Information for citation:
Miruktamova, F. L. (2026). Rethinking the International Legal Protection of Children's Rights in the Digital Environment: Contemporary Challenges and Emerging Approaches. *European and Asian Law Review*. 9 (3), 95–105. DOI: 10.34076/27821668_2026_9_3_95.

Для цитирования:
Мируктамова Ф. Л. Переосмысление международно-правовой модели защиты прав детей в цифровой среде: современные вызовы и новые подходы // European and Asian Law Review. 2026. № 3. Т. 9. С. 95–105. DOI: 10.34076/27821668_2026_9_3_95.

УДК 341.231.14:342.7(575.1)
BISAC: 05100
DOI: 10.34076/27821668_2026_9_3_95

Research Article

RETHINKING THE INTERNATIONAL LEGAL PROTECTION OF CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT: CONTEMPORARY CHALLENGES AND EMERGING APPROACHES

Feruza L. Miruktamova
Tashkent State University of Law
ORCID ID: 0000-0002-9793-3717

Digital transformation has profoundly changed the mechanisms through which children's rights are exercised and protected, challenging traditional approaches to international legal regulation. This article examines the evolution of the international legal model for the protection of children's rights by analyzing contemporary digital risks through the framework of universal and regional international legal instruments, the practice of international organizations, and recent legal scholarship. It argues that digital risks should be understood not merely as new categories of threats but as indicators of a broader transformation in the object of international legal regulation. The study suggests that international law is no longer confined to regulating digital content and user behaviour; it is increasingly turning its attention to the digital environment as a whole – including algorithmic systems and the operation of digital platforms. It concludes that safeguarding children's rights in the digital era requires a new conceptual model of international legal protection that integrates legal, technological, and institutional approaches.

Keywords: *children's rights, digital environment, international law, digital risks, international legal protection, GDPR, Digital Services Act, General Comment No. 25, digital platforms, algorithmic systems*

Copyright© 2026. The Authors. Published by Ural State Law University named after V. F. Yakovlev.
This is an open access article distributed under the CC BY-NC 4.0. license http://creativecommons.org//license/by-nc/4.0/

Vol. 9. Is. 3

ПЕРЕОСМЫСЛЕНИЕ МЕЖДУНАРОДНО-ПРАВОВОЙ МОДЕЛИ ЗАЩИТЫ ПРАВ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ: СОВРЕМЕННЫЕ ВЫЗОВЫ И НОВЫЕ ПОДХОДЫ

Ф. Л. Мируктамова
Ташкентский государственный юридический университет
ORCID ID: 0000-0002-9793-3717

Цифровая трансформация коренным образом изменила механизмы реализации и защиты прав детей, поставив под сомнение традиционные подходы к международно-правовому регулированию. В настоящей статье исследуется эволюция международно-правовой модели защиты прав детей посредством анализа современных цифровых рисков на основе универсальных и региональных международно-правовых актов, практики международных организаций и современной юридической доктрины. Обосновывается, что цифровые риски следует рассматривать не только как новые категории угроз, но и как индикаторы более глубокой трансформации объекта международно-правового регулирования. Показано, что международное право постепенно выходит за рамки регулирования цифрового контента и поведения отдельных субъектов, распространяя свое воздействие на цифровую среду как самостоятельный объект правового регулирования, включая алгоритмические системы и цифровые платформы. Сделан вывод о том, что эффективная защита прав детей в цифровую эпоху требует формирования новой концептуальной модели международно-правовой защиты, объединяющей правовые, технологические и институциональные механизмы.

Ключевые слова: *права ребенка, цифровая среда, международное право, цифровые риски, международно-правовая защита, GDPR, Закон о цифровых услугах, Замечание общего порядка № 25, цифровые платформы, алгоритмические системы*

Introduction

The rapid development of digital technologies has become one of the most significant drivers of change in contemporary international human rights law. The digital environment is no longer merely a space for exchanging information; it has evolved into an autonomous sphere in which a broad range of human rights and freedoms, including children's rights, are exercised. At the same time, digitalization has generated new forms of risk associated with the processing of personal data, the operation of algorithmic systems, the activities of digital platforms, the dissemination of unlawful content, and the use of artificial intelligence technologies. The protection of children's rights in the digital environment has, in recent years, emerged as one of the most rapidly evolving fields of international legal regulation.

These developments have prompted a gradual but steady expansion of international standard-setting in the field of children's rights, both at the universal and regional levels. The Convention on the Rights of the Child of 1989, General Comment No. 25 of the Committee on the Rights of the Child of 2021, the modernized Council of Europe Convention 108+, the General Data Protection Regulation of the European Union, the Digital Services Act, and other international and regional instruments aimed at ensuring a safe digital environment for children have significantly influenced the development of the relevant

legal framework. However, the expansion of this normative framework has also been accompanied by substantial changes in the very logic of the international legal protection of children's rights.

Despite the considerable body of scholarship devoted to children's rights in the digital environment, most existing studies focus either on individual categories of digital risk or on the content of international standards designed to address them [Livingstone, Third, Lansdown, 2020]. Far less attention has been paid to the way in which digital transformation has altered the international legal model for the protection of children's rights itself and has contributed to the emergence of new conceptual approaches to the regulation of the digital environment. Addressing this gap constitutes the central research task of the present article.

Unlike most existing studies, this article examines the international legal protection of children's rights not only through the development of international standards, but also through the transformation of the object of international legal regulation. The digital environment is increasingly becoming such an object in its own right, as it independently shapes the conditions under which children's rights are exercised [Verdoodt, 2024].

The author proceeds from the proposition that digital transformation has brought about a qualitative change in the international legal model for the protection of children's rights. As a result, the object of international legal regulation is gradually expanding beyond the conduct of States and other legal actors to encompass the digital environment itself, insofar as it determines the conditions under which children's rights are realized.

An additional dimension of this transformation is the increasing **datafication of childhood**. Children's participation in the digital environment continuously generates personal and behavioural data that may be collected, inferred, combined, and subsequently used for purposes that are not always visible or comprehensible to the child. Importantly, the legal significance of this process extends beyond conventional concerns about privacy. Datafication creates an informational architecture through which children may be profiled, categorized, and subjected to personalized digital experiences, thereby influencing the practical conditions under which a broader range of their rights are exercised. As Livingstone, Stoilova and Nandagiri demonstrate, children's data are generated not only through information they consciously disclose, but also through their digital traces and data inferred from their online activities. This makes the distinction between an individual act of disclosure and the structural processing of children's data increasingly difficult to sustain [Livingstone, Stoilova, Nandagiri, 2019].

The purpose of this study is to identify the principal patterns in the transformation of the international legal model for the protection of children's rights in the context of digitalization through an analysis of contemporary digital risks, doctrinal tensions, and emerging conceptual approaches in international law.

Contemporary threats to children's rights in the digital environment are not homogeneous in their legal nature. Whereas traditional international legal doctrine generally viewed violations of children's rights as the consequence of unlawful conduct by identifiable actors, digital transformation has generated a qualitatively new category of risks arising not only from users' actions, but also from the manner in which the digital environment itself is designed and operated. Contemporary digital risks therefore require not merely classification, but differentiation according to their underlying mechanisms, since those mechanisms determine the appropriate international legal means of protection.

Contemporary Risks to Children's Rights in the Digital Environment

The development of digital technologies has not only generated new threats to children's rights but has also fundamentally transformed the mechanisms through which such threats arise. Whereas, in the traditional social environment, violations of children's rights were generally understood as resulting from the unlawful conduct of identifiable individuals, in the digital environment a significant proportion of risks stem from the functioning of digital platforms, algorithmic systems, data-processing technologies, and other components of digital infrastructure. Consequently, international legal protection faces an entirely new challenge: violations of children's rights are increasingly caused not by isolated unlawful acts but by the structural characteristics of the digital environment itself[1].

From this perspective, digital risks in the contemporary context are far from homogeneous in their legal nature. They differ not only in content but also in the ways they arise, the actors involved, and the subject matter of international legal regulation. This suggests that analysis of digital risks should move beyond traditional classification schemes. Instead, closer attention ought to be paid to how each category of risk mirrors the broader, ongoing transformation of the international legal framework for the protection of children's rights in the digital age [Livingstone & Stoilova, 2021].

From a scholarly perspective, such an approach is of fundamental importance. Traditional classifications of digital risks primarily describe different categories of threats, yet they pay considerably less attention to the underlying mechanisms of their emergence and to the corresponding implications for international legal regulation. However, it is precisely the mechanism through which a risk arises that determines the appropriate legal means of protection. For this reason, contemporary digital risks may be understood as successive stages in the increasing complexity of threats to children's rights-from unlawful digital content and harmful interactions between users to the influence of the digital environment itself on children's development and, ultimately, to the impact of the architecture of digital platforms and algorithmic systems. Such an analytical framework makes it possible to trace the evolution of international legal protection in the digital era and to identify the principal directions of its further development[2].

Based on this approach, contemporary risks to children's rights in the digital environment may be classified according to both their mechanisms of emergence and the object of international legal regulation. Such a classification not only systematizes the existing spectrum of digital threats but also illustrates the progressive evolution of international legal responses to them. Accordingly, the following analysis examines content risks, contact risks, behavioural risks, and structural risks, each representing a distinct stage in the transformation of the international legal model for the protection of children's rights in the digital environment.

Content Risks

The first category comprises **content risks**, which arise from the dissemination of digital content capable of causing harm to a child's physical, psychological, moral, or social development. These risks include sexually explicit material, violent content, extremist and terrorist propaganda, content promoting self-harm or suicide, disinformation,

[1] Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25*, paras. 12–18.

[2] OECD, *Recommendation of the Council on Children in the Digital Environment* (OECD/LEGAL/0389, 2021); Committee on the Rights of the Child, *General Comment No. 25*, paras. 16–21.

and other forms of digital information that may adversely affect children's rights and legitimate interests. Of particular concern is online child sexual abuse material (CSAM), the transnational dissemination of which has become significantly more rapid and extensive due to the borderless nature of the Internet[3].

From an international legal perspective, content risks represent the earliest category of digital threats to receive comprehensive legal regulation. Initially, the digital environment was perceived primarily as a new medium for the dissemination of information. Consequently, international legal responses focused predominantly on restricting children's access to harmful and unlawful online content. Early international instruments therefore concentrated on the criminalization of specific forms of illegal digital content, strengthening international cooperation in combating the online sexual exploitation of children, and developing mechanisms for preventing children's exposure to harmful information[4].

In contemporary international legal doctrine, the restrictive paradigm of child protection in the digital environment is increasingly being called into question. The Committee on the Rights of the Child, in its **General Comment No. 25 (2021)**, has explicitly stated that efforts to ensure online safety must not come at the expense of disproportionate limitations on children's rights to freedom of expression, information, participation, and other fundamental guarantees enshrined in the Convention on the Rights of the Child. The proper task of international legal protection, therefore, is to strike a nuanced balance: guarding children against genuinely harmful content, while at the same time respecting their status as rights-holders in the digital realm[5].

This tension also reveals a broader conceptual problem in the traditional protective approach to children's digital rights. A regulatory model centred predominantly on shielding children from harmful information may inadvertently conceptualize the child primarily as a vulnerable object of protection rather than as an autonomous holder of rights. Such an approach is increasingly difficult to reconcile with the participatory dimension of the Convention on the Rights of the Child. Livingstone has argued that the application of children's rights to the digital environment requires protection, provision and participation to be considered together rather than treated as mutually exclusive objectives. From this perspective, the legal challenge is not simply to minimize children's exposure to digital risks, but to construct a regulatory environment in which safety measures remain compatible with children's access to information, expression, communication and meaningful participation [Livingstone, 2019].

Accordingly, the analysis of content risks demonstrates that, at this stage of legal development, **the primary object of international legal regulation is the digital content itself**. The principal responsibility of States lies in preventing children's exposure to unlawful and harmful online content through the establishment of appropriate legal prohibitions, regulatory mechanisms, and international cooperation. Nevertheless, the continuing evolution of digital technologies has demonstrated that threats to children's rights arise not only from the content they encounter but also from their interactions with other users within the digital environment. This development has, in turn, led to the recognition of a distinct category of threats, commonly referred to as **contact risks**.

[3] UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, paras. 82–87.

[4] Convention on Cybercrime, arts. 9–10; Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, arts. 18–23.

[5] UN Committee on the Rights of the Child, *General Comment No. 25 (2021),* paras. 95–99.

Contact Risks

The second group of risks is linked to contact. Unlike content-related harms, where the source of danger lies in the information itself, contact risks originate from direct digital interaction between a child and other users. These may take the form of online grooming, sexual exploitation, trafficking facilitated by digital means, extortion, coercion, or the recruitment of minors into criminal and extremist networks through communication technologies[6].

From the standpoint of international law, the growing recognition of contact risks represented a significant step forward in the evolution of child protection in the digital sphere. As social media, instant messaging, and other interactive platforms gained traction, it became increasingly clear that threats to children's rights were not limited to harmful content – they also arose from problematic interactions with other users. This realisation prompted a gradual expansion of international legal responses, extending beyond content regulation to address unlawful conduct facilitated through digital communication[7].

Within this framework, particular weight has been given to the positive obligations of States in preventing online grooming, child sexual exploitation, and other forms of abuse facilitated by technology. Contemporary approaches to child protection are no longer confined to prosecuting offenders after the fact; rather, they increasingly emphasise proactive measures. These include cross-border law enforcement cooperation, early detection systems for online threats, digital literacy programmes targeting both children and parents, and the imposition of due diligence duties on platforms to identify and respond to illegal content affecting minors [Livingstone, Stoilova, Nandagiri, 2020].

The recognition of contact risks has also brought about a notable shift in the allocation of responsibilities under international law. While the traditional framework placed the primary burden of protecting children's rights squarely on States, more recent developments have brought private actors into the picture – digital platforms, social media providers, and other online service providers are now increasingly seen as bearing a share of the responsibility for preventing rights violations. Consequently, the protection of children in the digital environment is no longer understood solely as a matter of public regulation but also as a shared responsibility involving private digital actors[8].

The growing role of private digital actors also raises a deeper question concerning the allocation of responsibility within the international human rights framework. Digital platforms do not merely transmit communications between users; through their terms of service, interface architecture, moderation systems, recommender mechanisms and commercial practices, they actively structure the environment in which children interact. This functional transformation makes it increasingly difficult to conceptualize platforms exclusively as neutral intermediaries. In the context of children's rights, their capacity to shape visibility, accessibility and patterns of interaction gives them a particular form of regulatory power over the digital environment. The resulting challenge for international law is therefore to translate the general expectation that businesses respect children's rights into more concrete duties of due diligence, risk assessment and rights-sensitive service design [Livingstone, Third, Lansdown, 2020].

Nevertheless, contact risks do not fully explain the contemporary mechanisms through which children's rights may be affected. Even in the absence of unlawful content or

[6] Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, paras. 82–90.

[7] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, arts. 18–24.

[8] Regulation (EU) 2022/2065 (Digital Services Act), arts. 28, 34–35.

direct harmful interactions, the digital environment itself is capable of shaping children's behaviour through recommender systems, personalization technologies, and other algorithmic mechanisms. This development has led to the recognition of a further category of threats – **behavioural risks**.

Behavioural Risks

The third category comprises behavioural risks, which arise from the influence of the digital environment on children's behaviour, worldview, and psychological well-being. These risks include cyberbullying, internet addiction, the recruitment of minors into harmful online communities, participation in dangerous online challenges, and the influence of algorithmically personalized content on children's identity formation. Unlike content and contact risks, the source of harm in this context is neither the information itself nor the actions of other users, but rather the manner in which children interact with the digital environment as a whole [Livingstone & Stoilova, 2021].

From the perspective of international law, behavioural risks represent a qualitatively new challenge in the evolution of child protection. Traditional legal frameworks were largely designed to address unlawful conduct by identifiable actors. The digital environment, however, has revealed that serious harm can occur even in the absence of formally unlawful behaviour. Recommendation algorithms, personalisation technologies, gamification, and user-engagement systems may exert a continuous and subtle influence on children's development – shaping their behaviour, social interactions, and decision-making in ways that are not easily captured by conventional legal categories[9].

This shift has expanded the scope of international legal protection well beyond the traditional notion of child safety. The concern is no longer confined to preventing discrete violations of children's rights; it increasingly extends to shaping the conditions that enable healthy development in digital spaces. In this connection, Article 6 of the **Convention on the Rights of the Child** – which guarantees every child's right to life, survival, and development – acquires a renewed relevance. In the digital age, this provision calls for an evolutionary reading, one that takes into account the profound influence of digital technologies on children's personal growth[10].

Behavioural influence in the digital environment also has an important **commercial dimension**. Many digital services operate through business models that seek to maximize attention, engagement and the generation of user data. For children, the implications of such models are particularly significant because persuasive design, personalization and commercial profiling may exploit developmental vulnerabilities without necessarily involving conduct that would traditionally be characterized as unlawful. The distinction between ordinary commercial persuasion and interference with children's rights therefore becomes increasingly difficult to maintain where digital architectures are deliberately designed to influence behaviour. Van der Hof and her co-authors demonstrate that the commercialization of children's digital participation raises questions not only of data protection and consumer law but also of the child's right to protection from economic exploitation. This perspective broadens the legal analysis from individual harmful practices to the economic structures underlying the digital environment itself [Van der Hof, et al., 2020].

The analysis of behavioural risks thus reveals a further expansion in the object of international legal protection. Content risks centre on the regulation of digital information;

[9] UNICEF. *Policy Guidance on AI for Children.* 2021; Committee on the Rights of the Child, *General Comment No. 25 (2021)*, paras. 67–76.

[10] Convention on the Rights of the Child, art. 6; Committee on the Rights of the Child, *General Comment No. 25 (2021)*, paras. 13–18.

contact risks concern interactions between users. Behavioural risks, by contrast, require international law to go a step further – addressing the very impact that the digital environment itself has on children's development. Nevertheless, even this approach does not fully explain the origins of contemporary digital threats, as many of them are embedded in the design and operation of digital platforms and algorithmic systems. This, in turn, necessitates consideration of the most complex category of contemporary threats – **structural risks**.

Structural Risks

The most complex and conceptually advanced category of contemporary digital threats is constituted by **structural risks**, which arise from the inherent characteristics of the digital environment itself. Their defining feature is that violations of children's rights do not result from unlawful content or the misconduct of individual users, but rather from the operation of algorithms, digital platforms, data-processing mechanisms, and artificial intelligence systems. In this context, the architecture of the digital environment itself becomes a potential source of harm, shaping the conditions under which children's rights are exercised[11].

From the perspective of international law, structural risks most clearly expose the limitations of the traditional model of children's rights protection. Classical international law has generally proceeded on the assumption that human rights violations are attributable to the unlawful conduct of States or other identifiable legal actors. The digital transformation, however, demonstrates that many contemporary threats arise independently of any specific unlawful act. Algorithmic profiling of children, continuous collection and commercial exploitation of personal data, recommender systems designed to maximize user engagement, and automated decision-making systems may significantly affect the enjoyment of children's rights even where the operation of such technologies formally complies with applicable legal requirements [Zuboff, 2019].

This development also demonstrates why **data protection alone cannot provide a complete legal response to structural digital risks**. Privacy rules traditionally concentrate on the collection and processing of personal data, whereas algorithmically mediated environments may affect children even where individual processing operations formally satisfy applicable requirements. Nissenbaum's theory of contextual integrity is particularly useful in explaining this problem: privacy is not simply a question of secrecy or individual control over information, but also concerns whether information flows are appropriate to the social context in which they occur. Applied to children's digital rights, this suggests that legal analysis should examine not only whether data processing is formally lawful, but also whether the resulting informational relationships, profiling practices and algorithmic decisions are compatible with the child's status, developmental needs and legitimate expectations within a particular digital context [Nissenbaum, 2010].

These developments have given rise to a new direction in international legal regulation that extends beyond preventing individual rights violations and seeks to establish legal requirements for the design and governance of digital services themselves. This approach has found its way into European Union law, notably through provisions on systemic risk assessment, safety by design, and the expanded responsibilities of digital service providers in relation to algorithmic systems that affect children. The regulatory focus of international law is thus gradually moving beyond the conduct of States, private actors, and individual

[11] Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, paras. 70–79.

users – extending to the very architecture of the digital environment, which is now seen as an independent variable in the realisation of children's rights[12].

What emerges from the analysis of structural risks is a profound transformation of the international legal model for the protection of children's rights. The trajectory is clear: international law began with the regulation of digital content, then broadened to address the conduct of participants in digital interactions, and later extended to the influence of the digital environment on children's development. Today, it is increasingly concerned with the digital infrastructure itself. This evolution represents one of the most significant shifts in contemporary international children's rights law and provides the conceptual backdrop for the doctrinal tensions explored in the following section.

Taken together, these developments point towards a transition from a predominantly **reactive model of legal protection to an anticipatory model of digital governance**. Traditional mechanisms of human rights protection generally operate after a violation has occurred or after an identifiable risk has materialized. Yet structural digital risks may be embedded in technological systems long before harm becomes visible at the individual level. Consequently, effective protection of children's rights increasingly requires ex ante mechanisms capable of evaluating the potential impact of digital products and services during their design and deployment. Recent scholarship on Child Rights Impact Assessment illustrates this emerging approach by seeking to integrate the Convention on the Rights of the Child into technological decision-making before adverse consequences materialize. Such mechanisms indicate a broader normative shift: the protection of children's rights is gradually becoming a requirement governing the architecture and development of digital systems themselves rather than merely a remedial response to individual violations [Livingstone, Pothong, 2025].

Conclusion

The findings of this study point to a fundamental reshaping of the international legal model for children's rights protection, driven by digital transformation. Contemporary digital risks are distinguished not only by their nature but also by the mechanisms through which they arise – which calls for a rethinking of traditional regulatory approaches. The proposed typology of content, contact, behavioural, and structural risks illustrates a progressive expansion of the regulatory object: from digital content and individual conduct, to the architecture of the digital environment itself.

The study also points to a further development: the expanding regulatory scope has given rise to new doctrinal tensions. Balancing child protection against children's participation rights, and reconciling privacy concerns with the imperatives of a data-driven digital economy, has become increasingly difficult. These tensions suggest that traditional legal frameworks are no longer adequate for striking a proper balance between competing rights and interests in the digital age.

The transformation of the regulatory object therefore calls for a new conceptual framework – one that is capable of integrating legal, technological, and institutional mechanisms for the protection of children's rights. Future international legal regulation should therefore focus not only on preventing individual violations of children's rights but also on establishing normative requirements governing the design, operation, and accountability of digital platforms, algorithmic systems, and artificial intelligence technologies.

[12] Regulation (EU) 2022/2065 (Digital Services Act), arts. 34–35; Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 28–38

The study supports the proposition that digital transformation has qualitatively altered the international legal model for the protection of children's rights. As a consequence, the object of international legal regulation is gradually expanding beyond the conduct of States, private actors, and individual users to encompass the digital environment itself as an autonomous factor determining the effective realization of children's rights. It is this transformation that is likely to shape the future evolution of international legal mechanisms for the protection of children's rights in the digital era.

References

Livingstone, S. & Pothong, K. (2025) Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment. *Policy & Internet*, (17), e70008, DOI: 10.1002/poi3.70008.

Livingstone, S. & Stoilova, M. (2021) *The 4Cs: Classifying Online Risk to Children. CO:RE Short Report Series on Key Topics*. Hamburg, Leibniz-Institut für Medienforschung, Hans-Bredow-Institut (HBI), CO:RE – Children Online: Research and Evidence, 15, DOI: 10.21241/ssoar.71817.

Livingstone, S. & Stoilova, M. & Nandagiri, R. (2020) Data and Privacy Literacy: The Role of the School in Educating Children in a Datafied Society. Frau Meigs D., et al. (eds.) *The Handbook of Media Education Research*. Hoboken, NJ, Wiley Blackwell, 413–425, DOI: 10.1002/9781119166900.ch38.

Livingstone, S. & Stoilova, M. & Nandagiri, R. (2019) *Children's Data and Privacy Online: Growing Up in a Digital Age. An Evidence Review*. London, London School of Economics and Political Science, 57.

Livingstone, S. & Third, A. & Lansdown, G. (2020) Children's Rights in the Digital Environment: A Challenging Terrain for Evidence Based Policy. Green L., et al. (eds.) The Routledge Companion to Digital Media and Children. London, Routledge, 378–389, DOI: 10.4324/9781351004107-36

Livingstone, S. (2019) Claiming Rights and Righting Wrongs: Children's Rights in the Digital Environment. *Exploring Key Issues in Early Childhood and Technology: Evolving Perspectives and Innovative Approaches*. New York, Routledge, 42–48, DOI: 10.4324/9780429457425-8.

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Stanford University Press, 288.

Van der Hof, S., et al. (2020) The Child's Right to Protection against Economic Exploitation in the Digital World. *The International Journal of Children's Rights*, 28 (4), 833–859, DOI: 10.1163/15718182-28040003.

Verdoodt, V. (2024) Children's Rights in the Digital Environment. Lievens E., Verschaeve S., Vander Maelen C. (eds.) *An Introduction to Law & Technology*, 3rd ed. Ghent, Owl Press Legal, 137–155.

Zuboff, S. (2019) *The Age of Surveillance Capitalism*. New York, Public Affairs, 704.

Библиографический список

Livingstone S. Claiming Rights and Righting Wrongs: Children's Rights in the Digital Environment // Exploring Key Issues in Early Childhood and Technology: Evolving Perspectives and Innovative Approaches. – N. Y.: Routledge, 2019. – P. 42–48. – DOI: 10.4324/9780429457425-8.

Livingstone S., Pothong K. Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment // Policy & Internet. – 2025. Vol. 17. – e70008. – DOI: 10.1002/poi3.70008.

Livingstone S., Stoilova M. The 4Cs: Classifying Online Risk to Children. CO:RE Short Report Series on Key Topics. Hamburg: Leibniz-Institut für Medienforschung; Hans-Bredow-Institut (HBI); CO:RE – Children Online: Research and Evidence, 2021. – 15 p. – DOI: 10.21241/ssoar.71817.

Livingstone S., Stoilova M., Nandagiri R. Children's Data and Privacy Online: Growing Up in a Digital Age. An Evidence Review. – L.: London School of Economics and Political Science, 2019. – 57 p.

Livingstone S., Stoilova M., Nandagiri R. Data and Privacy Literacy: The Role of the School in Educating Children in a Datafied Society // The Handbook of Media Education Research / ed. by D. Frau-Meigs, et al. – Hoboken, NJ: Wiley-Blackwell, 2020. – P. 413–425. – DOI: 10.1002/9781119166900.ch38.

Livingstone S., Third A., Lansdown G. Children's Rights in the Digital Environment: A Challenging Terrain for Evidence Based Policy // The Routledge Companion to Digital Media and Children / ed. by L. Green, et al. – L.: Routledge, 2020. – P. 378–389. – DOI: 10.4324/9781351004107-36.

Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. – Stanford: Stanford University Press, 2010. – 288 p.

The Child's Right to Protection against Economic Exploitation in the Digital World / S. Van der Hof [et al.] // The International Journal of Children's Rights. – 2020. – Vol. 28. – № 4. – P. 833–859. – DOI: 10.1163/15718182-28040003.

Verdoodt V. Children's Rights in the Digital Environment // An Introduction to Law & Technology / ed. by E. Lievens, S. Verschaeve, C. Vander Maelen. – 3rd ed. – Ghent: Owl Press Legal, 2024. – P. 137–155.

Zuboff S. The Age of Surveillance Capitalism. – N. Y.: Public Affairs, 2019. – 704 p.

Information about the author

Feruza L. Miruktamova – PhD in Law, Associate Professor of the Tashkent State University of Law (e-mail: miruktamovaf@gmail.com).

Информация об авторе

Феруза Лутфуллаевна Мируктамова – доктор философии по юридическим наукам (PhD), доцент Ташкентского государственного юридического университета (e-mail: miruktamovaf@gmail.com).

© Ф. Л. Мируктамова, 2026

Дата поступления в редакцию / Received: 15.07.2026
Дата принятия решения об опубликовании / Accepted: 06.08.2026