How to cite this article:
Amanat, M., Shamloo, S., & Jadali Araghi, S. (2025). International Legal Mechanisms for Protecting Child Content Creators on Social Media. *Journal of Historical Research, Law and Policy, 3*(3), 1-15. https://doi.org/10.61838/jhrlp.104

Article history:
Original Research

Dates:
Submission Date: 12 June 2025
Revision Date: 16 August 2025
Acceptance Date: 21 August 2025
Publication Date: 01 September 2025

International Legal Mechanisms for Protecting Child Content Creators on Social Media

1. Maryam. Amanat[1] : Department of Law, CT.C., Islamic Azad University, Tehran, Iran
2. Soodeh. Shamloo[2*]: Department of Law, CT.C., Islamic Azad University, Tehran, Iran
3. Safinaz. Jadali Araghi [3]: Department of Law, CT.C., Islamic Azad University, Tehran, Iran

*corresponding author's email: s.shamloo@iauctb.ac.ir

ABSTRACT

With the expansion of social networks and digital technologies, children have increasingly become not only consumers of online content but also active content creators. This phenomenon provides educational, social, and creative opportunities for children, yet it simultaneously entails risks such as violations of privacy, economic exploitation, and psychological harm. Using a descriptive–analytical approach and based on documentary studies, this article examines the international legal mechanisms for protecting child content creators on social media. Key instruments such as the Convention on the Rights of the Child (1989), its Optional Protocols, General Comment No. 25 of the Committee on the Rights of the Child (2021), and operational frameworks issued by UNICEF and UNESCO are analyzed. The core axes of the analysis include the protection of privacy and data, prevention of economic exploitation, ensuring equitable access to digital opportunities, informed participation, and the educational empowerment of children. The findings indicate that international law, by providing binding and non-binding instruments, has established a relatively comprehensive framework for the protection of children; however, challenges such as the rapid pace of technological change, weak international monitoring and reporting systems, and the absence of effective enforcement mechanisms continue to hinder the full realization of protective goals.

Keywords: *child rights, content creation, social networks, international protection, children's privacy*

Introduction

The digital space and social networks in the present era have evolved into platforms far beyond communication and entertainment, playing a significant role in content production, the formation of social identity, and even income generation. Children, as an active group in this environment, are present both as consumers and as producers of content. Content created *by* children includes creative, educational, and entertainment activities, while content created *about* children involves the publication of their images, voices, or personal information by parents, brands, or media. These phenomena create opportunities such as the development of digital skills, strengthening of social abilities, and active participation in the information society, yet they are accompanied by serious threats as well (1).

Threats such as violations of privacy, economic exploitation, media-driven manipulation, and psychological harm are among the most significant challenges related to children's presence on social networks. Due to their young

age and incomplete understanding of the consequences of their online activities, children are vulnerable to misuse and exploitation. In some cases, the economic benefits derived from children's digital activities accrue to parents or advertising companies without providing a fair share to the child.

International law has attempted to guarantee the protection of children through the *1989 Convention on the Rights of the Child* and its Optional Protocols; however, many of these instruments were drafted before the emergence of social networks and modern technologies. Concepts such as "child influencer" and "digital exploitation" are not clearly defined within these frameworks, and the available international enforcement mechanisms are limited (2).

Issues of privacy and data protection have also become more complex with the rise of artificial intelligence and data-analysis algorithms. Profiling, targeted advertising, and the collection of children's personal information have raised serious concerns, while no comprehensive binding international treaty exists to address these challenges.

Furthermore, the conflict between the right to freedom of expression and the right to protection from online harms remains one of the central legal challenges. Children must be able to express themselves and participate socially, yet they simultaneously require protection from harmful content and online abuse. Achieving balance between these two rights has not yet been fully resolved within international legal systems.

Digital inequality also affects the effectiveness of protective mechanisms. Children in disadvantaged regions or those with disabilities may lack access to digital education and safe technologies, which results in unequal enjoyment of digital rights (3).

At the national level, states have attempted to create safe environments for children by adopting legislation and strategic documents—such as national frameworks for the protection of children and adolescents in cyberspace—aimed at ensuring responsibility for content monitoring. Families also play a crucial role in managing children's digital presence and must guide them effectively by selecting appropriate games and content and by improving their own digital literacy.

Education and empowerment of children and parents—particularly in the areas of media literacy, privacy protection, online behavior management, and ethical skills—form an essential aspect of safeguarding children in the digital environment. These actions enhance children's independence, awareness, and sense of responsibility, enabling them to participate actively and safely in social networks (4).

The case study of child bloggers represents a practical example that highlights the need to protect children's rights in the digital sphere. Due to their extensive online activity, these children are exposed to various forms of exploitation and require legal and protective frameworks that safeguard their economic rights, privacy, and psychological well-being.

Ultimately, legal and scholarly analysis of these phenomena can contribute to the development of preventive policies and mechanisms, strengthen enforcement guarantees, and create forward-looking frameworks to ensure the dignity, security, and welfare of children in the digital age, enabling future generations to benefit safely and responsibly from digital opportunities.

International Legal Protection Mechanisms for Children's Content Creation on Social Networks

Platform Responsibility

The responsibility of social media platforms regarding the production and dissemination of child-related content—especially in educational, entertainment, and advertising contexts—holds significant complexity in both international law and national legal systems. These responsibilities include protecting children's privacy, preventing economic and social exploitation, and ensuring access to healthy and appropriate content (5, 6).

At the international level, instruments such as the *Convention on the Rights of the Child* obligate states to take measures to protect children from harmful information and materials, emphasizing the role of media and digital platforms in providing safe content (7). At the national level, various states have adopted regulations aimed at strengthening platform accountability; for example, the United Kingdom implements age-appropriate design requirements (8), and the United States restricts the collection of data from children under 13 to situations with verified parental consent (9).

Platforms must establish monitoring and content-management mechanisms to detect and remove harmful or illegal content; such mechanisms include algorithmic filtering tools, human review teams, and user reporting features. Additionally, providing parental-control tools, age restrictions, protection of children's personal data, prevention of inappropriate commercial use, and ensuring data security are among the essential duties of platforms. Educating children and parents, offering guidelines for safe digital engagement, and maintaining transparent and accessible policies help build user trust and facilitate oversight of platform practices (10).

Moreover, platform responsibility also includes reducing psychological and social threats to children, participating in international cooperation to combat harmful content, designing child-centered and safe technologies, and creating mechanisms for rapid response to complaints and violations (11).

Continuous monitoring and evaluation of platform performance in safeguarding children and protecting privacy, issuing transparent public reports, and improving policies are also necessary components of platform accountability (12, 13). Overall, platform responsibility is multidimensional and includes privacy protection, content management, user education, safe design, accountability, and ongoing oversight. Achieving these responsibilities is essential for creating a secure and supportive environment for children on social networks and plays a key role in reducing risks and ensuring children's digital rights. Additionally, these efforts must align with ethical, cultural, and social standards to ensure that while protecting children's rights, legitimate user freedoms are also preserved (14).

Protection of Children's Data and Privacy

Protecting children's data and privacy in the digital environment is one of the most important responsibilities of social platforms and international legal frameworks, as children—due to their young age and limited awareness of online risks—are more vulnerable, and their personal information can easily be misused (15). According to the *Convention on the Rights of the Child* and the recommendations of the Committee on the Rights of the Child, states and platforms are obliged to adopt preventive measures to avoid the unauthorized collection, storage, and processing of children's data (7). At the national level, countries such as the United States require companies to obtain parental consent before collecting data from children under age 13 (9), and in the European Union, regulatory standards and age-appropriate design codes obligate platforms to implement protocols for children's privacy and restrict targeted advertising based on children's profiles (8).

Platforms must implement technical and operational systems such as data encryption, parental-control tools, reporting mechanisms, and data-deletion options to limit access to children's personal information, and must provide education for child users and parents regarding risks associated with data collection and privacy protection (16). Practical challenges include verifying the exact age of users, the complexity of emerging technologies such as artificial intelligence and machine learning, and differences among national laws, all of which can make legal data protection more difficult (17). Successful international examples include the European Union's implementation of design-code requirements and the United States' enforcement actions against violating companies, demonstrating that strict laws can improve children's data protection (8).

The protection of children's data and privacy includes preventing unauthorized use, sale, or commercial exploitation without parental consent, and requires legal frameworks, technical standards, and user education. Educating children and parents, designing privacy-protective default systems, continuous monitoring of data access, and transparent reporting are essential tools for this protection. Using artificial-intelligence technologies to detect risks can also be beneficial. Overall, safeguarding children's data and privacy requires a combination of legal, technological, and educational measures that not only reduce psychological and social harms but also strengthen parental and child trust in the digital environment and enable safe and responsible use of social networks.

Limiting Economic Exploitation

Limiting the economic exploitation of children in the digital environment is a key component of international and national child-rights protection, as content produced by children or the commercial use of their images and activities on social networks can constitute economic exploitation, especially when monetization occurs through advertising, sponsorships, or product sales (18). The *Convention on the Rights of the Child* and the Optional Protocol on the sale, prostitution, and pornography of children obligate states to prevent the economic exploitation of children and require platforms to comply with legal limitations (12).

At the national level, different countries have adopted various laws to regulate economic exploitation. For instance, France's *Loi n° 2020-1266* restricts economic exploitation of children's images on online platforms and imposes strict requirements for parental consent and monitoring of child-produced content (19). In the United States, child-protection laws and lawsuits against companies such as Google and YouTube demonstrate that commercial use of children without compliance can lead to prosecution and fines (9). Australia also enforces similar laws to protect child influencers and prevent economic misuse (20).

Platforms must adopt policies to limit the economic exploitation of children, including restricting targeted advertising, setting income limits or types of content allowed for children, and providing guidance and information to parents regarding economic risks associated with children's digital activity (6). International cooperation and the implementation of shared standards—such as OECD guidelines—can help prevent large-scale economic exploitation (12, 13).

Practical challenges include difficulties in monitoring content produced by children, diversity of national laws and their international enforcement, and the emergence of new digital advertising technologies that may obscure or intensify economic exploitation (21). Limiting economic exploitation requires a combination of national legislation, international standards, platform responsibility, and parental awareness to ensure that as social networks evolve, children's economic security is protected (6).

Overall, limiting economic exploitation involves establishing legal regulations, enforcing policy mechanisms, educating children and parents, and using technology for monitoring and control. These measures allow children to benefit from the digital environment safely and without economic pressure, while protecting their economic and social rights. Observing these principles also promotes healthy and responsible use of social networks and enhances family and societal trust in digital spaces.

International Monitoring and Reporting

International monitoring and reporting in the area of children's rights in the digital environment—particularly regarding content produced by children—constitutes one of the essential mechanisms of international law to ensure implementation of standards and protection of children's rights. International organizations such as the Committee on the Rights of the Child, UNICEF, UNESCO, and the UN Human Rights Council have developed frameworks for monitoring children's digital environments and require member states to submit periodic reports on their actions (7). These reports provide information on policies, national laws, platform activities, and implementation challenges, enabling an accurate assessment of children's situations in digital environments (15).

Operationally, platforms are also required to submit data related to child-produced content, minors' access to harmful materials, and measures taken to remove or restrict such content to regulatory bodies (16). These data help national and international institutions identify emerging risks and threats and issue recommendations or corrective measures in cases of rights violations (14).

Successful international examples include the European Union's "Better Internet for Kids" initiatives and periodic reports on children in the digital environment, providing statistical and analytical information on children's internet access, the degree of risks, and protective measures (22). UNICEF also publishes annual reports assessing the protection of children on social networks and encourages member states to improve policies and enforcement of relevant laws (12).

Nevertheless, challenges exist within these mechanisms, including lack of coordination among countries, variations in national laws, and technical limitations in data collection. Children may provide incorrect age information or use tools to conceal their digital identity, which affects the accuracy of reports (17). However, international monitoring and regular reporting enable the identification of emerging digital trends and threats, provide policy guidance, and exert pressure on platforms to fulfill their responsibilities (14).

Ultimately, combining international monitoring, transparent reporting, and national law enforcement creates an effective mechanism for protecting children in digital spaces, preventing economic exploitation, harmful content dissemination, and violations of privacy (6). This mechanism increases transparency, accountability, and international cooperation, forming a strong foundation for protecting children's digital rights and ensuring policy reform and stronger commitment from states and platforms.

Guidelines and Ethical Codes for Content Creation

Guidelines and ethical codes for content creation by or about children in the digital environment play a crucial role in protecting their rights and function as a complement to national and international laws. These frameworks provide platforms, parents, and content creators with instructions to ensure that the content produced complies with ethical and legal standards and prevents exploitation, abuse, or psychological harm to children (5).

At the international level, organizations such as UNICEF and UNESCO have developed frameworks for the publication of content and the protection of children. For example, the “Better Internet for Kids” initiative recommends that content should be transparent, age-appropriate, and free from harmful economic or advertising pressures (12). Likewise, the UN Committee on the Rights of the Child recommends that states and platforms adopt ethical guidelines for the production and dissemination of digital content so that the best interests of the child are treated as the primary consideration (7).

Successful national examples include the “design code” guidance in the United Kingdom, which requires platforms to tailor their design and content to children’s needs and safety and to prevent exploitation or exposure to inappropriate material (8). In Iran, researchers have also recommended the development of specialized laws and ethical guidelines to protect child influencers and underage users so that the use of their content in advertising or economic activities is regulated and controlled (6).

These guidelines and codes typically include provisions such as respect for privacy, limiting the dissemination of harmful content, preventing targeted advertising to children, involving parents in decision-making, and educating children about the risks of the digital space (15). However, the main challenge in implementing these codes is their adaptation to new technologies, artificial-intelligence algorithms, and differences among national legal systems, which may lead to violations or divergent interpretations of children’s rights (23).

Overall, guidelines and ethical codes are vital tools for complementing legal mechanisms and strengthening the social responsibility of platforms, and they play a key role in reducing economic exploitation, protecting privacy, and ensuring healthy content for children. By establishing global standards, increasing parental and child awareness, and enhancing platform accountability, these frameworks help make the digital environment safer and more ethical for underage users.

Access Control and Age Restrictions

Access control and age restrictions on social networks are among the key mechanisms of international law for protecting children in the digital environment. They are designed to prevent children’s exposure to inappropriate content and to reduce risks related to economic exploitation, psychological harm, and privacy violations (10). These mechanisms require platforms to create systems capable of identifying users’ ages and, based on that, restricting access to harmful content or economic activities (16).

At the international level, the Children’s Online Privacy Protection rules in the United States oblige platforms to obtain parental consent before collecting data from children under 13 and to limit their access to certain services or types of content (9). In the European Union, age-appropriate design guidance and EU regulatory standards similarly require that platform design be aligned with children’s protective needs and applicable age limits (24).

Some countries, such as France and Australia, have enacted strict national laws to limit children’s access to social networks. For example, French legislation (*Loi n° 2020-1266*) sets specific age restrictions and requires platforms to accurately verify users’ ages and provide age-appropriate content. These laws not only protect children but also increase platforms’ responsibilities to prevent economic exploitation and the dissemination of harmful content.

Nonetheless, there are practical challenges in enforcing age restrictions, including children providing inaccurate age information, difficulties in monitoring published content, and the use of new technologies to circumvent restrictions (17). Despite these challenges, implementing access control and age restrictions, combined with

educating parents and children, reporting systems, and ethical guidelines, remains one of the most effective tools for reducing digital risks and safeguarding children's rights (6).

This mechanism enables platforms to offer their content and services with social responsibility and in line with international standards, preventing economic exploitation, targeted advertising, and violations of children's privacy (14). Access control and age restrictions help ensure that children are exposed only to content appropriate to their age and psychological maturity and that the digital environment remains safe and healthy. They also provide parents and regulatory bodies with better means to manage children's digital experience and fulfill part of the social responsibility of platforms and content producers.

Education and Empowerment of Children and Parents

Education and empowerment of children and parents is one of the fundamental mechanisms for protecting children's rights in the digital environment, aimed at increasing awareness of online risks, safeguarding privacy, and reducing economic exploitation. This mechanism includes teaching children digital skills for safe and informed use of social networks, recognizing inappropriate content, and managing online behavior, as well as empowering parents to supervise effectively, configure privacy settings, and guide children in the digital environment. Practical tools such as parental-control software, safe-use guidelines, and digital counseling programs are also part of this approach. Successful international examples, including the Better Internet for Kids program in the European Union and educational campaigns in the United States, show that combining education, empowerment, and legal and ethical policies can make the digital environment safer and prevent economic, advertising, and psychological exploitation of children. Ultimately, digital education and empowerment enhances the social responsibility of platforms, strengthens cooperation among families, schools, and governmental and non-governmental institutions, and provides safe educational, recreational, and social opportunities for children.

Multilateral Cooperation and International Agreements

Multilateral cooperation and international agreements play a central role in protecting children in the digital environment and in the context of their content creation, since online threats are often transboundary and complex, and the actions of a single state are not sufficient. The Convention on the Rights of the Child and its Optional Protocols establish an international legal framework, while organizations such as UNICEF and UNESCO facilitate coordination among governments and platforms by formulating global standards and guidelines. Programs such as "Better Internet for Kids" in the European Union make it possible to share data, exchange best practices among countries, and cooperate in implementing protective policies. These collaborations increase platform accountability, strengthen states' enforcement capacities, enhance education and awareness among parents and children, and establish global standards for privacy protection and prevention of economic exploitation. Without such international engagement, national efforts alone cannot ensure full security, fairness, and protection of children's digital rights, and multilateral cooperation forms the foundation for a safe, sustainable, and coherent global digital environment for children.

Challenges of International Protective Mechanisms for Safeguarding Children in the Digital Environment

Rapid Pace of Technological Change

The rapid pace of transformation in digital technologies is one of the fundamental challenges in protecting children in cyberspace. The continuous expansion of social networks, online games, and artificial intelligence systems has exposed children to risks such as unauthorized collection of personal data, targeted advertising, and digital exploitation (25). On the other hand, national and international laws and regulations, due to the time-consuming process of drafting and adoption, are unable to keep pace with the speed of technological developments (21).

Successive innovations have delayed the updating of international standards and guidelines, and the actions of institutions such as UNICEF and UNESCO in awareness-raising and regulation lag behind technological change. As a result, parents and regulatory bodies are often unable to effectively monitor or guide children's digital behavior.

Therefore, to counteract the negative effects arising from rapid technological change, it is essential to establish flexible protective mechanisms, regularly review laws, enhance parental and child education, and strengthen cooperation among governments, international organizations, and digital platforms (19). This approach can improve the protection of children's rights and reduce harms associated with the fast-paced digital environment.

Lack of Cross-Border Coordination

The lack of cross-border coordination is one of the most significant challenges in protecting children in the digital environment. The global nature of social networks and online platforms means that activities and content related to children extend beyond national borders, and domestic laws are often unable to comprehensively cover such situations (14). Because platforms such as YouTube, TikTok, and Instagram maintain offices and servers in different countries, the uniform enforcement of national laws becomes difficult, creating legal gaps and limiting the ability to prosecute abusers effectively (21).

International bodies such as UNICEF and the UN Human Rights Council have attempted to strengthen cooperation among states by providing shared frameworks and guidelines, but differences in legal systems, political constraints, and the absence of binding obligations have hindered the achievement of effective coordination.

As a result, many platforms exploit these inconsistencies to disseminate harmful content or misuse children's data at the international level. For example, in some cases, children's data in African and Asian countries have been processed on servers located in Europe or the United States, making legal follow-up difficult (26).

Overall, the lack of cross-border coordination prevents effective monitoring and enforcement of laws and reduces platform accountability. To address this challenge, it is necessary to draft binding international treaties, establish joint supervisory bodies, and ensure rapid information exchange among states so that children's digital rights are protected globally.

Enforcement Limitations

Enforcement limitations are among the most important obstacles to the realization of international protective mechanisms for safeguarding children in the digital space. Despite the existence of various national and supranational laws, including European Union regulations and children's online protection laws in the United States, the practical implementation of these rules faces numerous difficulties (25). A lack of financial and human resources,

weak technical infrastructure, and technological constraints make effective monitoring of social networks and online content difficult (27).

Moreover, insufficient preparedness and lack of training among supervisory and judicial personnel hinder the prompt and accurate handling of child-related violations (28). In addition, the inadequate cooperation of technology companies and digital platforms with governments has further complicated law enforcement. In many cases, even where legal judgments exist, the process of pursuing and imposing penalties on violating companies remains lengthy and inefficient.

Weak interaction between public authorities and the private sector has also prevented preventive measures—such as harmful-content reporting systems and automated monitoring—from being fully implemented. This problem is more acute in developing countries, where fragile technological infrastructures and a shortage of specialized personnel hinder the effective enforcement of regulations (26).

Taken together, enforcement limitations show that the existence of laws alone is not sufficient; to achieve real protection for children in cyberspace, it is necessary to expand specialized training, strengthen resources, improve infrastructure, and enhance international cooperation between governments and technology companies.

Conflict with Freedom of Expression

Conflict with freedom of expression is one of the core challenges in implementing international protective mechanisms for children in the digital environment. Laws and regulations aimed at ensuring children's safety and mental well-being can sometimes restrict their access to information and opportunities for creative expression (7). For example, limiting children's presence on social networks or removing content produced by them, while reducing the risk of exploitation, may weaken their freedom of expression and their right to active participation (18).

In some cases, parents or governments, relying on protective laws, remove educational or cultural content produced by children, resulting in unnecessary restrictions on freedom of expression. Furthermore, automated content-removal algorithms and systems used by platforms—due to technical errors or data bias—may also block harmless or beneficial content (11).

Consequently, the tension between protection and freedom of expression indicates that protective policies must be tailored to children's age, level of maturity, and cultural context so that a fair balance between protection and empowerment in the digital environment can be maintained.

Weaknesses in Education and Awareness

Weaknesses in education and awareness constitute one of the fundamental challenges to the effectiveness of international protective mechanisms for children in the digital environment. Many children, parents, and even teachers lack sufficient digital literacy to use the internet safely and identify its risks (10). This lack of knowledge prevents children from recognizing threats such as economic exploitation, digital sexual abuse, or privacy violations, and parents are unable to provide effective protection.

In many countries, formal education on digital rights and online safety either does not exist or is offered in a limited and impractical manner (20). Even in existing educational programs, the content is often outdated and inconsistent with new technologies, whereas the digital environment is changing at high speed (7).

In developing countries, weak educational infrastructure, scarce financial resources, limited internet access, and the absence of specialized trainers mean that digital education programs lack the necessary effectiveness (26). In

addition, many parents are unaware of monitoring tools and safety settings on platforms, resulting in inadequate supervision of children's online behavior (29).

This lack of awareness undermines the effectiveness of international and national laws, such as data-protection laws, digital regulations, and online child-protection acts, because without empowering families and underage users, no legal mechanism can function effectively on its own (21). Therefore, comprehensive and continuous digital-literacy education for children, parents, and teachers, the development of age-appropriate educational content, and cooperation between governments and international organizations to expand educational programs are key strategies for addressing this challenge (12, 22).

Deficiencies in Platform Accountability

Deficiencies in platform accountability are another major challenge in protecting children in the digital environment. Many social networks and online platforms, despite the existence of national and international rules such as data-protection and digital-services laws and children's online protection regulations, do not fully meet their responsibilities regarding content produced by or about children (21, 24). This problem stems from weak oversight, technological complexity, inadequate internal policies, and a lack of transparency in content management and recommendation algorithms.

Platforms often fail to adequately detect and remove harmful content or digital exploitation, and reporting procedures for users and parents are complex and time-consuming (19). These shortcomings expose children to psychological risks, sexual abuse, or economic exploitation, even where applicable laws exist (18). A practical example is the Google and YouTube case in the United States, which resulted in a 170-million-dollar fine for violating children's online privacy rules (9).

Deficient platform accountability also creates international regulatory gaps, as companies can evade full compliance with national or regional rules by locating servers and offices in different jurisdictions (26). In addition, the lack of user and parental education, the absence of effective parental-control tools and age-verification systems, and insufficient oversight of child-targeted advertising increase children's vulnerability.

Lack of Effective Self-Regulatory Mechanisms

The lack of effective self-regulatory mechanisms is one of the key challenges in protecting children in the digital environment. Many online platforms, even in the presence of national and international laws such as data-protection, digital, and online child-protection regulations, are unable to fully manage content and protect children due to the absence of coherent internal frameworks and precise operational policies (19, 21).

Self-regulatory mechanisms include platforms' internal policies and protocols for identifying and removing harmful content, restricting children's access to inappropriate material, and controlling the dissemination of personal data. The ineffectiveness of these mechanisms exposes children to digital violence, sexual abuse, and economic exploitation (11, 18). An example of weak self-regulation is seen in ineffective reporting systems or delayed platform responses to user complaints (12, 13).

This weakness is even more pronounced in developing countries and disadvantaged regions, where there are insufficient resources and oversight to control online content (26). In addition, the lack of adequate education for children and parents means that even where policies and restrictions exist, children may still remain at risk.

Access Barriers and Digital Inequality

Access barriers and digital inequality are among the fundamental challenges in protecting children in the digital environment. Despite technological progress and the expansion of the internet, many children—especially in developing countries and deprived areas—lack access to high-speed internet and digital tools, which deprives them of educational, recreational, and participatory digital opportunities while simultaneously exposing them to online threats (26).

This inequality prevents international policies and regulations—such as data-protection frameworks and the guidelines of UNICEF and UNESCO—from uniformly protecting all children (12, 13). Children with limited access may remain unaware of digital-literacy training and preventive programs and may be unable to recognize risks arising from harmful content or digital exploitation (20).

In developing countries, weak infrastructures, high internet costs, and a shortage of digital devices aggravate disparities in protecting children, and even in developed countries, a digital divide exists between urban and rural areas or between low-income and high-income groups (12, 26).

To mitigate this challenge, it is necessary to implement programs that ensure equitable access to technology, develop infrastructure, and provide digital education for children and parents. Combining these measures with legal mechanisms and educational efforts can reduce digital inequality and enhance the effectiveness of international policies and regulations in protecting children (13, 22).

Lack of Data and Accurate Reporting

The lack of comprehensive data and reporting is one of the main obstacles to assessing and strengthening international protective mechanisms for children in the digital environment. Many states and platforms lack integrated systems for collecting information on children's activities on social networks, resulting in decisions and policies being based on incomplete data and diminishing the effectiveness of legal protections (12, 20).

Incomplete or non-transparent reporting by platforms and public authorities also hinders the precise identification of risks related to harmful content, economic exploitation, and sexual abuse of children (18, 19). This data gap further obstructs international comparison and evaluation of the effectiveness of laws such as data-protection rules, digital regulations, and online child-protection acts (9).

In developing countries, weak data-collection and analysis infrastructures exacerbate this problem, and many disadvantaged children are not captured in official reports (26). To address this challenge, it is essential to strengthen data-collection and analysis systems, establish clear international reporting standards, and enhance cooperation among governments, international organizations, and platforms (12, 13).

Cultural and Social Challenges

Cultural and social challenges are also important obstacles to implementing international protective mechanisms. Differences in attitudes and cultural norms across societies can influence how children use the digital environment and the degree to which protective regulations are accepted (30). For example, in some communities, sharing children's images or their active participation on social networks is considered part of family culture, even though such practices can increase risks related to privacy and digital exploitation (31).

Varying levels of digital literacy and awareness among parents and teachers also affect children's vulnerability. In contexts where there is limited understanding of data protection and the risks of online content, protective regulations are not effectively implemented (10).

Furthermore, gender discrimination, economic disparities, and unequal access to technology expose particular groups of children—such as girls or children from low-income families—to greater risks (13). Cultural resistance to external monitoring and regulation can also obstruct the effective implementation of international rules (7).

Strategies for Addressing the Challenges of International Protective Mechanisms for Children in the Digital Environment

Strategies for addressing the challenges of international protective mechanisms for children in the digital environment encompass several key dimensions. First, strengthening national and international laws and regulations is of critical importance; updating and aligning existing laws with rapid technological changes, drafting comprehensive regulations, and adopting international treaties can provide the legal framework necessary to protect children's data and privacy and to clarify the responsibilities of platforms and digital entities. Second, establishing effective cross-border mechanisms to combat international abuses is essential, including international agreements, judicial-cooperation protocols, and common platform standards that can increase responsiveness and reduce legal gaps. Third, enhancing the enforcement and oversight capacity of public authorities and organizations for monitoring online activities, identifying harmful content, and implementing laws—alongside transparent reporting systems—is a key requirement for effective implementation.

Fourth, maintaining a balance between child protection and freedom of expression is vital; laws and policies should provide age-appropriate and needs-based frameworks so that freedom of expression is not unduly restricted, and the use of intelligent content-control tools and digital education can enable safe and responsible participation by children. Fifth, increasing education and awareness among parents and children about online risks and protective strategies is one of the most effective ways to reduce vulnerability and must be combined with parental-control tools and platform ethical codes. Sixth, strengthening platform accountability through obligations related to transparency, reporting, systematic risk assessment, and an organizational culture committed to child protection helps ensure a safe and fair digital environment.

Seventh, developing and improving platforms' self-regulatory mechanisms—including intelligent algorithms for detecting harmful content, age restrictions, advanced filters, and rapid reporting systems—must be combined with external oversight and binding regulations. Eighth, reducing digital inequality and ensuring fair access to technology, including infrastructure development, subsidized internet and educational devices, and training in digital skills and media literacy, is needed so that all children, regardless of geographical or economic status, can benefit from digital opportunities. Ninth, strengthening data collection and accurate reporting through coherent statistical systems, internationally comparable data, and transparent platform reporting enables evidence-based policymaking and evaluation of the effectiveness of protective measures. Finally, attention to cultural and social dimensions—including the participation of local communities and parents, localization of digital-literacy training, and recognition of gender and class differences—ensures that policies are both legally valid and socially acceptable and applicable. Together, these measures, through an integrated approach, combine law, education, oversight, and platform responsibility and make it possible to create a safe and equitable digital environment for children.

Conclusion

This study showed that protecting child content creators in cyberspace is a multidimensional issue dependent on the cultural, social, and legal conditions of each country. In the United States, children's online privacy law, with its focus on protecting the privacy of children under the age of thirteen, represents an important step in safeguarding data but pays less attention to economic, social, and intellectual-property dimensions. In the European Union, comprehensive data-protection regulations, with a child-centered and multidimensional approach, have provided a broader protective structure, although their uneven implementation across member states has created challenges. France, by adopting special legislation to protect children active on social networks, has introduced an innovative focus on the financial and social aspects of their activities.

In Iran, despite some general laws related to child protection and cybercrime, there is still no specific and independent statute for safeguarding children in the digital environment. Weaknesses in monitoring, education, and awareness-raising have left children exposed to economic exploitation, privacy violations, and psychological harms.

At the international level, instruments such as the Convention on the Rights of the Child, the General Comments of the Committee on the Rights of the Child, and the guidelines of international organizations emphasize principles such as privacy protection, prohibition of exploitation, the right to participation, and children's safe access to the digital environment. Despite the importance of these frameworks, the lack of sufficient enforcement guarantees and the rapid pace of technological change have prevented some emerging threats from being adequately controlled.

To address these gaps, it is essential to draft comprehensive national legislation, establish independent supervisory bodies, educate parents and children, and strengthen the responsibilities of virtual platforms. In addition, the use of intelligent technologies to detect and remove harmful content, the development of parental-control tools, and the creation of effective reporting systems can contribute to enhancing the safety of children in cyberspace.

Ultimately, real protection of child content creators requires a comprehensive approach that integrates targeted legislation, education, cultural change, effective oversight, and international cooperation. Only through such an integrated framework can a safe, healthy, and constructive environment be created for children's presence in the digital world.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Amiri M. Legal Challenges to the Protection of Children in Cyberspace. Research in Technology Law. 2021;12(1):45-60.
2. Bani Hashemian SM. Investigating the Status of Children's Rights in Iran's Social Networks 2024.
3. Jalali M, Sadat R. The Necessity of Formulating Specialized Laws for the Protection of Child Influencers in Cyberspace. Journal of Law and New Technology. 2022;2(3):105-23.
4. Hossein Pour Z. Iran's Legal Protections for Online Children Based on the OECD's Typology of Risks 2024.
5. Shari'ati M, Zamanian M, Khalili M. Publication of Children's Images in Cyberspace and Its Impact on Pre-Puberty Personality Development, in Light of Iranian Law and International Regulations. Journal of Law and New Studies. 2021(2).
6. Farahani M, Karimi D. The Rights of Child Influencers on Social Networks: Requirements and Challenges. Journal of New Legal Studies. 2023;3(1):50-75.
7. Child UNCotRot. General Comment No. 25 on Children's Rights in Relation to the Digital Environment. 2019.
8. Information Commissioner's Office. Age Appropriate Design Code. 2021.
9. Federal Trade C. Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law. 2019.
10. Panahi S. The Role of Parents and Teachers in Protecting Children's Privacy in Cyberspace. Quarterly Journal of Child Law. 2022;3(2):65-82.
11. Gillespie T. Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media: Yale University Press; 2021.
12. Unicef. Protecting Children in the Digital Age: Challenges and Opportunities. New York: UNICEF Publications, 2022.
13. OECD. Protecting Children Online: OECD Guidelines. 2020.
14. Rashidi N. Multilateral Cooperation in the Protection of Children's Digital Rights. Journal of International Studies. 2022;15(1):120-45.
15. Livingstone S, Stoilova M, Nandagiri R. Children's data and privacy online: Growing up in a digital age. UNICEF Office of Research - Innocenti, 2019.
16. Musavi S. The Role of International Organizations in the Protection of Children in Cyberspace. Research Journal of Information Technology Law. 2020(4):75-102.
17. Livingstone S, Stoilova M, Nandagiri R. Children's data and privacy online: Growing up in a digital age. 2021.
18. Charlotte BW. Kidfluencers: How the Law's Failure to Keep up Leaves Children across the Country at Risk of Labor Abuse and Financial Exploitation. Charleston L REV. 2022;16:111-2022 46.
19. European Commission. BIK+ Strategy: Better Internet for Kids Plus. 2022.
20. Fereshteh N, Davoud T, Bahram Saleh S, Gholam Ali A. A Comparative Study on the Opportunities and Threats of the Internet and Considering the Rights of Kids Online in Australia, Brazil, Iran, and South Africa. 2021;4(4):1550-74.
21. Ahmed B. Regulating Cyberspace for Children: Reflections on the Qatari Case. British Journal of Cyber Criminology. 2024.
22. Oecd. Children in the Digital Environment: Revised Recommendation. 2021.
23. Burgess J, Green J. YouTube: Online Video and Participatory Culture: Polity; 2018.
24. European Data Protection B. Guidelines on Children's Data. 2020.
25. Hosseini Z. Obstacles to the Implementation of International Regulations on the Protection of Children in the Digital Space. Quarterly Journal of Information Technology Law. 2022(7):135-60.

26. Ezekia G, Abdul M, Gideon R. Protecting Africa's Future: Cybersecurity Strategies for Child Safety, Learning, and Skill Acquisition in Tanzania. 2024.
27. Rahmani M. Executive Obstacles to the Protection of Children in the Digital Space in Developing Countries. Journal of Comparative Legal Studies. 2020(10):80-110.
28. Najafi F. Legal Study of Children's Privacy in the Digital Space. Legal Research. 2021;8(1):97-115.
29. Meta. Parental Supervision Tools on Instagram. 2022.
30. Staksrud E, Ólafsson K. Children's rights and parental responsibilities in the digital age. New Media & Society. 2020;22(7):1189-206. doi: 10.1177/1461444819876576.
31. Steinberg SB. Sharenting: Children's privacy in the age of social media. Emory Law Journal. 2017;66(4):839-84.