

Legal Protection of Children's Privacy Rights from Global EdTech Governance Oversight

Putu Fairnanda Sastra Devi^{1*}, Dewa Gede Sudika Mangku², Ni Putu Rai Yuliantini³

^{1,2,3}Law, Faculty of Law and Social Science, Universitas Pendidikan Ganesha, Bali, Indonesia

ABSTRAK

Pergeseran masif padateknologi pendidikan (EdTech) telah mengungkap kerentanan dalam eksploitasi sistematis terhadap data anak. Laporan Human Rights Watch tahun 2022 mengungkapkan bahwa 89% produk EdTech yang dianalisis melakukan praktik data yang berisiko atau melanggar hak-hak anak. Penelitian ini mengkaji celah hukum antara prinsip "The Best Interests of the Child" dengan realitas komersial penambangan data lintas batas. Menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, studi ini menganalisis instrumen internasional saat ini, seperti Konvensi PBB tentang Hak Anak, dalam menangani pengawasan digital modern. Temuan penelitian menunjukkan penerapan prinsip the best interests of the child dalam tata kelola EdTech global belum optimal, menciptakan kekosongan tata kelola di mana platform global beroperasi di luar yurisdiksi nasional, menyebabkan anak-anak di negara berkembang tidak terlindungi secara memadai. Artikel ini mendesak perlunya kerangka kerja internasional yang mengikat yang mewajibkan akuntabilitas algoritma yang ketat dan mekanisme penegakan hukum lintas batas. Dengan menyelaraskan kebijakan dan hukum global, komunitas internasional dapat menumbuhkan ekosistem pendidikan digital yang tangguh dan inklusif yang memprioritaskan hak asasi manusia di atas kepentingan komersial.

Kata Kunci: Privasi Digital, EdTech, Hukum Internasional, Hak Anak, Tata Kelola Data

ABSTRACT

The massive shift to education technology (EdTech) has exposed a critical vulnerability in international law: the systematic exploitation of children's data. A 2022 Human Rights Watch report revealed that 89% of analyses EdTech products engage in data practices that risk or violate children's rights, yet international law enforcement remains weak. This research examines the legal gap between the principle of "The Best Interests of the Child" and the commercial reality of cross-border data mining. Using normative legal methods with a statutory approach, the study analyses the inadequacy of current international instruments, such as the UN Convention on the Rights of the Child, in addressing modern digital surveillance. The findings suggest a "governance vacuum" where global platforms transcend national jurisdictions, leaving children in developing countries inadequately protected. This article urges the need for a binding international framework that mandates rigorous algorithmic accountability and cross-border enforcement mechanisms. By aligning global policies and laws, the international community can foster a resilient and inclusive digital education ecosystem that prioritizes human rights over commercial interests.

Keywords: Digital Privacy, EdTech, International Law, Children's Rights, Data Governance

1. INTRODUCTION

The massive global development of education technology in recent years has exposed deep systemic vulnerabilities related to the exploitation of children's data. The transformation driven by technological developments has migrated physical classrooms into digital ecosystems dominated by commercial interests and sophisticated surveillance mechanisms. A 2022 Human Rights Watch (HRW) report revealed that 89% of the EdTech products analyzed engaged in data practices that risked or directly violated children's fundamental rights. This phenomenon creates an acute legal tension between the fundamental principle of international law, namely "The Best Interests of the Child," and the economic realities of aggressive cross-border data mining.

*Corresponding author

E-mail addresses: fairnanda@student.undiksha.ac.id

These human rights are fundamental in that their implementation is absolutely necessary for human development in accordance with their talents, aspirations, and dignity as human beings, regardless of differences that lead to discrimination based on nationality, race, religion, and gender (Mangku D.G.S., 2021: 4). Moreover, human rights in this digital era are not always accompanied by adequate protection for children's privacy rights and personal data security. A Human Rights Watch report revealed that the majority of educational apps used by children in various countries collect massive amounts of personal data without transparency or adequate protection mechanisms, potentially exposing children to the risk of tracking, profiling, and data misuse for commercial or manipulative purposes (Human Rights Watch, 2022). These findings indicate that the digitalization of education, which should facilitate learning, is instead creating new threats to children's privacy, particularly when data is collected by third parties without explicit consent.

Furthermore, in addition to privacy aspects, issues arise regarding the governance of children's data on EdTech platforms. Data collection in schools and EdTech is subject to a weak governance framework, with education authorities and technology providers often lacking a full understanding of the legal implications of processing children's data, particularly regarding who controls the data and how it is used (Emma.etc., 2022). UNICEF also emphasized that data governance arrangements in EdTech must be structured with precautionary principles, transparent audits, and access control mechanisms to prevent misuse that could harm children in the future (UNICEF, 2021). This demonstrates the unpreparedness of educational institutions to manage digital data ethically and in accordance with child rights protection standards.

The growth of the global EdTech market should not be viewed solely as a pedagogical advancement, but rather as an extension of what has been termed "surveillance capitalism" into educational institutions (Lavi.M, 2024). The EdTech market is estimated to reach US\$142.37 billion by 2023, with a projected fourfold increase due to the increasingly massive integration of artificial intelligence (AI) (UNICEF, 2025). However, this economic growth is accompanied by data collection practices that go beyond functional educational needs.

General Comment No. 25 of the UN Committee on the Rights of the Child emphasizes that states have an obligation to ensure a safe digital environment for children, including ensuring that technology used in schools, educational apps, and online platforms comply with child rights principles such as non-discrimination, the best interests of the child, the right to be heard, and protection from exploitation (UNCRC, 2021). This document also underscores that every digital actor – whether states, companies, or educational institutions – has a shared responsibility to maintain a balance between the use of technology and the protection of children's rights. In other words, technological development must not compromise the best interests of children as a primary principle.

Another risk arises from the use of algorithms and artificial intelligence (AI) on digital platforms that interact with children. A legal analysis from American University shows that recommendation algorithms can target children with age-inappropriate content or even endanger their mental health and safety if there are no control and oversight mechanisms (Lavi.M, 2024). Another study from the CSA Group adds that the use of AI in children's lives has the potential to violate privacy rights if AI systems are not designed with the principles of security, transparency, auditability, and bias prevention. Thus, the development of AI has a significant impact on shaping children's digital behavior and safety, necessitating a more comprehensive regulatory approach.

In addition to technological threats, cross-border data transfer is a critical issue because children's data collected by digital platforms can be sent to other countries without adequate legal protection. The 2023 Global Cross-Border Privacy Rules (CBPR) framework explains that the international data transfer system still has significant gaps, particularly in protecting the data of vulnerable groups such as children (Global CBPR). Atlantis Press also highlights that international regulations regarding data transfers are sometimes overlapping and unsynchronized, posing challenges to enforcing child data protection globally. Meanwhile, global regulatory bodies are showing an increasing focus on enforcing laws regarding children's digital data protection, as evidenced by simultaneous inspections by international privacy regulators of platforms processing children's data (Insivide Privacy, 2024).

Previous research has addressed various aspects related to data protection and children's privacy in the digital age. First, a study by Widyaningsih et al. examined the legal framework for protecting children's digital personal data in Indonesia, identifying weaknesses in national regulations

in anticipating child privacy violations resulting from the widespread use of digital technology. Second, a study by Sofian and Pratama evaluated online privacy regulations for children in Indonesia, showing that although national laws regulate digital privacy, weaknesses remain in the implementation and effectiveness of protecting children's data online (Media Informasi, 2025). Third, a technical study by Sun et al. focused on privacy practices in children's apps in app stores by measuring permission requests and tracker usage, revealing high levels of irrelevant data access without legal review of its long-term effects.

This study differs from these three studies because it goes beyond evaluating national laws and normatively assesses the effectiveness of international legal instruments, particularly the Best Interests of the Child principle and General Comment No. 25, and examines how these instruments are implemented or experience governance gaps in global EdTech governance, which operates across jurisdictions. The above conditions indicate a significant regulatory gap in international law regarding the protection of children's personal data.

Many regulatory instruments still focus on adult privacy and do not specifically address children's needs in the digital environment. This is exacerbated by regulatory inconsistencies across countries and weak oversight of technology companies. While General Comment No. 25 provides direction, its implementation varies widely across countries and often lacks robust enforcement mechanisms. Therefore, there is an urgent need to more systematically analyze child data protection within the context of international law. This research thus contributes to a new understanding of the need for a binding international legal framework for algorithmic accountability, cross-border oversight, and comprehensive child privacy protection in the EdTech ecosystem.

2. METHOD

The research method used is normative legal research, which aims to provide legal arguments in dealing with the emptiness, ambiguity, or conflict of legal norms, so as to be able to emphasize the critical aspects of legal science as a sui generis normative science (Diantha, 2017:12). This research uses a conceptual and legislative approach, where data sources are collected through library research from primary legal sources in the form of relevant international laws and regulations, secondary legal sources in the form of scientific articles, journals, books, and related research documents, as well as tertiary legal sources such as encyclopedias, legal commentaries, and publications of international institutions. The collected data are then analyzed qualitatively, by reviewing, comparing, and interpreting legal norms and supporting literature to answer the research problem formulation. This research uses Alan Westin's privacy rights theory which views privacy as an individual's control over the use and dissemination of his personal data, making it relevant to assessing data collection practices by EdTech providers.

3. RESULT AND DISCUSSION

Child Privacy Protection in Edtech Regulated at the International Level

Protecting children's privacy in education technology (EdTech) is a pressing human rights issue because the rapid digitalization of education is increasing the collection, storage, and processing of children's personal data without effective and comprehensive legal governance. Children's personal data, including names, addresses, photos, interaction behavior, and learning data generated by EdTech platforms, is often processed to personalize services but also used for commercial purposes without adequate consent, potentially threatening children's rights to privacy and autonomy (UNICEF, 2025).

EdTech platforms such as Google Workspace for Education raise concerns about data collection practices that encompass not only learning activities but also behavioral data. This demonstrates that while regulations like the GDPR in Europe are robust, stronger enforcement is still needed to ensure effective child protection in digital education (Fernandez.L, 2025). Governance of children's data in digital education remains highly fragmented. A UNICEF report states that only around 16% of countries have specific laws related to protecting children's data privacy in education, while most countries only rely on general data protection laws that do not specifically regulate the EdTech sector (UNICEF, 2025). This indicates that international and national legal instruments are not yet fully developed to address EdTech's challenges to children's privacy, even though international human rights principles, such as the United Nations Convention on the Rights of the Child (UNCRC), emphasize the right to privacy as part of children's rights in general.

International law itself has created a framework and pattern of international relations agreed upon by the international community, accommodating the interests of its members (Mangku D.G.S., 2021). A national legal study of Indonesia also highlighted the lack of specific legal protection for children's personal data in the digital realm. High internet penetration among children increases the risk of privacy violations because their personal data, including addresses and telephone numbers, is often shared without adequate legal controls (Widyarningsih, 2025). Other research also shows that although Law Number 27 of 2022 concerning Personal Data Protection establishes basic principles of the right to privacy, there remains a normative gap regarding specific implementation mechanisms for children in EdTech services, resulting in a high potential for data misuse (Andiani, 2025).

Every individual has fundamental rights that must not be violated, including the right to dignity, privacy, and protection from arbitrary intervention (Mangku D.G.S., 2021). Universal human rights principles are applied to the issue of children's privacy in EdTech because they concern the protection of vulnerable groups from abuse of power or domination by others. This principle demonstrates that the right to privacy is not merely an additional facility, but an integral part of the human rights inherent in every individual, especially children. By understanding the universality of human rights, the issue of child privacy violations in EdTech can be viewed as a serious violation, not simply a technical omission. Other risks emerging in international literature include non-transparent data collection practices and the lack of clear consent from children or parents. A comparative study of EdTech systems across countries revealed that young digital users often lack adequate control over their data, particularly on platforms using artificial intelligence (Shrestha et al., 2024). This aligns with UNICEF's recommendations on the importance of privacy-by-design and privacy-by-default principles in EdTech to provide the highest level of protection for children from the beginning of technology development.

Children are a vulnerable group, and therefore legal protection for vulnerable groups must be viewed as a state effort to achieve substantive justice, not merely normative justice (Mangku D.G.S., 2022). States must not only establish formal regulations but must ensure implementation that effectively protects vulnerable groups. This is certainly relevant when applied to the issue of child data privacy in EdTech, as children occupy a legally, socially, and digitally vulnerable position. The state must be actively involved in ensuring that EdTech platforms do not exploit children's vulnerabilities for commercial gain.

From a national legal child protection perspective, children's personal data is information inherent in their identity, including their names, photos, videos, and creative expressions. If shared without protection, it can lead to various forms of rights violations, such as exploitation and unauthorized distribution. This highlights the urgency of establishing legal mechanisms that not only protect data but also respect the right to privacy as part of a child's dignity and development. The state's obligation to protect children's rights is fundamentally characterized as a positive obligation, namely the obligation to prevent, protect, and remedy any form of violation against children as vulnerable subjects. This principle demonstrates that the state must provide comprehensive protection mechanisms when children's rights are threatened. This principle applies not only to the context of sexual violence but also to other situations that have the potential to harm children, including the use of educational technology that processes their personal data (Mangku D.G.S., 2023).

Furthermore, international norms will not be effective without being internalized into national policies (Mangku D.G.S., 2022). This implementation principle requires countries to align EdTech policies with international obligations stipulated in the CRC, particularly regarding the right to privacy. Therefore, failure to establish a mechanism for monitoring child privacy in the EdTech sector could be seen as a state's negligence in fulfilling its international obligations.

In the European Union, the GDPR is a frequently referenced standard for child data protection in digital education, with an emphasis on parental consent and transparency principles. Meanwhile, in Indonesia, recent initiatives such as Government Regulation Number 17 of 2025 (PP TUNAS) emphasize the need for safe digital space governance for children, including age control features and parental consent in the implementation of electronic systems, which is a policy response to contemporary digital challenges (Kemen PPPA & Komdigi, 2025). Children's privacy in EdTech must be seen as an integral part of the overall human rights of children, which must be fulfilled by the state and technology service providers. Therefore, there remains a gap between ideal legal principles and the reality of implementation on the ground, particularly in law enforcement and oversight of child data

management practices. Thus, specific international legal standards for EdTech, effective oversight mechanisms involving data protection authorities, and increased digital literacy of children and parents are needed to ensure that children's privacy is truly protected in the global digital education ecosystem.

The Principle of Best Interests of the Child and Protection of Children's Privacy in the EdTech Ecosystem

The principle of the Best Interests of the Child is one of the fundamental principles in international human rights law concerning children. This principle is most explicitly stated in Article 3(1) of the United Nations Convention on the Rights of the Child (UNCRC), which affirms that in all actions related to children, whether undertaken by social institutions, administrative authorities, legislative bodies, or courts (UNICEF, n.d.), the best interests of the child must be the primary consideration. This principle is not only an ethical norm but also an interpretive legal principle that guides all interpretations of other children's rights, such as the right to privacy and data protection.

Since the convention's adoption in 1989, the development of digital technology has brought new challenges beyond the context in which it was originally formulated. The UN Committee on the Rights of the Child, through several General Comments (including No. 14 and most recently No. 25), has expanded the implementation of the Best Interests principle to the modern digital realm. In General Comment No. 25 on children's rights in the digital environment, the Committee affirmed that children's rights enshrined in the UNCRC, including the right to privacy (Article 16), apply fully in the digital environment, and that threats to children's privacy can arise from data collection, profiling, automated processing, and mass surveillance practices that are increasingly prevalent in digital products.

The Best Interests of the Child principle must be the foundation of global digital policy, as the risk of tracking and profiling of children in the digital space continues to increase, particularly on online education platforms that integrate data analytics systems (Livingstone et al. 2023). Without the implementation of this principle, child protection regulations in the digital space will be ineffective. It serves as the basis for a clear legal framework under which any educational technology affecting children must be designed, regulated, and monitored with full consideration of its impact on children. The Best Interests principle needs to be integrated into public policy and digital industry practices related to children to achieve a balance between the benefits of technology and child protection. A rights-based approach is needed, including taking into account children's evolving capacities, so that countries and industry players do not only assess technology from a pedagogical perspective but also from the perspective of its impact on children's privacy, security, and psychosocial development (UNICEF, 2025).

The principle of the Best Interests of the Child must be placed within a comprehensive framework of human rights protection. Human rights protection at the international level is not merely declarative but creates substantive legal obligations for states through ratified international treaties (Mangku, 2022). This interpretation clarifies that the principle of the best interests of the child does not stand alone but is embedded within a comprehensive set of human rights norms, including the right to privacy and the protection of personal data in the digital environment. Therefore, states cannot ignore the risk of misuse of children's data by digital platforms, including the increasingly widespread use of EdTech services.

Furthermore, General Comment No. 25 clarifies that the principle of Best Interests serves not only as an ethical guideline but also as a positive legal obligation that States Parties to the UNCRC must implement through legislation, policies, and enforcement mechanisms. The Committee states that states are obliged to formulate and implement comprehensive data protection laws that include specific protections for children, and to ensure that digital practices that could threaten privacy, such as commercial profiling and targeted advertising, are prohibited or strictly limited. In relation to educational technology, this means that countries must require technology companies to integrate privacy principles from the design stage (privacy by design) and provide children with the right to access, change, or delete their data and obtain legal remediation for any violations (Ayelaw et al., 2024).

More specifically, the Best Interests principle also requires a Child Rights Impact Assessment (CRIA) before implementing technology that has the potential to significantly impact children's lives. A CRIA is a procedural tool proposed in General Comment No. 14 and revived in No. 25, which requires policymakers and digital service providers to evaluate the positive and negative impacts of digital

technology on children's rights, including on children's privacy, security, and well-being. Without such an assessment, educational technology risks prioritizing efficiency, commercial gain, or technological functionality over the protection of fundamental children's rights.

The Best Interests principle also has implications for the concept of children's participation in digital policymaking. General Comment No. 25 emphasizes that children should have a reasonable say in policies that affect them, including in the design and governance of digital technology. Countries are expected to provide training opportunities and access to digital education for children, parents, and educators on children's digital rights, so that children can express their views on the technology they use. This is relevant in the context of EdTech, where technical decisions about data collection and processing are often made without children's involvement or transparent parental oversight. Although many countries have adopted data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), which provides robust protection for children's data, international instruments still lack legally binding global standards. General Comment No. 25 itself is an interpretive guideline, not a new, independently binding treaty. Therefore, its effective implementation depends heavily on the commitment and capacity of individual countries, as well as collaborative efforts between regulatory bodies across jurisdictions. This poses a significant challenge in the global EdTech ecosystem, where digital platforms operate across borders and often process children's data beyond the reach of national law enforcement (Ayelaw et al., 2024).

To address these challenges, the Best Interests principle has been used as a basis for strengthening the protection of children's privacy rights in various international forums, including policy recommendations and multi-stakeholder forums involving states, international organizations, and the private sector. In some jurisdictions, this principle has encouraged the development of more specific laws regarding child data protection, as well as the establishment of independent oversight bodies that proactively oversee digital practices and ensure that children's rights are not compromised for commercial or operational purposes.

Therefore, the Best Interests of the Child principle has evolved into a substantive, procedural, and interpretive legal obligation that must be considered in the regulation and use of digital technologies, including EdTech. Implementing this principle requires states to develop, enforce, and oversee comprehensive data protection and privacy policies that take into account the impact on children and encourage children's participation in matters affecting their rights in the digital world.

4. CONCLUSION

Protection of children's privacy rights in the education technology (EdTech) ecosystem remains far from adequate, even though the international legal framework, particularly the Convention on the Rights of the Child (CRC), has clearly placed the principle of the Best Interests of the Child (BIC) as a primary consideration in all actions concerning children. The provisions of Article 3 and Article 16 of the CRC, as reinforced by General Comment No. 14 and General Comment No. 25, have obligated states to ensure that digital data collection practices do not harm or exploit children. The international community needs to shift from a model of self-regulation of EdTech to a coordinated, collective oversight system oriented towards children's rights. Efforts to shape global policy are an urgent step towards creating a digital education ecosystem that is safe, inclusive, and respects children's human rights above the commercial interests of technology industry players.

5. ACKNOWLEDGE

The author expresses his deepest appreciation and gratitude to Ganesha University of Education, especially the Faculty of Law and Social Sciences and to Prof. Dr. Dewa Gede Sudika Mangku, S.H., LL.M., and Mrs. Dr. Ni Putu Rai Yuliantini, S.H., M.H., for their academic guidance and scientific input in directing the strengthening of the concepts of international law, human rights and child protection.

6. REFERENCES

Aziz, H., Rahmaddani, I., & Kuntadi, K. (2022). Child Perpetrators of Drug Crimes: Legal Protections and Effectiveness. *Lex Publica*, 5(1), 34–49.

- Basu, T. (2023). Children's Data and Algorithmic Profiling: A Global Governance Gap. *Journal of Digital Law & Ethics*, 8(2), 55–78.
- Cohen, J. (2021). Digital Rights and the Child's Best Interests Principle. *Harvard Human Rights Journal*, 34(1), 14–32.
- CSA Group. (2023). *Children's Privacy in the Age of Artificial Intelligence*. CSA Publishing.
- Docherty, L. (2022). Targeting Children: Liability for Algorithmic Recommendations. *American University Washington College of Law*.
- Febriyani, K. A. D., Yuliantini, N. P. R., & Mangku, D. G. S. (2023). Perlindungan hukum terkait pelaksanaan visum et repertum bagi anak dan perempuan korban kekerasan seksual. *Jurnal Gender dan Hak Asasi Manusia*, 4(1), 12–25.
- Global Cross-Border Privacy Rules (CBPR) Framework. (2023). CBPR Secretariat.
- Global Privacy Regulators Enforcement Sweep. (2024). International Privacy Regulators Association.
- Human Rights Watch. (2022). *How Dare They Peep into My Private Life? Children's Rights and Privacy in Education Technology*. HRW Publishing.
- Kurniawan, K. D., Hehanussa, D. J. A., & Setiawan, R. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. *Lex Publica Journal*, 6(2), 88–104.
- Livingstone, S., Byrne, J., & Burton, P. (2022). *Children's Privacy Online: Global Governance Challenges*. UNICEF Research Briefs.
- Mangku, D. G. S. (2021). Legal Protection for Women and Children with Disabilities in Indonesia. *Jurnal Magister Hukum Udayana*, 10(1), 4–5.
- Mangku, D. G. S. (2021). Pemenuhan hak asasi manusia terhadap etnis Rohingya dalam perspektif hukum internasional. *Perspektif Hukum*, 21(1), 30–45.
- Mangku, D. G. S. (2022). Legal Protection for People with Disabilities in Indonesia in the Perspective of Justice Theory. *Unnes Law Journal*, 8(2), 248.
- Mangku, D. G. S., Ardana, I. K. A., & Sugiarta, I. W. (2022). Implementation of international law and the role of Indonesia. *Jurnal Komunikasi Hukum*, 8(2), 772–784.
- Mangku, D. G. S., Yuliantini, N. P. R., & Lasmawan, I. W. (2022). Legal protection for people with disabilities in Indonesia in the perspective of justice theory. *Unnes Law Journal*, 8(2), 134–148.
- OECD. (2023). *Education in the Digital Age: Privacy and Child Data Governance*. OECD Publishing.
- Sofian, A., & Pratama, B. (2025). Perlindungan Data Privasi Anak Online dalam Mencegah Pelanggaran Hak Anak. *Media Informasi Penelitian Kesejahteraan Sosial*.
- Sun, R., et al. (2023). Not Seen, Not Heard in the Digital World! Measuring Privacy Practices in Children's Apps. Preprint Manuscript.
- UNCRC. (2021). General Comment No. 25 on Children's Rights in the Digital Environment. United Nations Committee on the Rights of the Child.
- UNICEF. (2021). *Data Governance for EdTech: Policy Recommendations*. UNICEF Publishing.

UNICEF Innocenti. (2025). Data Governance Education Technology Policy Recommendations. UNICEF Innocenti Office of Research.

Widyaningsih, T., & Suryaningsi. (2022). Kajian Perlindungan Hukum Terhadap Data Pribadi Digital Anak Sebagai Hak Atas Privasi di Indonesia. *Nomos: Jurnal Penelitian Ilmu Hukum*, 1(5).

Williamson, B., & Kizilcec, R. (2021). Who Controls Children's Education Data? *Taylor & Francis Online Journal*.