

Protecting Children's Rights in Indonesia's Digital Landscape: Between Innovation and Legal Safeguards

Rizki Adi Pinandito^{1*}, Hartiwiningsih² and Muhammad Rustamaji³

¹ Faculty of Law, Universitas Sebelas Maret (UNS), Surakarta, Indonesia

² Faculty of Law, Universitas Sebelas Maret (UNS), Surakarta, Indonesia

³ Faculty of Law, Universitas Sebelas Maret (UNS), Surakarta, Indonesia

*E-mail: rizkyadipinandito@student.uns.ac.id

Abstract. The rapid growth of digital technology in Indonesia has reshaped the way children interact, learn, and socialize, but it has also introduced serious risks such as cyberbullying, online exploitation, and data privacy violations. This research aims to analyze the adequacy of Indonesia's legal framework in protecting children's rights in digital spaces and to explore ways of integrating such protection into digital governance without hampering technological progress. Employing a normative juridical (doctrinal) approach, the study examines national legislation in light of international human rights standards such as the Convention on the Rights of the Child, General Comment No. 25, the GDPR, and the Age-Appropriate Design Code. The findings indicate that Indonesia's regulations are still predominantly system- and innovation-focused, leaving significant legal gaps in addressing child-specific digital risks. To overcome these shortcomings, the study recommends integrating the best interests of the child into all digital policies through child impact assessments, adopting safety by design and privacy by design principles, enhancing digital literacy among children and parents, and strengthening international cooperation. Such measures would enable Indonesia's digital governance to maintain technological innovation while ensuring comprehensive protection of children in the digital environment.

Keyword: Children's rights; digital governance; legal safeguards; child protection

1. Introduction.

The growth of digital technology in Indonesia over the past decade has been extraordinarily rapid. Data from the Indonesian Internet Service Providers Association (APJII) indicate that internet penetration has steadily increased year after year, with the number of users surpassing 200 million in recent years. (Survei APJII, 2025) This progress has been driven by increasingly accessible internet services, the growing affordability of digital devices, and the expansion of telecommunication networks into remote areas. These changes carry significant implications, particularly for children who are now growing up in a digitally mediated environment from an early age. (Dandan Wu, 2024)

For children, digital technology creates new opportunities for learning, social interaction, and skill development. (Lowery, 2023) Online learning platforms, educational games, and social media enable them to acquire knowledge more rapidly and connect with a broader world. (Norouzi, 2024) As a result, digital technology has become an integral part of children's lives in

Indonesia, shaping their behavioral patterns and the ways in which they interact with their surroundings. (Mega Mustika Sari, 2024)

However, these developments bring not only benefits but also serious challenges. Children are often vulnerable internet users due to their limited understanding of digital security, privacy, and the social consequences of online interactions. (Musaddag Elrayah, 2023) Phenomena such as cyberbullying, online sexual exploitation, and the misuse of personal data pose real threats that can significantly affect children's well-being and overall development. (Laczi, 2024) This situation demonstrates that although digital technology offers significant opportunities, without proper regulation and adequate protection, children can be easily exposed to risks that endanger their fundamental rights. The positive benefits—such as access to education, social interaction, and self-development—must therefore be carefully balanced against these potential harms. (Musaddag Elrayah, 2023)

As digital technology becomes increasingly embedded in children's lives, the risks associated with its use have also grown more complex. One of the most pervasive threats is cyberbullying, a form of harassment carried out through digital media. This phenomenon frequently occurs in social media interactions, messaging groups, and online gaming platforms. (Rihhadatul Aisya, 2024) Cyberbullying may take the form of insults, threats, harassment, or the spread of false information targeting children. Its impact is not limited to psychological harm—such as fear, anxiety, and diminished self-esteem—but can also disrupt academic performance and have enduring consequences for children's mental health.

In addition, children face the risk of online exploitation, including grooming, child trafficking, and digital sexual exploitation. (UNICEF, 2024) Their limited ability to recognize criminal schemes, combined with insufficient supervision, makes them more susceptible to perpetrators who exploit digital spaces for illegal purposes. Reports from international organizations such as UNICEF and Interpol reveal an alarming increase in cases of online child sexual exploitation. (UNICEF, 2024)

This phenomenon illustrates how the digital sphere, which should serve as a medium for learning and creativity, can instead be transformed into a vehicle for crimes against children. In many cases, children access digital services without fully understanding the implications of sharing personal details such as addresses, photographs, or school data. (Novira, Astuti, Albadi, & Harmono, 2024) At the same time, national regulations often fail to provide specific protections for children's data.

Privacy is a fundamental right guaranteed by the Convention on the Rights of the Child (CRC), and its violation can have long-term consequences, from identity theft to misuse of children's data for commercial or criminal purposes. (Sofian, Pratama, & Capaldi, 2021) While digital technology offers vast opportunities for children, it also poses serious risks such as cyberbullying, online exploitation, and data privacy breaches that demand a clear, comprehensive, and child-centered legal framework. In Indonesia, digital regulations—including the Electronic Information and Transactions Law (UU ITE), the Child Protection Law (Law No. 35 of 2014 in conjunction with Law No. 23 of 2002), and the Personal Data Protection Law (UU PDP)—reflect the state's commitment to cybersecurity and digital economic growth.

However, these laws leave significant gaps in child-specific protection: the Child Protection Law provides general safeguards but does not regulate online interactions, and the PDP Law lacks explicit measures for children's data, while UU ITE focuses on system security and post-violation enforcement rather than proactive protection. This regulatory imbalance exposes children to risks and underscores the urgent need for comprehensive, child-centered reforms that integrate the best interests of the child into Indonesia's digital governance framework without hindering technological innovation.

This study aims to analyze the adequacy of legal protections for children in digital spaces under existing national regulations, while also formulating strategies to integrate children's

rights into Indonesia's digital governance framework without hindering technological innovation. With this focus, the research seeks to contribute both theoretically and practically, particularly by promoting the development of regulations that prioritize the best interests of the child in the digital era.

The research employs a normative juridical (doctrinal) approach, drawing on several methods. The statutory approach is used to examine national legal instruments such as the Electronic Information and Transactions Law (UU ITE), the Child Protection Law, the Personal Data Protection Law (UU PDP), and related regulations. The conceptual approach is applied to explore principles of child protection and the concept of equitable digital governance. In addition, a comparative approach reviews international standards, including the Convention on the Rights of the Child (CRC), General Comment No. 25 on children's rights in relation to the digital environment, the General Data Protection Regulation (GDPR), and the United Kingdom's Age-Appropriate Design Code. Through this methodology, the study seeks to identify gaps between national law and international standards while offering a more comprehensive model for the legal protection of children in digital contexts.

2. Adequacy of Child Protection in the Digital Space in Indonesia.

The expansion of digital spaces in Indonesia offers both opportunities and considerable challenges for safeguarding children's rights. (Sihabudin, 2023) While national legislation has established several relevant legal instruments—such as the Electronic Information and Transactions Law (ITE Law), the Child Protection Law, and the Personal Data Protection Law (PDP Law)—their effectiveness in protecting children within digital environments remains uncertain. Unlike conventional social spaces, digital contexts introduce unique risks (Azzaakiyyah, 2023), including exposure to harmful content, cyberbullying, online sexual exploitation, and the misuse of personal data. (Laczi, 2024) This raises a critical question: to what extent do existing laws provide comprehensive, child-centered protection that addresses these distinctive vulnerabilities? Addressing this question requires a detailed analysis of the scope, limitations, and implementation of current regulations in light of the evolving digital landscape.

The Electronic Information and Transactions Law (ITE Law) serves as one of the primary instruments regulating online activities, including prohibitions on the dissemination of content containing violence, pornography, and hate speech. From a child protection perspective, the ITE Law plays an important role in preventing the circulation of content that could negatively affect children's development. For instance, Article 27 of the ITE Law prohibits the distribution of indecent or pornographic content that can clearly harm children. However, the regulation is largely reactive, focusing on enforcement after a violation has occurred rather than on proactive prevention and protection measures. In this framework, children are positioned merely as general objects of protection, without specific provisions addressing their unique needs and vulnerabilities in digital environments.

The Child Protection Law (Law No. 35 of 2014, as an amendment to Law No. 23 of 2002) explicitly affirms children's rights to protection from all forms of violence, exploitation, and discrimination, including those occurring in digital contexts. Article 59 of this law obligates the state, government, and other institutions to provide special protection to children who are victims of sexual exploitation, trafficking, or violence facilitated by information technology. Normatively, these provisions clearly establish the state's responsibilities. However, in practice, this specialized protection has not yet been fully integrated into national digital governance. There are no detailed technical guidelines specifying how digital platforms should adjust their design, algorithms, or content moderation systems to comply with the principles of child protection. (Comission, 2024)

Furthermore, the Personal Data Protection Law (Law No. 27 of 2022) provides an important legal framework for safeguarding children's personal data in digital spaces. Article 9 stipulates that the processing of children's personal data must be carried out with the valid consent of a parent or guardian. This aligns with international principles emphasizing the need for additional protections for children's data due to their heightened vulnerability compared to adults. (Li & Yu, 2024) Nevertheless, a significant weakness lies in the limited technical mechanisms to ensure that digital platforms comply with this principle. For example, there are no national standards for age verification, parental oversight mechanisms, or child-friendly default settings for digital applications and services.

Overall, an analysis of these three regulations indicates that they provide a legal foundation for protecting children in digital spaces. However, their focus tends to lean more toward cybersecurity and the promotion of digital technological innovation rather than the best interests of the child. The ITE Law is primarily oriented toward system security and enforcement after violations occur; the Child Protection Law affirms general protections but has yet to penetrate the technical dimensions of digital governance; and the PDP Law emphasizes data protection, though its implementation remains largely declarative.

The primary weakness of the existing legal framework is the absence of a child-centered approach in Indonesia's digital regulations. Children are often treated as part of the general population to be protected (Tahir & Lestari, 2025), without mechanisms or rules specifically governing how digital environments should be designed to ensure safe and healthy participation for them. This contrasts with practices in other jurisdictions, such as the United Kingdom's Age-Appropriate Design Code, which mandates digital service providers to comprehensively implement child protection principles across all aspects of their services. (Mootz & Blocker, 2024)

In conclusion, the adequacy of legal protection for children in Indonesia's digital spaces remains suboptimal. Although overarching legislation exists through the ITE Law, the Child Protection Law, and the PDP Law, these regulations primarily emphasize cybersecurity and technological innovation. Specific protections for children remain largely normative and declarative, lacking clear technical frameworks and strong integration with digital governance. Therefore, policy reform is needed that places the best interests of the child at the forefront of every policy, regulation, and practice within Indonesia's digital governance framework.

3. Integration of Child Rights Protection into Indonesia's Digital Governance

The increasing penetration of digital technology in Indonesia has highlighted the need for governance that not only emphasizes security and innovation but also ensures comprehensive child protection. Digital governance fundamentally encompasses a set of rules, policies, and mechanisms that regulate how digital technologies are developed, accessed, and utilized by society. Within this context, integrating child protection means embedding principles of child safeguarding into the design of regulations, public policies, and operational practices of digital platforms in Indonesia. One of the primary principles that should serve as a foundation is the best interests of the child, as enshrined in the Convention on the Rights of the Child (CRC). (George & Awal, 2019) This principle is further reinforced by General Comment No. 25 (2021), which specifically addresses children's rights in digital environments, obligating states to ensure that children have access to safe, inclusive digital spaces that support their development. The application of this principle can be operationalized by requiring all digital policies and regulations in Indonesia to undergo a child impact assessment, which evaluates the potential effects of digital policies on children. In this way, legal frameworks and technological innovations can be designed to prioritize not only security and innovation but also the optimal protection of children.

This principle aligns with other, more advanced international standards, such as the European Union's General Data Protection Regulation (GDPR), which provides specific protections for children's data, including the requirement for parental consent when processing the data of children below a certain age (Jasmontaite & hert, 2014), and the United Kingdom's Age-Appropriate Design Code, which obligates digital platforms to implement child-friendly default settings, prohibit location tracking, and present information in language that is easily understandable by children. These examples demonstrate that child protection can be integrated from the technology design stage (safety by design and privacy by design) without compromising innovation. (OECD, 2024) By adopting similar principles, Indonesia can strengthen its digital governance framework so that it not only focuses on system security and economic growth but also ensures comprehensive protection of children's rights in digital spaces.

With this approach, the development of regulations such as the ITE Law, the PDP Law, and other derivative policies would not only assess cybersecurity and digital economic considerations but also evaluate the extent to which these policies protect—or potentially harm—children. For example, when the government issues rules regarding content blocking or digital identity verification, it must ensure that such mechanisms do not restrict children's access to information that supports their education and development. Within this framework, it is also essential for Indonesia to learn from international practices and standards that have already integrated child protection principles into digital governance. For instance, the European Union's General Data Protection Regulation (GDPR) sets high standards for the protection of personal data, including children's data, by requiring additional safeguards and parental consent for the processing of data for children below a specified age.

Moreover, the United Kingdom's Age-Appropriate Design Code provides a concrete example of how child protection principles can be implemented in digital technology design. The Code requires digital platforms to prioritize child-friendly default settings, restrict the tracking of children's locations, and ensure that information is presented in language that is understandable to children. Such an approach could be adapted in Indonesia so that digital platforms operating under national jurisdiction are required to meet child protection standards from the product design stage itself, following principles of privacy by design and safety by design.

However, despite the importance of integrating child protection into digital governance, there are several challenges in its implementation. First, regulations in Indonesia remain sectoral and uncoordinated, with the ITE Law, the Child Protection Law, and the PDP Law operating independently without a unified policy framework that places child protection in digital spaces at the forefront. This lack of integration results in inconsistencies in implementation, such as differing standards for the minimum age to access digital services or variations in content oversight mechanisms involving children.

Second, there exists a dilemma between protection and innovation. Indonesia actively promotes the growth of the digital economy as a key driver of national development. (Nuryakin, 2025) However, this push for innovation often overlooks child protection. For example, many educational technology applications or social media platforms accessible to children lack adequate parental control features or data protection measures. (Morgan & KRISTJÁNSSON, 2017) If regulations are too strict, they risk stifling innovation; conversely, if regulations are too lenient, children's interests may be compromised.

Third, implementation challenges also stem from the limited capacity of law enforcement and regulatory bodies. For instance, the authority of the Ministry of Communication and Information Technology (Kominfo) to block harmful content remains primarily focused on pornography and online gambling, while more specific issues such as cyberbullying, online grooming, or digital sexual exploitation have not yet received sufficient prioritization.

To address these challenges, several strategies can be undertaken. First, strengthening a unified regulatory framework that places child protection as a core principle in all digital policies.

This can be achieved through the issuance of government or presidential regulations that specifically govern digital governance with a focus on safeguarding children.

Second, the implementation of the safety by design principle within the digital industry. The government can require digital service providers to incorporate child protection features from the application design stage. For example, this could include default settings that limit interactions with strangers, restrictions on behavioral advertising, and easily accessible reporting mechanisms for children.

Third, enhancing digital literacy among children and parents. Regulations cannot be effective without public understanding and engagement. Therefore, public education programs targeting children, parents, and teachers are necessary to raise awareness of digital risks and to provide guidance on how to protect themselves in online environments.

Fourth, strengthening international cooperation. Given the transboundary nature of the digital space, Indonesia needs to actively adopt and adapt international standards, as well as collaborate with other countries in efforts to combat online child exploitation, the trafficking of children's personal data, and the spread of harmful content.

A central issue in integrating child protection is how to safeguard children without stifling technological innovation. To address this, it is important to establish a regulatory sandbox that allows digital innovations to be tested within a controlled environment under strict supervision. Through this mechanism, developers can trial digital products or services while ensuring compliance with child protection principles before a full-scale launch. Additionally, a principle-based co-regulation approach can be applied, where the government sets baseline child protection standards, and the industry is given flexibility to develop internal mechanisms that align with these standards. In this way, children's protection is maintained without constraining innovation or the growth of the digital economy.

4. Conclusion

This study demonstrates that child protection in Indonesia's digital space remains inadequate, as regulations such as the ITE Law, the Child Protection Law, and the PDP Law prioritize system security and technological innovation over children's specific needs. Consequently, legal gaps persist in addressing risks such as cyberbullying, online exploitation, and data privacy violations. Therefore, a child-centered legal reform is necessary, integrating the principle of the best interests of the child into digital governance through a unified regulatory framework, the application of safety by design principles in the digital industry, the enhancement of digital literacy for children and parents, and the strengthening of international cooperation. By adopting these strategies, Indonesia can create a digital environment that is not only safe and inclusive for children but also continues to foster technological innovation.

References

- [1] Azzaakiyyah, H. K. (2023). The Impact of Social Media Use on Social Interaction in Contemporary Society. *Technology and Society Perspectives (TACIT)*, 1-9.
- [2] Commission, E. (2024, March 7). *European Commission*. Retrieved from [comission.europa.eu: https://commission.europa.eu/system/files/2022-12/10_principles_for_integrated_child_protection_systems_en.pdf](https://commission.europa.eu/system/files/2022-12/10_principles_for_integrated_child_protection_systems_en.pdf)
- [3] Dandan Wu, X. D. (2024). How Early Digital Experience Shapes Young Brains During 0-12 Years: A Scoping Review. *Early Education and Development*, 1395-1431.
- [4] Fund, U. N. (2024). *Protecting children from violence and exploitation in relation to the digital environment: Policy Brief*. New York: UNICEF Child Protection Team.
- [5] George, M., & Awal, N. A. (2019). THE BEST INTEREST PRINCIPLE WITHIN ARTICLE 3(1) OF THE UNITED NATIONS. *International Journal of Business, Economics and Law*, 30-36.

- [6] Jasmontaite, L., & hert, P. d. (2014). he EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law*, 20-33.
- [7] Laczi, S. (2024). Navigating Children's Cybersecurity Landscape: Understanding the impact of cyberbullying, online harrasment and identity theft on children. *IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (pp. 1-6). Timisoara, Romania: IEEE (Institute of Electrical and Electronics Engineers) .
- [8] Li, B., & Yu, W. (2024). Enhancing Legal Protection of Children's Rights in the "Internet Plus". *International Journal of Information Security and Privacy*, 1-17.
- [9] Lowery, T. L. (2023). The Impact of Digital Technology on Children's Social Interaction: A Literature Review. *Conference: Communications Studies*.
- [10] Mega Mustika Sari, D. F. (2024). The Influence of Digital Parenting on the Social Behavior of Early. *Jurnal Multi disiplin Indonesia*.
- [11] Mootz, J., & Blocker, K. (2024). *UK Age-Appropriate Design Code Impact Assessment*. Children and Screens, Institute of Digital Media and Child Development.
- [12] Morgan, B., & KRISTJÁNSSON, K. (2017). Parents and Social Media: Adolescents Perception of Parental Response to Morally Salient Social Media Scenario. *The Jubilee Centre for Character and Virtues*.
- [13] Musaddag Elrayah, S. J. (2023). Impact of Digital Literacy and Online Privacy Concerns. *International Journal of Cyber Criminology*, 166-187.
- [14] Norouzi, B. S. (2024). Enabling children's genuine participation in digital design and fabrication: instructors' perspective. *International Journal of Technology and Design Education* , 1067-1091.
- [15] Novira, D., Astuti, W. S., Albadi, M. F., & Harmono, H. (2024). Legal Protection of Children's Personal Data in the Digital Era. *Journal Of Social Research*.
- [16] Nuryakin, C. (2025). Indonesia's Development of Digital Economy. In *ASEAN Digital Community 2045 Country Perspectives* (p. 27). Economic Research Institute for ASEAN and East Asia.
- [17] OECD. (2024). *TOWARDS DIGITAL*. OECD DIGITAL ECONOMY PAPERS.
- [18] Rihhadatul Aisya, N. (2024). Cyberbullying: The Silent Epidemic of The Digital Age. *Journal of World Science*, 691-697.
- [19] Sihabudin, S. (2023). Expanding the Limitations of the Protection and Processing of Children's Personal Data: An Overview of Current Regulations, Challenges, and Recommendations. *Brawijaya Law Journal*, 59-71.
- [20] Sofian, A., Pratama, B., & Capaldi, M. (2021). Children's Privacy and Data Protection in Judicial Decisions in Indonesia. *US-China Law Review*, 153-161.
- [21] *Survei APJII*. (2025). Retrieved from <https://survei.apjii.or.id/>: <https://survei.apjii.or.id/>
- [22] Tahir, R., & Lestari, T. Y. (2025). Children's Digital Rights: An In-depth Analysis of Indonesia, Europe, and the US. *Eduvest, Jiurnal Of Universal Studies*, 1942-1964. .
- [23] UNICEF. (2024). *Protecting children from violence and exploitation in relation to the digital environment: Policy Brief*. New York: UNICEF Child Protection Team.