INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 12, issue 11 (2025)

12.00.00 - Legal Sciences

LEGAL MECHANISMS FOR PROTECTING CHILDREN FROM HARMFUL INFORMATION IN THE DIGITAL ENVIRONMENT

Gulnoza Shorasulova
Master's student at Tashkent State University of Law
Email: gulnozashorasulova@gmail.com
Tashkent region, Uzbekistan

Abstract: This article is devoted to the analysis of legal mechanisms for protecting children from harmful information in the digital environment. It examines the types of risks that children face online, their impact on mental and physical health, and the international and national legal mechanisms regulating this process. The research analyzes the UN Convention on the Rights of the Child, UNICEF's General Comment No. 25 (2021), OECD recommendations, and the current legislation of the Republic of Uzbekistan. The study discusses the implementation of the child-rights by design and privacy-by-default principles, the control of age-appropriate content, and the strengthening of parental involvement as key elements for ensuring children's digital safety.

Keywords: digital environment, children's rights, information security, harmful content, digital policy, parental control, child rights by design, General Comment No. 25.

I. Introduction

In contemporary society, digital technologies and online environments are increasingly permeating the daily lives of children. The internet, mobile devices, various digital gadgets, social networks, and online platforms offer significant opportunities for children to access education, engage in social interaction, and obtain information. Alongside these advantages, however, the digital environment also facilitates the dissemination of content that may harm children's physical, psychological, and social well-being—such as depictions of violence, pornography, incitement to self-harm, promotion of drug use, and the misuse of personal data.

From a legal perspective, this issue intersects with the protection of children's rights, information security, and the allocation of responsibility among the state and digital platforms. Therefore, examining the legal mechanisms for safeguarding children from harmful content in the digital environment constitutes a highly relevant scholarly and legal inquiry. The objective of this article is to analyze the impact of harmful digital content on children's health, assess the legal mechanisms governing this sphere, study both international and national regulatory frameworks, identify existing shortcomings, and develop practical measures and recommendations.

In order to design effective mechanisms to protect children from health-impairing information in the digital sphere, it is essential first to clarify the meaning of the term "digital environment." The digital environment refers to the information space accessible to children via internet networks, mobile applications, social media platforms, video-sharing environments, and online games. The information disseminated within this environment constitutes content, which may be presented in the form of platform-based materials or interactive communication. Moreover, the concept of children's health encompasses not only physical well-being, but also

psychological health, mental development, and social and moral dimensions. Consequently, any form of information has the potential to influence children's cognition, development, behavior, and social interactions. Numerous scientific studies have identified specific categories of risks that children encounter in digital spaces. For example, Sonia Livingstone and her colleagues, in the report "The 4Cs: Classifying Online Risk to Children," demonstrate that children face online risks in four domains: content, contact, conduct, and contract [5]. Likewise, UNICEF's document "Children's Rights in the Digital Environment" underscores that the digital environment exerts both positive and negative impacts on children's rights and well-being [2].

Furthermore, international legal standards explicitly safeguard children's online rights, including access to information, safety, privacy, and the protection of personal data. In particular, Article 17 of the Convention on the Rights of the Child (1989) requires States Parties to ensure that children have access to information from mass media that is beneficial for their well-being, while also protecting them from harmful content. The General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment further expands states' obligations within the digital sphere. According to this document, states are required to ensure that digital products and services used by children are designed with their best interests in mind, enforce age-appropriate content controls, regulate data collection practices, guarantee privacy safeguards, and oversee the responsibilities of online platforms [2]. Under this General Comment, technology companies and online platforms are also required to adopt child-beneficial design principles, ensuring that digital systems are conceptualized and implemented in ways that prioritize children's rights and well-being. In this regard, the document promotes the integration of the "child rights by design" principle, which obliges platforms to implement effective content filtering, age-appropriate restrictions, and protective design features to create a safe online environment for children.

The General Comment No. 25 also outlines a set of specific obligations for actors involved in the digital ecosystem, particularly information technology developers. These obligations include applying the "child-rights by design" principle, creating systems that are age-appropriate, blocking harmful content, and ensuring robust protection of children's personal data. Additionally, documents adopted within the frameworks of the European Union and the Council of Europe provide guidance on mechanisms for safeguarding children online, such as age-verification systems, parental controls, and content-classification standards.

One of the notable international practices is the use of the "4Cs" model to categorize risks faced by children in the digital environment. This model encompasses four dimensions: content (risks arising from harmful material), contact (risks from harmful interaction), conduct (risks linked to a child's own behavior), and contract (commercial and transactional risks). These mechanisms can serve as important legal tools for protecting children's health, particularly in cases where exposure to violent content or targeted advertising may negatively affect their psychological well-being.

In Uzbekistan, several legal instruments exist to protect children's rights. For instance, the Law "On Guarantees of the Rights of the Child" establishes the fundamental state obligations for ensuring children's welfare. Likewise, the Law "On Informatization" defines key regulatory norms concerning information products, services, and their security. However, specialized legal mechanisms aimed specifically at combating harmful digital content affecting children's health remain underdeveloped. Age-verification procedures for accessing platforms, content-monitoring requirements, platform accountability standards, parental-control mechanisms, and algorithmic oversight are either limited or insufficiently implemented in practice. This situation, as revealed through legal and scholarly analysis, constitutes a significant regulatory gap. Given the rapid

evolution of digital technologies, legislative frameworks may lag behind, leaving children insufficiently protected in the online environment.

Various categories of information may adversely affect children's health in the digital environment. These include content promoting violence, pornography, self-harm or suicide, and drug use; applications that collect children's personal data or exploit them for advertising purposes; and platforms that expose children to inappropriate or harmful online interactions. Regulating this sphere therefore requires the development of comprehensive legal mechanisms.

Accordingly, digital platforms and service providers should be subject to obligations such as implementing reliable age-verification systems, obtaining parental consent, adhering to the data-minimization principle (privacy-by-default), and detecting and blocking harmful content. States, in turn, must exercise specific oversight functions, including establishing age-appropriate content classification systems (e.g., "12+," "16+"), adopting codes of online child protection, creating monitoring and supervisory bodies, and imposing sanctions for violations of established rules.

Ensuring children's safety in the digital environment also relies heavily on the involvement of parents and society. This includes promoting children's digital literacy, as well as providing parents with educational programs on online risks and effective monitoring tools. When these legal and educational mechanisms are properly implemented, they can play a decisive role in safeguarding children's physical and psychological well-being. For example, exposure to violent content may lead to psychological trauma, directly affecting a child's mental health; therefore, regulatory restrictions and oversight mechanisms serve to uphold the child's right to healthy development.

II. Metodology

In the present research, several methodological approaches were employed. The primary method utilized was normative–legal analysis, through which relevant legislative and regulatory instruments—laws, conventions, resolutions, and policy documents—were examined with regard to their content, structure, purpose, and legal obligations. Using this method, laws concerning the restriction of "harmful information," age-appropriate content frameworks, platform responsibilities, and state oversight mechanisms were analyzed. For instance, Article 17 of the Convention on the Rights of the Child and General Comment No. 25 serve as foundational normative documents for regulating children's rights in the digital environment. This method enabled the identification of legal obligations as well as gaps within existing legislation, thereby providing a basis for future legal reforms [11]. However, normative instruments often fail to respond promptly to rapidly evolving digital realities.

Another method applied was the analysis of policy and documentary materials. This involved systematically reviewing normative acts, policy papers, platform guidelines, research reports, and expert assessments. For example, the Council of Europe's "Handbook for Policy Makers on the Rights of the Child in the Digital Environment" was examined using this method. In academic literature, such approaches correspond to the methodologies of document research and literature critique [12].

A comparative legal analysis was also conducted, enabling the comparison of legal frameworks, regulatory practices, and platform governance standards across different jurisdictions. Within this research, France's 2023 law requiring parental consent for social media access under the age of 15, as well as recommendations from the Council of Europe, were analyzed to identify normative gaps within Uzbekistan's regulatory landscape. The comparative–legal method is crucial in legal scholarship, as it facilitates cross-jurisdictional learning and the transfer of best regulatory practices [13].

Additionally, the study made use of archival and data analysis techniques to examine the structure, algorithms, and age-appropriateness of advertisements, videos, and comment patterns on social networks. Through this analysis, harmful and inappropriate content was identified.

III. Results

The present study identified several legal challenges inherent in this regulatory field. Since digital platforms operate on a transnational scale, norms adopted within a single jurisdiction face a significant risk of non-enforceability beyond that territory. This problem arises from conflicts of laws, questions regarding the scope of application of national legislation, and uncertainties concerning jurisdictional boundaries.

Even within the European Union, the Digital Services Act (DSA)—although imposing requirements aimed at reducing risks for minors, ensuring safe-by-design features, and mandating protective default settings—faces enforcement difficulties. These challenges stem from the fact that platforms' "operational centers" and user bases are often distributed across multiple regions. In 2025, the European Commission issued guidance under Article 28 DSA clarifying its interpretation of risk assessment and mitigation obligations concerning minors. However, these guidelines constitute soft law, meaning they do not automatically guarantee compliance, thereby revealing practical enforcement gaps.

Livingstone emphasizes the importance of distinguishing between online risk and harm, arguing that the likelihood of harm increases when amplified by recommendation algorithms. This dynamic places an additional regulatory burden on authorities operating in a cross-border digital environment [5].

Another significant challenge concerns the technical complexity of age assurance. According to analyses by the European Parliament, many online services fail to implement adequate age-verification and parental-consent mechanisms. As a result, younger users can easily bypass the European Union's minimum age requirements [7]. A 2025 study further demonstrated that registration processes on major social media platforms rely heavily on weak age-verification methods—such as self-declaration and disposable email addresses—which can be easily circumvented when compared with verification standards in "adult-oriented" digital markets [8]. Under IEEE robustness criteria, substantial deficiencies have been identified in this domain.

The lack of parental oversight and digital literacy remains another urgent concern. A monitoring report on the implementation of the UK's Children's Code (AADC) by the Information Commissioner's Office (ICO) highlights that service design itself must support parental control. It identifies 15 default standards—including strict privacy settings, limits on profiling, deactivation of geolocation, and restrictions on manipulative "nudges"—that digital services should implement. Without such design features, excessive responsibility is shifted onto the user [4].

A theoretical foundation for this argument can be found in Cass Sunstein's "influence ethics" theory, which proposes that digital platforms owe minors an enhanced protective regime against manipulative nudging [10]. Accordingly, effective parental controls must be embedded within platform architecture; otherwise, the risk of manipulative influence on children increases.

Moreover, current normative instruments struggle to keep pace with rapidly evolving technologies. OECD recommendations urge states to adopt a proactive policy approach, introducing tools such as child-impact assessments and design-by-default mechanisms to anticipate risks rather than respond only reactively [3]. This underscores that a merely reactive legal framework is insufficient in the context of fast-advancing digital technologies.

IV. Discussion

A number of recommendations have been developed to address the identified problems:

First, it is necessary to adopt a specialized law on the "Protection of Children in the Online Environment." Such a law should incorporate obligations relating to the duty of care, age-appropriate design, mandatory child-impact assessments, and clear rules on oversight and sanctions. The UK Children's Code may serve as a practical model, as its standards have demonstrably led to tangible design changes in digital services. This model can be adapted to the national context.

Second, age verification, age restrictions for digital transactions, and mandatory parental consent must be formalized in legislation. The law should establish clear technical criteria for age-assurance mechanisms, including risk-based documentation, operator verification, parental-consent verification systems, and rules preventing acceptance of self-declaration without additional checks. This recommendation is supported by analyses from the European Parliamentary Research Service (EPRS), which indicate that children routinely bypass current verification systems. Studies conducted in 2025 further reveal that many major social media platforms fail to meet IEEE robustness standards. Thus, a multi-layered, risk-based age-assurance approach is necessary. For example, under France's 2023 law, the use of social media by children under the age of 15 requires parental consent, and platforms that violate this requirement may be fined up to 1% of global turnover.

Third, all platforms should be required to adopt "child-rights by design" and "privacy by default" principles. These include disabling profiling by default, restricting geolocation, limiting push notifications and direct messages during certain hours, filtering harmful content, and adapting advertisements or recommendations to children's age. The ICO's standards provide a regulatory foundation for these measures, while OECD principles designate such design requirements as approaching "mandatory norms."

Fourth, national programs on digital literacy and parental mediation should be developed. This includes integrating digital safety into school curricula, introducing mandatory facilitation courses for parents, and creating practical guides on media literacy and online behavior. Livingstone identifies both parental mediation and age-appropriate digital literacy as key determinants that reduce online risks for children.

Fifth, large digital platforms should be required to undergo an annual Child Safety Audit, with the audit results submitted to the national regulatory authority. The regulator would impose compliance-related sanctions where necessary and mandate corrective action plans for identified deficiencies. OECD principles and UNCRC General Comment No. 25 emphasize monitoring, accountability, and transparency as indispensable components of state policy in the digital environment.

V. Conclusion

The protection of children from harmful information in the digital environment has evolved into a complex legal domain situated at the intersection of state sovereignty, human rights, and technological ethics within today's globalized information ecosystem. In this field, not only normative–legal measures, but also principles of algorithmic fairness, platform accountability, and user well-being have become subjects of legal regulation. In other words, safeguarding children's rights is no longer merely a pedagogical or social concern; it is increasingly understood as a systemic issue that requires a legal balance across information policy, the data economy, and digital ethics.

According to Sunstein's theory of choice architecture, technological interfaces directly shape human behavior; therefore, the design of digital environments to which children are exposed must be integrated into the scope of legal responsibility. Likewise, the 4Cs model proposed by Livingstone and Stoilova demonstrates the importance of analyzing online risks through differentiated categories of content, contact, conduct, and contract. Together, these

approaches form the conceptual foundation of a new model of preventive law aimed at safeguarding children's psychological resilience.

The legal system of Uzbekistan must be effectively integrated into this global regulatory trajectory. Through the adoption of a dedicated Law on Online Child Safety, the introduction of mandatory child-impact assessment mechanisms, the establishment of age-appropriate design requirements, and the legal incentivization of parental mediation, the state, society, and the technological sector can collectively build a sustainable digital social contract. Strengthening the child's digital immunity thus becomes a key indicator of legal modernization and a central pillar of forward-looking regulatory policy.

References:

1. UN Committee on the Rights of the Child. (2021). General Comment No. 25 on Children's Rights in Relation to the Digital Environment.

2. UNICEF. (2021). General Comment No. 25 on Children's Rights in Relation to the Digital Environment.

3. Organisation for Economic Co-operation and Development (OECD). (2021/2022). Recommendation on Children in the Digital Environment: Principles and Policy Framework, Sections II–IV.

4. UK Information Commissioner's Office (ICO). Children's Code (Age Appropriate Design Code – AADC).

5. European Commission. (2025). Guidance on Article 28 of the Digital Services Act (DSA) Concerning Minors: Interpretation of Risk-Mitigation Obligations for Platforms.

6. Livingstone, S., & Stoilova, M. (2021). The 4Cs Model of Online Risk.

7. European Parliamentary Research Service (EPRS). (2023). Age Verification Brief: Analysis of Methods and Current Challenges.

8. Eltaher, A. (2025). Age Verification Effectiveness: Gaps in Relation to IEEE Robustness Standards.

9. Government of France. (2023). Law Requiring Parental Consent for Social Media Use by Children Under 15.

10. Sunstein, C. R. (2016). The Ethics of Influence: Government in the Age of Behavioral Science. Cambridge University Press.

11. Stadniczeńko, D. (2022). Children's Rights in the Digital Environment Under the Convention on the Rights of the Child. Tkppan, Vol. XV(2), 321–331.

12. Nawaila, M. B. (2018). A Review on the Rights of Children in the Digital Age. Children and Youth Services Review.

13. Guštin, M. (2022). Challenges of Protecting Children's Rights in the Digital Environment.