-technical systems, volume 2, Ontario Quality of Working Life Centre Toronto, 1981.

[27] C. Jarvie, K. Renaud, Online age verification: government legislation, supplier responsibilization, and public perceptions, Children 11 (2024) 1068.
[28] European Commission, The digital services act (DSA) explained: Measures to protect children and young people online, 2025. URL: https://digital-strategy.ec.europa.eu/en/library/digital-services-act-dsa-explained-measures-protect-children-and-young-people-online, accessed: 2025-08-08.
[29] UK Parliament, Online safety act 2023, https://www.legislation.gov.uk/ukpga/2023/50, 2023. UK Public General Acts 2023 c. 50. Accessed: 30 June 2026.
[30] I. Milkaitė, M. Mačėnaitė, Advancing children's privacy and data protection rights: Emerging data protection trends and challenges in selected cee countries, Children's Rights in Central and Eastern Europe: A Comparative Analysis with a Spotlight on Lithuania (2026) 325–348.
[31] European Data Protection Board (EDPB), Statement 1/2025 on age assurance, 2025. URL: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf, accessed: 2025-08-08.
[32] European Commission, Protection of minors guidelines — public consultation (initiative 14352), 2025. URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en, accessed: 2025-08-08.
[33] Parliament of Australia, Online safety amendment (social media minimum age) bill 2024, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284, 2024. Government Bill, Parliament No. 47, Act No. 127 of 2024. Accessed: 30 June 2026.
[34] F. Eltaher, R. Gajula, L. Miralles-Pechuán, C. Thorpe, S. McKeever, The digital loophole: evaluating the effectiveness of child age verification methods on social media, Technical Report, Technological University Dublin, 2025.
[35] L. S. Fernández, La responsabilidad parental en los entornos digitales. necesario equilibrio entre acceso, control y seguridad, Actualidad jurídica iberoamericana (2022) 1076–1097.
[36] Italian Republic, Legge 13 novembre 2023, n. 159: Conversione in legge, con modificazioni, del decreto-legge 15 settembre 2023, n. 123, recante misure urgenti di contrasto al disagio giovanile, alla poverta educativa e alla criminalita minorile, nonche per la sicurezza dei minori in ambito digitale, Gazzetta Ufficiale della Repubblica Italiana, Serie Generale No. 266, 2023. URL: https://www.gazzettaufficiale.it/eli/id/2023/11/14/23G00172/SG, law No. 159, published November 14, 2023, accessed 2026-07-01.
[37] G7 Data Protection and Privacy Authorities, G7 data protection and privacy authorities joint paper on connected home devices and children's privacy, https://www.cnil.fr/sites/default/files/2026-06/g7_children_s_privacy_in_connected_home_devices_paper.pdf, 2021. Accessed: 2026-07-01.
[38] S. Livingstone, K. R. Sylwander, Conceptualizing age-appropriate social media to support children's digital futures, British Journal of Developmental Psychology 44 (2026) 300–312.
[39] nformation Commissioner's Office, Age appropriate design: a code of practice for online services — ico.org.uk, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/, 2025. [Accessed 04-10-2026].