The Easta Journal Law and Human Rights
Vol. 4, No. 02, February 2026, pp. 171- 180
ISSN: 2985-7112, DOI: 10.58812/eslhr.v4i02

Protection of Children's Personal Data (CPD) in the Digital Environment, Legal Obligations of Online Platforms (OPs) in Indonesia

Nurhabibah[1], Dian Puspa Iwari[2], Istiarsyah[3]
[1] STAI Darul Hikmah, Aceh Barat
[2] Universitas Muhammadiyah Palembang
[3] Universitas Muhammadiyah Mahakarya Aceh

Article Info

Article history:

Received Feb, 2026
Revised Feb, 2026
Accepted Feb, 2026

Keywords:

Child Personal Data;
Data Protection Law;
Digital Environment;
Indonesia;
Online Platforms

ABSTRACT

The rapid expansion of the digital environment has intensified the collection and processing of children's personal data by online platforms, raising significant legal concerns regarding privacy and child protection. This study examines the protection of Child Personal Data (CPD) in Indonesia by focusing on the legal obligations of Online Platforms (OP) within the digital ecosystem. Employing a normative juridical approach, the research analyzes statutory regulations on personal data protection, electronic systems, and child protection to assess their coherence and effectiveness. The findings indicate that although Indonesia has established a legal foundation recognizing children as a vulnerable group requiring heightened data protection, regulatory fragmentation, limited operational guidance, and enforcement challenges remain. In particular, ambiguities related to consent mechanisms, age verification, accountability standards, and cross-border platform operations weaken the practical protection of children's data. This study concludes that clearer, more specific, and enforceable legal obligations for online platforms are necessary to ensure effective CPD protection and to strengthen children's rights in Indonesia's digital environment.

Corresponding Author:

Name: Nurhabibah
Institution: STAI Darul Hikmah, Aceh Barat
Email: nurhabibah@staidarulhikmah.ac.id

1. INTRODUCTION

The rapid advancement of digital technology has significantly transformed patterns of communication and information access, with children becoming one of the most active users of digital platforms such as social media, online games, educational applications, and video-sharing services. Although these platforms provide substantial benefits for learning, creativity, and social interaction, they also expose children to heightened risks related to the collection, processing, and exploitation of personal data. Children's limited capacity to understand privacy risks and the long-term consequences of data misuse makes them particularly vulnerable to practices such as data profiling, targeted advertising, and algorithmic decision-making, which may result in identity theft, cyberbullying, online grooming, and commercial exploitation [1], [2].

In response to these risks, various legal frameworks have been developed at national and international levels to protect children's personal data in the digital environment. In Indonesia, legal protection is provided through instruments such as the Child Protection Act and the Personal Data Protection Act, which aim to mitigate cybercrime risks and prevent psychological harm to children [3]. At the international level, the United Nations Convention on the Rights of the Child (UNCRC) affirms children's right to privacy and underscores the need for legal adaptation to address digital challenges (Arnetta et al., 2023), while countries such as Brazil have also strengthened regulations addressing cyberbullying and digital privacy violations involving children [4]. However, challenges remain in regulating consent within data-driven digital economies and ensuring effective implementation, highlighting the importance of coordinated efforts among governments, digital service providers, parents, and educators to enhance children's digital literacy, autonomy, and dignity [1], [3].

Internationally, the protection of children's personal data is increasingly recognized as an essential element of child rights protection, positioning children as rights holders who require heightened safeguards in data processing, particularly in terms of consent, transparency, and accountability. However, the effectiveness of these protections largely depends on the extent to which clear and enforceable legal obligations are imposed on online platforms as central actors in the digital ecosystem. Comparative perspectives, including international frameworks such as the GDPR, highlight gaps in national approaches and emphasize the importance of adopting international best practices alongside strengthened digital literacy initiatives to ensure meaningful protection of children's data [5].

In Indonesia, the issue of children's personal data protection has gained urgency alongside the rapid increase in internet use among children and adolescents. Although several legal instruments—such as the Child Protection Act, the Electronic Information and Transaction Act, and the Personal Data Protection Act—have been enacted, recurring incidents of data misuse and privacy violations reveal persistent challenges related to regulatory coherence, enforceability, and practical effectiveness [3]. These limitations have prompted calls for more specific legal provisions addressing children's data, including potential amendments to existing laws to better reflect children's vulnerabilities in the digital environment [6]. Furthermore, Law Number 1 of 2024 underscores the responsibilities of electronic system providers in ensuring child protection through data safeguards and content control, highlighting the need for strong government oversight and active stakeholder participation in creating a safer digital space for children [7].

Online platforms play a strategic role in determining how children's personal data is collected and processed, as they function as data controllers and processors with significant control over technological design, data governance, and compliance mechanisms. Therefore, the protection of children's personal data cannot rely solely on parental supervision or individual awareness but must be supported by clear and enforceable legal obligations imposed on online platforms, including lawful and fair data processing, valid consent mechanisms, adequate data security, the prevention of harmful profiling, and the availability of effective remedies in cases of data misuse.

Despite the growing regulatory framework, normative ambiguities and implementation challenges remain, particularly due to overlapping legal instruments, limited enforcement capacity, and the transnational nature of digital platforms operating in Indonesia. These challenges raise complex issues related to jurisdiction, cross-border data transfers, and regulatory compliance, underscoring the need for a systematic legal analysis of the responsibilities of online platforms in protecting children's personal data. Accordingly, this paper examines the protection of Child Personal Data (CPD) in the digital environment using a normative

juridical approach, focusing on the scope, consistency, and effectiveness of Indonesian laws and regulations in regulating online platforms and assessing whether the current legal framework provides adequate protection for children in the digital era.

2. LITERATURE REVIEW

2.1 Concept of Personal Data Protection

The protection of personal data constitutes a fundamental aspect of privacy rights in the digital age, particularly amid increasing risks of data breaches and misuse, prompting the evolution of legal frameworks that emphasize transparency, fairness, accountability, purpose limitation, data minimization, accuracy, storage limitation, and security as core principles of lawful data processing. These principles, which underpin major data protection regimes such as the General Data Protection Regulation (GDPR), are designed to ensure that personal data is collected, processed, and stored in a lawful and transparent manner while protecting individuals from discrimination, surveillance, and other forms of harm [8]–[10]. However, the rapid advancement of digital technologies and the global exchange of information continue to pose legal and technological challenges, particularly in balancing the promotion of data-driven innovation with the need for effective privacy protection, requiring legal frameworks to continuously adapt to emerging risks and practices [11].

2.2 Child Personal Data Protection (CPD)

The protection of children's personal data (CPD) represents a crucial intersection between privacy rights and child protection, as children are particularly vulnerable in digital environments due to their limited understanding of privacy risks and their inability to provide fully informed consent. Consequently, many legal frameworks have introduced enhanced safeguards that prioritize the best interests of the child by emphasizing safety, well-being, and long-term protection in data processing activities involving children, especially in response to risks such as profiling, targeted advertising, and exposure to harmful content [12]. Comparative legal approaches illustrate these efforts, including the EU's General Data Protection Regulation (GDPR), which requires explicit parental consent and embeds the best interests of the child principle, although its application remains uneven across jurisdictions such as Vietnam [13], as well as Brazil's data protection regime, which recognizes children as a vulnerable group despite ongoing ambiguities regarding parental consent exceptions [14]. In Indonesia, the absence of specific legal norms governing online child data protection underscores the urgency of regulatory reform to prevent violations of children's rights, particularly as the balance between parental authority and children's evolving privacy rights becomes increasingly complex with age, especially from around 12 years old when children gain the right to be heard [15], [16].

2.3 Digital Environment and Data Vulnerability

The digital environment has fundamentally transformed personal data processing, particularly affecting children who engage with online platforms often without sufficient awareness or meaningful consent, thereby intensifying privacy and data protection challenges. The literature highlights a structural power imbalance between users and digital platforms that exacerbates children's vulnerability, as data are frequently collected automatically without the knowledge of children or their parents, increasing risks of data breaches, exploitation, and unethical data practices [17]. Limited understanding of data processing among children and parents further compounds these risks, revealing persistent regulatory gaps that call for updates to existing laws and the development of stronger policy

frameworks, including the adoption of privacy-by-design principles and international standards such as the GDPR [18]. In Indonesia, recent legal amendments have emphasized the responsibility of electronic system providers to protect children's data, underscoring the importance of effective government oversight and public participation [7]. At the same time, emerging technologies such as artificial intelligence and digital content creation introduce new ethical concerns, including premature adultification and commercial exploitation of children's data, highlighting the need for integrated technological, legal, and ethical strategies within broader digital ecosystems and smart city initiatives [7], [19] (Beckmann-Cavalcante et al., 2025; Freitas, 2023).

2.4 Legal Obligations of Online Platforms

Online platforms occupy a central position in the digital ecosystem and, as data controllers or processors, bear primary responsibility for ensuring compliance with data protection principles, particularly in relation to children's personal data. The literature emphasizes that platforms must obtain valid consent, provide clear and age-appropriate privacy information, limit data collection, implement robust security measures, and prevent the commercial exploitation of children's data, supported by a proactive regulatory approach grounded in privacy by design and privacy by default [20]. International standards such as UNICEF's Manifesto and the Children's Rights by Design framework further articulate specific legal requirements that place the burden of compliance on platforms themselves [20]. Nevertheless, data-driven business models continue to pose significant risks, as existing regulatory approaches often emphasize post-collection safeguards rather than meaningful consent, while children's mediated interactions with digital spaces—frequently involving family members—further complicate privacy protection [2]. In this context, enhancing children's media literacy is essential to enable critical engagement with digital environments and to address persistent gaps in understanding privacy implications [1]. Recent legal developments, including the Meta decision of the European Court of Justice, reinforce the need for a fundamental reassessment of platform data-processing practices, particularly with respect to minors, highlighting the growing expectation of stricter and more enforceable legal obligations for online platforms [21].

2.5 Research Gap

Although there is a growing body of literature on personal data protection and digital privacy, studies that specifically focus on the legal obligations of online platforms in protecting children's personal data in the Indonesian context remain limited. Much of the existing literature discusses data protection from a general perspective or focuses on comparative analysis with foreign legal systems. Consequently, there is a lack of in-depth normative analysis that systematically examines how Indonesian laws regulate online platforms in relation to CPD.

This research addresses this gap by focusing on the Indonesian legal framework and by analyzing the specific obligations imposed on online platforms concerning children's personal data. By adopting a normative juridical approach, this study contributes to the academic discourse by clarifying legal responsibilities, identifying regulatory weaknesses, and providing a structured legal understanding of CPD protection in Indonesia's digital environment.

3. RESEARCH METHOD

3.1 Research Type and Approach

This research employs a normative juridical method, a doctrinal legal approach that examines law as a system of norms by analyzing legal rules, principles, and doctrines governing the protection of children's personal data in

the digital environment, particularly the obligations imposed on online platforms in Indonesia. This approach is appropriate because the study focuses on assessing the coherence, scope, and adequacy of existing legal norms, evaluating whether current legal provisions sufficiently address children's unique vulnerabilities and impose clear, enforceable responsibilities on online platforms, rather than examining empirical behavior or social perceptions.

3.2 Research Object and Scope

The object of this research is the legal regulation of Child Personal Data (CPD) protection in Indonesia, with a particular focus on the legal obligations of Online Platforms (OP) operating in the digital environment, encompassing laws and regulations on personal data protection, electronic systems, child protection, and digital services relevant to the processing of children's data. The study is limited to the analysis of Indonesian positive law and concentrates on the normative aspects of regulation—such as rights, obligations, prohibitions, and sanctions related to CPD protection—without engaging in comparative legal analysis except where conceptually necessary to clarify legal principles.

3.3 Types and Sources of Legal Materials

This research relies exclusively on legal materials rather than empirical data, comprising primary legal materials in the form of binding instruments such as the Constitution of the Republic of Indonesia, laws and regulations on personal data protection, electronic information and transactions, child protection, and related government and ministerial regulations on electronic systems and data processing; secondary legal materials including legal textbooks, monographs, academic journal articles, legal commentaries, expert opinions, and research reports that analyze and interpret child personal data protection and digital law; and tertiary legal materials such as legal dictionaries, legal encyclopedias, and indexes or legal databases used to support understanding and facilitate access to primary and secondary sources.

3.4 Data Collection Technique

This research employs a library research (desk research) method for data collection, whereby legal materials are systematically gathered through the review of statutes, official government publications, academic databases, and reputable legal journals. The collection process focuses on identifying authoritative, up-to-date, and contextually relevant legal norms concerning child personal data protection and the responsibilities of online platforms in Indonesia, enabling a comprehensive and structured analysis of the regulatory framework governing CPD.

3.5 Legal Material Analysis Method

The analysis of legal materials in this research is conducted through qualitative normative analysis, involving statutory interpretation to examine the meaning, scope, and implications of legal provisions on child personal data protection and online platform obligations, systematic interpretation to assess the coherence and interrelation of relevant laws and regulations, and conceptual analysis to clarify key legal concepts such as personal data, child consent, data controller responsibilities, and digital platform accountability, with the aim of identifying normative standards, legal obligations, and potential regulatory gaps in the protection of children's personal data.

4. RESULTS AND DISCUSSION

4.1 Legal Framework for Child Personal Data Protection in Indonesia

The protection of Child Personal Data (CPD) in Indonesia is governed by an integrated yet multi-layered legal framework that combines general data protection regulations, child protection laws, and rules governing electronic systems and digital services. The enactment of the Personal Data Protection

Law Number 27 of 2022 represents a pivotal development, as it formally recognizes personal data protection as a legal right and introduces binding obligations for all parties involved in data processing. This law marks a shift from fragmented, sectoral regulation toward a more unified approach, while explicitly identifying children as a vulnerable group that requires heightened protection [22]. Complementary regulations, including the Child Protection Act and the Electronic Information and Transaction Act, further address specific risks faced by children in digital environments [3]. In addition, Law Number 1 of 2024 strengthens the responsibilities of electronic system providers, particularly with regard to safeguarding children's data through content filtering mechanisms and reporting systems [7].

Despite this normative commitment, significant challenges remain in practice. One of the main issues is the persistence of overlapping and dispersed legal provisions concerning CPD, which can lead to regulatory ambiguity and inconsistent interpretation [23]. While the Personal Data Protection Law provides a general foundation, its effective application to children's data depends heavily on coordination with sector-specific regulations and child protection norms. This fragmented structure complicates compliance for digital platform providers, particularly in determining consent mechanisms, age verification standards, and the precise scope of their legal responsibilities when processing children's personal data. Comparative legal studies therefore recommend aligning national regulations with international standards, such as the Children's Online Privacy Protection Rule, to strengthen consent requirements and enhance the overall protection of children's data [24].

From a normative and practical perspective, Indonesian law adopts the principle that children's personal data must be processed with a higher standard of care than adult data. This principle is reflected in provisions emphasizing lawful processing, purpose limitation, data security, and accountability, as well as in child protection legislation that recognizes children as rights holders whose best interests must be prioritized in all actions affecting them, including digital activities. The consequences of inadequate protection are substantial, ranging from cybercrime and misuse of data to emotional trauma and impaired child development [3]. Accordingly, future efforts must focus not only on strengthening regulatory coherence but also on effective implementation, requiring active collaboration among government authorities, technology providers, and parents to ensure a safe and rights-respecting digital environment for children [7].

4.2 Legal Position and Responsibility of Online Platforms

Online platforms occupy a central position in the digital ecosystem as primary actors responsible for collecting, processing, and controlling personal data. Under Indonesian law, these platforms are normatively classified as electronic system operators as well as personal data controllers or processors, depending on their functional roles. Consequently, they are legally obliged to ensure that all data processing activities comply with fundamental data protection principles, including lawfulness, transparency, and accountability. In the context of Child Personal Data (CPD), these responsibilities are further reinforced by the Personal Data Protection Law of 2022, which requires platforms to guarantee data security, obtain valid consent, and respect the rights of data subjects [25], [26]. In addition, Law Number 1 of 2024 explicitly emphasizes the duty of electronic system providers to protect children in digital spaces through mechanisms such as content filtering and enhanced data protection measures [7].

From a normative standpoint, online platforms are not merely passive

intermediaries but active entities that exercise direct control over technological architecture, data governance policies, and operational practices. This level of control positions them as key gatekeepers in the protection of children's personal data, as they determine how data is collected, stored, processed, and shared. Accordingly, the law imposes heightened obligations on platforms to implement adequate technical and organizational safeguards, prevent unauthorized access or misuse of children's data, and ensure that processing activities are conducted in a manner consistent with the best interests of the child. Failure to meet these obligations may give rise to administrative sanctions, civil liability, or other legal consequences, depending on the severity and impact of the violation [26].

Despite the existence of a relatively strong legal framework, significant challenges persist in its practical implementation. These challenges include limitations in digital infrastructure readiness, uneven compliance among business actors, and gaps in awareness and technical capacity to implement robust data protection systems [26], [27]. To address these issues, scholars highlight the importance of targeted education and training for business actors, alongside the development and adoption of more advanced data security technologies [26]. From a comparative perspective, Indonesia may also benefit from adopting selected elements of the European Union's Digital Markets Act, particularly in regulating platform power and strengthening accountability mechanisms within the digital ecosystem [28].

4.3 Consent and Age-Related Protection Mechanisms

One of the most critical aspects of Child Personal Data (CPD) protection concerns consent. Normatively, Indonesian law recognizes that children may lack both the legal capacity and cognitive ability to provide informed consent for the processing of their personal data. Consequently, consent involving children must be accompanied by special safeguards, particularly through the involvement of parents or legal guardians. The Child Protection Act and the Personal Data Protection Act explicitly acknowledge the importance of parental consent in relation to children's data; however, these laws do not provide detailed procedural guidance for online platforms on how such consent should be obtained, verified, and managed in digital environments [3], [29].

The absence of specific and operational regulations governing children's data protection in online contexts creates significant practical challenges. Automated data collection and user registration systems used by digital platforms make it difficult to ensure that parental consent is genuinely obtained and verified, particularly in cross-border settings where jurisdictional issues further complicate enforcement [30]. As a result, online platforms often rely on self-declared age mechanisms that are insufficient to guarantee effective protection, increasing the risk of misuse and exploitation of children's personal data [24] (Putri et al., 2024; Widyaningsih & Suryaningsi, 2022). From a normative perspective, this regulatory gap weakens the effectiveness of CPD protection and creates uncertainty for platforms regarding their legal obligations.

To address these shortcomings, comparative legal studies recommend the adoption of clearer and more detailed consent frameworks similar to those applied in the European Union and the United States. In particular, legislation such as the Children's Online Privacy Protection Act (COPPA) provides explicit standards for obtaining and verifying parental consent in digital environments, which could serve as a useful reference for Indonesia [15], [29]. Indonesian policymakers are therefore encouraged to develop age-verification systems and parental consent mechanisms that are

tailored to the realities of digital platforms, while imposing affirmative duties on platforms to act in a child-sensitive manner [30]. Achieving effective CPD protection ultimately requires close collaboration among government authorities, technology providers, and parents to ensure a safe and rights-based online environment for children [3].

4.4 Data Processing, Security, and Accountability Obligations

Indonesian data protection law emphasizes that personal data processing must adhere to core principles such as purpose limitation, data minimization, accuracy, and security. In the context of children, these principles carry greater normative weight. Online platforms are legally required to collect only data that is strictly necessary, to use it solely for legitimate purposes, and to protect it against data breaches and unauthorized access.

The findings indicate that although these principles are clearly articulated at a normative level, their application to CPD in practice faces significant challenges. Many online platforms rely on complex algorithms, profiling techniques, and data-sharing practices that may conflict with the principle of minimizing risks to children. Profiling and targeted advertising involving children's data, in particular, raise serious legal and ethical concerns.

Accountability mechanisms are another crucial aspect of CPD protection. Normatively, online platforms are expected to demonstrate compliance through internal policies, documentation, and risk assessments. However, the current legal framework does not yet comprehensively mandate child-specific data protection impact assessments or transparency obligations tailored to children. This gap limits the ability of regulators and affected parties to assess whether platforms are genuinely prioritizing children's best interests.

4.5 Enforcement Challenges and Regulatory Gaps

Despite the existence of legal norms regulating CPD, enforcement remains one of the most significant challenges in Indonesia. The results of the normative analysis reveal that regulatory institutions face limitations in terms of authority, technical capacity, and coordination. These limitations reduce the deterrent effect of sanctions and weaken incentives for online platforms to fully comply with CPD obligations.

Another major challenge arises from the transnational nature of online platforms. Many platforms operating in Indonesia are headquartered abroad, complicating jurisdictional enforcement and cross-border data governance. While Indonesian law applies to activities that have legal effects within its territory, practical enforcement against foreign platforms remains difficult.

Normative gaps are also evident in the absence of detailed implementing regulations that specifically address children's data in digital environments. Existing laws provide general obligations but often lack operational clarity. As a result, online platforms may comply formally with data protection requirements while failing to adequately address the unique risks faced by children.

5. CONCLUSION

The protection of Child Personal Data (CPD) in the digital environment constitutes a critical legal challenge in Indonesia, particularly in light of children's growing engagement in online activities and the data-driven nature of digital platforms. This study shows that Indonesia has made notable progress in developing a normative legal framework for personal data protection, including the explicit recognition of children as a vulnerable group entitled to special safeguards. The integration of personal data protection principles with child protection norms provides a fundamental legal

foundation for regulating the processing of children's personal data in digital contexts.

Nevertheless, the analysis indicates that the existing regulatory framework remains fragmented and lacks detailed operational guidance, especially with regard to the concrete legal obligations of online platforms. Unclear consent standards, inadequate age-verification mechanisms, limited accountability provisions, and enforcement constraints weaken the practical effectiveness of CPD protection, a problem further exacerbated by the transnational operations of many digital platforms. Accordingly, strengthening CPD protection in Indonesia requires more specific and coherent regulations that clearly define platform responsibilities, supported by enhanced institutional capacity, stronger enforcement mechanisms, and greater regulatory clarity to ensure that children's personal data is processed in a manner that truly prioritizes their rights and best interests within the evolving digital ecosystem.

REFERENCES

[1] S. Livingstone, M. Stoilova, and R. Nandagiri, "Children's data and privacy online: growing up in a digital age: an evidence review," 2019.

[2] O. B. Arewa, "Data Collection, Privacy, and Children in the Digital Economy," in *Families and New Media: Comparative Perspectives on Digital Transformations in Law and Society*, Springer Fachmedien Wiesbaden Wiesbaden, 2023, pp. 195–213.

[3] D. Novira, W. S. Astuti, M. F. Albadi, and M. S. Gunawan, "Legal Protection Of Children's Personal Data In The Digital Era.," *J. Soc. Res.*, vol. 3, no. 9, 2024.

[4] M. E. G. Ahouangbe, "O ordenamento jurídico brasileiro e a proteção de crianças no ambiente digital," *Virtuajus*, vol. 9, no. 17, 2024.

[5] A. B. Gunawan, "Protection of Children Personal Data in Digital Financial Services in Indonesia," *J. Law, Polit. Humanit.*, vol. 4, no. 5, pp. 1801–1807, 2024.

[6] S. Sihabudin, "Expanding the limitations of the protection and processing of children's personal data: An overview of current regulations, challenges, and recommendations," *Brawijaya Law J.*, vol. 10, no. 1, pp. 59–71, 2023.

[7] C. Ramadhan, E. Charlest, M. Ambarita, and S. Hutapea, "Analisis Kewajiban Penyelenggara Sistem Elektronik dalam Memberikan Perlindungan Bagi Anak: Konteks UU Nomor 1 Tahun 2024," *Demokr. J. Ris. Ilmu Hukum, Sos. dan Polit.*, vol. 2, pp. 21–27, Apr. 2025, doi: 10.62383/demokrasi.v2i2.845.

[8] W. Bülow and M. Wester, "The right to privacy and the protection of personal data in a digital era and the age of information," in *Human rights and risks in the digital era: Globalization and the effects of information technologies*, IGI Global Scientific Publishing, 2012, pp. 34–45.

[9] C. Tolani and J. Pareek, "Introduction to data protection frameworks: A review," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, pp. 251–255, 2024.

[10] V. Halinkina, "Basic Principles of Personal Data Processing and Protection," *Sci. Bull. Uzhhorod Natl. Univ. Ser. Law*, vol. 1, no. 81, pp. 111–115, 2024.

[11] D. Muharman, M. Wibowo, H. Sinaga, S. Sumiyati, and E. Sumartono, "The Evolution of Privacy Law in the Digital Age: Balancing Individual Rights and Technological Innovation," *Join J. Soc. Sci.*, vol. 1, no. 4, pp. 421–432, 2024.

[12] L. D. Arnetta, G. A. Fathyasani, and T. Suryawijaya, "Children's privacy in the digital world: A review of the law on the use of technology child," 2023.

[13] L. V. Chau, N. X. Quang, and N. K. Tung, "Processing of children's personal data: a comparative study of the EU legal framework and Vietnamese law," *TalTech J. Eur. Stud.*, vol. 15, no. 2, pp. 56–71, 2025.

[14] S. R. Sena, "A Proteção de Dados Pessoais de Crianças no Ordenamento Jurídico Brasileiro," *Cad. Virtual*, vol. 2, no. 44, 2019.

[15] A. Sofian, "Perlindungan Data Privasi Anak Online dalam Mencegah Pelanggaran Hak Anak," 2020.

[16] A. H. Cerezo, "La protección de datos de los menores de edad. Especial referencia a sus excepciones en materia sanitaria y de educación," *La Ley Derecho Fam. Rev. jurídica sobre Fam. y menores*, no. 15, p. 13, 2017.

[17] A. Third, S. Livingstone, and G. Lansdown, "Recognizing children's rights in relation to the digital environment: challenges of voice and evidence, principle and practice," in *Research Handbook on Human Rights and Digital Technology*, Edward Elgar Publishing, 2025, pp. 325–360.

[18] D. A. Tayupanta-Guangatal, M. C. Mafla-Sánchez, N. Hurtado-Acosta, and I. Alfonso-Gonzáles, "Protección de datos personales en era digital [Personal data protection in the digital age]," *Verdad y Derecho. Rev. Arbitr. Ciencias Jurídicas y Soc.*, vol. 3, no. especial_Ambato, pp. 357–363, 2024.

[19] C. O. A. Freitas, "O Ciberespaço Nas Smart Cities Sob A Perspectiva Da Proteção De Dados Pessoais De Crianças E Adolescentes," *Conpedi Law Rev.*, vol. 9, no. 1, pp. 234–253, 2023.

[20] G. Valença, M. W. Sarinho, V. Polito, and F. Lins, "Do Platforms Care About Your Child's Data? A Proposal of Legal Requirements for Children's Privacy and Protection.," 2022.

[21] B. Buchner, "Der Schutz von Minderjährigen in der Datenökonomie: Die Meta-Entscheidung des EuGH und der Minderjährigendatenschutz," *Datenschutz und Datensicherheit-DuD*, vol. 47, no. 12, pp. 756–760, 2023.

[22] Y. L. Ngompat and M. G. M. Maran, "Legal Development And Urgency Of Personal Data Protection In Indonesia," *JILPR J. Indones. Law Policy Rev.*, vol. 5, no. 3, pp. 627–635, 2024.

[23] E. Lestari and R. Rasji, "Legal Study On Personal Data Protection Based On Indonesian Legislation," *Awang Long Law Rev.*, vol. 6, no. 2, pp. 471–477, 2024.

[24] C. C. Putri and R. Ganindha, "Legal Construction of the Protection and Processing of Children's Personal Data in Indonesia," in *12th UUM International Legal Conference 2023 (UUMILC 2023)*, 2024, pp. 147–155.

[25] N. Afifah, "Tanggung jawab hukum platform e-commerce terhadap keamanan data pribadi pengguna: Analisis berdasarkan UU PDP 2022," *J. Leg.*, vol. 2, no. 1, pp. 29–38, 2024.

[26] D. D. Wijayanto and K. W. Indrayanti, "Personal Data Protection in Digital Business Based on the Law on Personal Data Protection," *Int. J. Res. Soc. Sci. Humanit. ISSN 2582-6220, DOI 10.47505/IJRSS*, vol. 6, no. 8, pp. 6–12, 2025.

[27] F. Nadiah and S. A. Wiraguna, "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Dalam Transaksi Elektronik Di Indonesia," *J. Ris. Multidisiplin Edukasi*, vol. 2, no. 6, pp. 270–278, 2025.

[28] H. Hufron, S. Fikri, S. Hadi, I. Shulga, and A. S. Wibowo, "Digital Platform Power Play: Indonesian and European Union Law Perspective," *Lex Sci. Law Rev.*, vol. 8, no. 2, pp. 707–742, 2024.

[29] T. Widyaningsih and S. Suryaningsi, "Kajian Perlindungan Hukum Terhadap Data Pribadi Digital Anak Sebagai Hak Atas Privasi Di Indonesia," *Nomos J. Penelit. Ilmu Huk.*, vol. 2, no. 3, pp. 93–103, 2022.

[30] M. B. Narendra, L. L. M. SH, and A. Y. Karunian, "Protection of Children in Online Spaces: Examining Various Mechanisms for Age Verification and Parental Consent," 2024.