The Legal Position of Children's Sensitive Data in the Indonesian Personal Data Protection System: A Normative Analysis Based on the Best Interests of the Child Principle

Sidi Ahyar Wiraguna[1]*, Ayu Wulandari[2], Zhillan Zalzabilla Albana[3], Dhiyaksa Nugraha[4] , Yani Purwanti[5]

[1-5]Universitas Esa Unggul, Jakarta, Indonesia

Corresponding Author's e-mail : *adipatiwiraguna@gmail.com*

ARMADA
JURNAL PENELITIAN MULTIDISIPLIN

e-ISSN: 2964-2981

ARMADA : Jurnal Penelitian Multidisiplin

https://ejournal.45mataram.ac.id/index.php/armada

Vol. 04, No. 05 Mei, 2026

Page: 792-800

DOI:

https://doi.org/10.55681/armada.v4i5.2192

Article History:

Received: April 11, 2026

Revised: Mei 11, 2026

Accepted: Mei 20, 2026

Abstract : The digitalization of education, healthcare, and commercial platforms has intensified the collection of children's personal data, exposing vulnerabilities that remain inadequately addressed within Indonesia's legal framework. This study examines the legal position of children's sensitive data under Law No. 27 of 2022 on Personal Data Protection by analyzing normative gaps, rights redress mechanisms, and harmonization with international standards. Using normative legal research, the study applies statutory, conceptual, and functional comparative approaches supported by systematic-teleological interpretation and synchronization analysis based on the *best interests of the child* principle. The findings show that the PDP Law regulates children's data protection in a generic manner without differentiated legal standards, explicit digital consent age limits, or child-specific impact assessment obligations. Rights recovery mechanisms remain dependent on parental representation and lack child-friendly breach notification and restorative measures. Substantive inconsistencies also persist with the CRC and GDPR, particularly regarding commercial profiling restrictions and *privacy-by-design* obligations. The study recommends establishing a digital consent age of 13–15 years, mandatory parental verification, Child DPIA, and specialized supervisory mechanisms.

Keywords: *Children's Sensitive Data, Personal Data Protection, Best Interests of the Child, Regulatory Harmonization, Children's Rights Recovery.*

Abstrak: *Digitalisasi sektor pendidikan, kesehatan, dan platform komersial telah meningkatkan pengumpulan data pribadi anak, yang menimbulkan kerentanan yang masih belum direspons secara memadai dalam kerangka hukum Indonesia. Penelitian ini mengkaji kedudukan hukum data sensitif anak dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melalui analisis kesenjangan normatif, mekanisme pemulihan hak, serta harmonisasi dengan standar internasional. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif fungsional yang didukung penafsiran sistematis-teleologis serta analisis sinkronisasi berdasarkan prinsip kepentingan terbaik bagi anak (best interests of the child). Hasil penelitian menunjukkan bahwa UU PDP masih mengatur perlindungan data anak secara umum tanpa standar perlindungan yang*

terdiferensiasi, batas usia persetujuan digital yang eksplisit, maupun kewajiban penilaian dampak yang spesifik terhadap anak. Mekanisme pemulihan hak juga masih bergantung pada representasi orang tua serta belum mengakomodasi pemberitahuan pelanggaran yang ramah anak dan pendekatan restoratif. Ketidaksesuaian substantif masih ditemukan dengan CRC dan GDPR, khususnya terkait pembatasan profilisasi komersial dan kewajiban privacy by design. Penelitian ini merekomendasikan penetapan usia persetujuan digital 13–15 tahun, verifikasi persetujuan orang tua, Child Data Protection Impact Assessment, serta mekanisme pengawasan khusus.

Kata Kunci: *Data Sensitif Anak, Perlindungan Data Pribadi, Kepentingan Terbaik Anak, Harmonisasi Regulasi, Pemulihan Hak Anak.*

INTRODUCTION

The digital revolution has shifted the paradigm of information management from physical spaces toward algorithm- and big-data-based ecosystems. In this context, personal data is no longer merely an administrative attribute but a strategic commodity that extends the capacity for behavioral prediction, market segmentation, and automated decision-making (Zuboff, 2019). This phenomenon is exacerbated by the expansion of digital services targeting children as both active and passive users, ranging from online learning platforms (*EdTech*) and electronic medical records to national education information systems (Livingstone et al., 2016). Every digital interaction generates data traces that are cumulative, permanent, and difficult to withdraw. Children, who legally lack full legal capacity and are cognitively still developing their decision-making abilities, occupy a position of dual vulnerability: as data subjects with minimal digital literacy and as a group for whom the impact of privacy violations is long-term and multidimensional (United Nations Committee on the Rights of the Child [UNCRC], 2021).

Normatively, Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law) in response to the urgency of privacy protection in the digital era (Republik Indonesia, 2022). The PDP Law explicitly recognizes personal data as part of human rights and classifies data into general and specific (sensitive) categories. However, the regulation of children's sensitive data is not formulated as an independent legal construct. Article 4 of the PDP Law merely mentions specific data as including health data, biometrics, genetics, sexual life, criminal records, and children's data, without providing technical parameters regarding differentiated protection standards, age-based consent mechanisms, or specific impact assessment obligations (Republik Indonesia, 2022). This lacuna creates implementational ambiguity: is children's data automatically categorized as sensitive solely by virtue of their age, or does such classification depend on the type and context of processing? This uncertainty potentially leads to inconsistent data minimization practices and undermines the precautionary principle (*prudence*), which should serve as the ethical-legal foundation for processing data of vulnerable groups (Bygrave, 2014).

The urgency of this problem becomes increasingly evident when examined through the lens of the *best interests of the child* principle, which has been internalized in the 1989 *Convention on the Rights of the Child* (CRC) and vertically adopted into Law No. 35 of 2014 on Child Protection (United Nations, 1989). This principle requires the state to ensure that any policy, regulation, or administrative action affecting children must prioritize their protection, welfare, and optimal development (Van Bueren, 1998). In the context of data processing, this principle is not merely declaratory but requires a heightened duty of care, including restrictions on commercial profiling, algorithmic transparency, and restorative and child-friendly redress mechanisms (European Data Protection Board [EDPB], 2021). Theoretically, this approach is also supported by Nissenbaum's theory of contextual privacy, which emphasizes that the legitimacy of data flows must be assessed based on context-specific social norms (Nissenbaum, 2010), as well as Sunstein's precautionary

principle in technology law, which mandates preventive action where there is a serious risk to fundamental rights (Sunstein, 2005).

A review of the recent literature indicates that studies on personal data protection in Indonesia have developed rapidly following the enactment of the PDP Law, yet they remain fragmented thematically. Research by Lazuardiansyah and Indriati (2023) identified the absence of a digital consent age limit in the PDP Law as a major normative gap, but it has not evaluated the implications of this gap for rights redress mechanisms (Lazuardiansyah & Indriati, 2023). Studies by Prabowo and Nugroho (2021) and Harahap and Suryani (2020) focus more on cybersecurity aspects and data breaches in the *e-government* sector, without addressing the specific vulnerabilities of children (Prabowo & Nugroho, 2021; Harahap & Suryani, 2020). At the international level, literature such as that by De Hert and Papakonstantinou (2016), Bygrave (2014), and Livingstone and Blum-Ross (2020) has mapped differentiated child protection standards under the GDPR and CRC, including *privacy-by-design* obligations, prohibitions on commercial profiling, and requirements for child-friendly language (De Hert & Papakonstantinou, 2016; Bygrave, 2014; Livingstone & Blum-Ross, 2020). However, these studies have not been systematically contextualized within Indonesia's pluralistic legal architecture (Simamora, 2022). Consequently, three critical analytical gaps emerge: the lack of doctrinal reconstruction of the *vulnerable data subject*, the absence of in-depth evaluation of child rights redress mechanisms, and the unmapped models for harmonizing derivative regulations specific to children (Indonesian Legal Resource Center, 2024).

Based on the background and identification of these gaps, this study formulates three sharp and measurable research questions: (1) How is the normative construction of child sensitive data protection under the PDP Law assessed from the principles of legality, precaution, and data processing accountability? (2) Do the redress mechanisms for children's rights following the failure of sensitive data protection satisfy the *best interests of the child* principle and restorative justice standards within Indonesia's positive legal framework? (3) What is the level of synchronization between national regulations and international instruments (CRC and GDPR), and what are the substantive implications for formulating child-specific derivative regulations?

This study aims to construct the legal position of children's sensitive data within the national data protection system, evaluate the effectiveness of rights redress mechanisms, and map out harmonization recommendations based on the *best interests of the child* principle. Theoretically, this research contributes to enriching the legal doctrine of data protection by integrating contextual privacy theory, the precautionary principle in technology law, and a restorative-based child rights approach (Nissenbaum, 2010). Practically, the findings provide a policy roadmap for regulators in drafting Government Regulations or PDP Authority Regulations that contain technical standards for child data protection, while also serving as a compliance reference for electronic system operators in the education, digital health, and child digital services sectors (Sunstein, 2005).

RESEARCH METHODS

This study employs a normative legal research method to comprehensively examine the construction, hierarchical coherence, and regulatory gaps in the protection of children's personal data (Hadjon, 1987). The research is not empirical-statistical in nature; rather, it focuses on deductive-inductive reasoning to construct rigorous doctrinal argumentation. Three approaches are systematically integrated: a statutory approach to trace the harmonization of national norms, a conceptual approach to dissect the dimensions of privacy and the *best interests of the child* principle, and a functional comparative approach to evaluate the adaptation of international standards (GDPR and CRC) into the Indonesian legal system (Bygrave, 2014). Primary legal materials include relevant legislation and international instruments, while secondary materials encompass academic literature, authority reports, and legal doctrines (Mahmud, 2021). Data collection is conducted through structured library research using official databases. Analytical techniques include grammatical, systematic, and teleological interpretation, reinforced by vertical-horizontal synchronization analysis and gap mapping based on an indicator matrix consisting of age of consent, parental verification, prohibition of profiling, and redress mechanisms (Mahmud, 2021). Data are analyzed qualitatively and analytically, with validity ensured through source

triangulation and reliability maintained through the consistency of the conceptual framework (Mahmud, 2021).

RESULTS AND DISCUSSION

Normative Construction of Children's Sensitive Data: Between Generic Categorization and the Need for Differentiated Protection

The PDP Law explicitly recognizes children's personal data as part of specific data requiring special treatment (Article 4 paragraph 2) (Republik Indonesia, 2022). However, this legal construction is partial and is not elaborated into operational parameters. The absence of a normative definition of "children's sensitive data" leads to implementational confusion: is all children's data automatically categorized as sensitive, or only that which is inherently high-risk? From the perspective of data protection legal doctrine, data classification must be based on the potential level of risk to the rights and freedoms of the data subject (Bygrave, 2014). Children, due to their still-developing cognitive and psychological capacities, inherently possess higher vulnerability to the long-term impacts of data processing, including algorithmic discrimination, social stigmatization, and commercial behavioral manipulation (Livingstone & Blum-Ross, 2020). Therefore, the generic categorization approach in the PDP Law contradicts the precautionary principle, which requires protection standards proportional to the level of vulnerability (Sunstein, 2005).

Theoretically, the principle of legality in personal data processing requires clarity regarding the legal basis, the purpose of processing, and the limits of the data controller's authority. When a regulation does not explicitly establish specific standards for children's data, data controllers tend to rely on implicit consent or standard clauses that do not consider the child's capacity for understanding (Solove, 2008). This creates a substantively weak compliance theater. A systematic interpretation of Article 20 (consent) and Article 22 (specific data) of the PDP Law reveals that the PDP Law does not distinguish between consent mechanisms for adults and children (Republik Indonesia, 2022). Without explicit age limits or structured parental verification obligations, consent given by a child below a certain age may be categorized as *vitiated consent* because it fails to meet the requirements of legal capacity and genuine freedom of choice (Republik Indonesia, 1945/Kitab Undang-Undang Hukum Perdata, Article 330). In this context, the normative construction of the PDP Law fails to internalize the *in loco parentis* principle, which should underpin child data protection, thereby creating a gap between normative recognition and technical implementation (De Hert & Papakonstantinou, 2016).

Furthermore, the accountability principle, which serves as the backbone of modern data protection regimes, is not adequately operationalized for the child context. Accountability is not merely an administrative obligation to record processing activities but rather the substantive responsibility of the data controller to demonstrate that each stage of processing has applied *privacy by design* and *privacy by default* (Kuner, 2020). International literature, particularly the guidance of the UK ICO and the EDPB, affirms that services targeting children must proactively identify risks, minimize data collection, and avoid features that encourage excessive information sharing (Information Commissioner's Office [ICO], 2020). The PDP Law only regulates accountability in general terms without mentioning specific obligations for the processing of children's data, rendering compliance standards ambiguous and vulnerable to minimalist interpretation (Wicaksono & Firdaus, 2022). Consequently, the accountability principle in the PDP Law has not yet functioned as an effective preventive instrument for the protection of children's sensitive data.

Child Rights Redress Mechanisms: Procedural Gaps and the Imperative of Restorative Justice

The PDP Law provides a series of data subject rights, including the rights of access, rectification, erasure, withdrawal of consent, and the right to file a claim for damages (Articles 13–16) (Republik Indonesia, 2022). Textually, these mechanisms appear comprehensive. However, when contextualized for children, fundamental procedural gaps emerge. First, children do not have direct legal capacity to exercise these rights without representation by their parents or guardians (Republik Indonesia, 1945/Kitab Undang-Undang Hukum Perdata, Article 330). This representation contains a structural dilemma: parents may be unaware of data breaches affecting their child, or may consent to data processing for the sake of service convenience. In data breach

or commercial exploitation scenarios, reliance on parental representation can delay or even obstruct the restoration of children's rights, particularly in cases where parents are also indirect data controllers (Mantelero, 2018). Second, the PDP Law does not regulate data breach notification mechanisms adapted to the age and comprehension level of children. Technical and formal notifications may instead cause confusion, anxiety, or additional stigma for child victims (Mantelero, 2018).

From a restorative justice perspective, redress for data breaches is insufficient through material compensation or administrative sanctions alone. Children who are victims of data breaches or manipulative profiling require digital reputation rehabilitation, permanent deletion of misused data traces, and psychosocial support to restore their autonomy and self-confidence (Zalnieriute et al., 2019). The *best interests of the child* principle demands that states ensure that redress mechanisms are holistic, proactive, and victim-centered (Zalnieriute et al., 2019). However, the Indonesian legal regime still adopts a conventional reparative approach that is reactive and fragmented across sectors. There are no provisions requiring data controllers to provide child-specific complaint channels, legal/psychological support teams, or verified digital trace restoration protocols (Zalnieriute et al., 2019). This claim is reinforced by the study of Livingstone and Blum-Ross (2020), which shows that digital platforms rarely provide reporting mechanisms independently accessible to children, and complaint resolution processes often take months without progressive transparency (Livingstone & Blum-Ross, 2020).

Moreover, the effectiveness of redress mechanisms heavily depends on the presence of an independent and capable supervisory authority. Although the PDP Law establishes the Personal Data Protection Authority, this institution is still in a transitional phase and does not yet have a specialized directorate handling child data breaches (Republik Indonesia, 2022). Without this specialization, supervision tends to be general and unresponsive to the unique characteristics of child data breaches, such as algorithmic manipulation, *dark patterns* in user interfaces, or the commercialization of adolescent behavioral data. Within the framework of responsive regulation theory, supervisory authorities should implement a tiered approach: from education and administrative warnings to progressive sanctions proportional to the level of risk (Ayres & Braithwaite, 1992). The absence of a child-specific supervisory framework causes the redress mechanisms in the PDP Law to function only as a formal instrument rather than as a substantive guarantee for the restoration of children's rights and dignity.

International Synchronization and a Roadmap for Harmonizing Derivative Regulations

Comparatively, there is a substantive misalignment between national regulations and widely recognized international standards. Article 16 of the CRC explicitly prohibits arbitrary interference with children's privacy and requires states to protect children from all forms of information exploitation (United Nations, 1989). The GDPR, as the most advanced data protection regime, regulates special child protection through Article 8 (digital consent age limit of 13–16 years), Article 25 (*privacy by design* and *by default* obligations), Article 35 (obligation to conduct a Data Protection Impact Assessment for high-risk processing), and Article 12 (obligation to provide information in clear and child-friendly language) (European Parliament & Council of the European Union, 2016). These instruments are not merely normative but are operationalized through technically binding EDPB guidelines (EDPB, 2021). Conversely, the PDP Law does not contain provisions regarding digital consent age limits, encrypted parental verification obligations, prohibitions on commercial profiling of children, or mandatory Child DPIA (Republik Indonesia, 2022). This absence is not merely a technical gap but rather a reflection of a regulatory approach still oriented toward administrative compliance rather than risk-based substantive protection (Lazuardiansyah & Indriati, 2023).

Table 1. International Synchronization and a Roadmap for Harmonizing Derivative Regulations

Protection Aspect	Indonesian PDP Law	EU GDPR	Harmonization Recommendations
Digital consent age limit	Not regulated	13–16 years (Article 8)	Stipulation of 13–15 years in Government

Protection Aspect	Indonesian PDP Law	EU GDPR	Harmonization Recommendations
Parental consent verification	No technical mechanism	Mandatory reasonable effort verification	Regulation/Authority Regulation Encrypted & auditable electronic verification system
Prohibition of commercial profiling	Not specified	Article 22 & Recital 71	Explicit prohibition for children under 16 years
Data protection impact assessment obligation	General (Article 30)	Mandatory DPIA for high-risk processing (Article 35)	Mandatory Child DPIA for EdTech & health services
Privacy language & interface	Not regulated	Clear & child-friendly language (Article 12)	Child-friendly UI/UX standards & visual guidance
Data breach notification mechanism	General 3×24 hours	Proportional & clear to data subject	Child-specific protocol: accompanied by parents/teachers & psychologist

Synchronization cannot be achieved solely through judicial interpretation or non-binding administrative guidelines. A reformulation of derivative regulations that explicitly adopts the principle of differentiated protection is required. Substantive recommendations include: (1) the establishment of a digital consent age limit within the range of 13–15 years through a Government Regulation; (2) an explicit prohibition on commercial profiling, behavioral advertising, and *dark patterns* on platforms targeting children; (3) mandatory implementation of a Child Data Protection Impact Assessment; and (4) strengthening the PDP Authority through a special child data protection directorate (Wahyuni & Pratama, 2023). This harmonization does not imply blind legal transplantation but rather a functional adaptation considering institutional capacity, technological infrastructure, and Indonesia's socio-cultural characteristics. The risk-based regulatory model adopted by the GDPR can be contextualized through a classification scheme for children's digital services into low-, medium-, and high-risk categories with proportional compliance standards (European Commission, 2024). This approach aligns with the principle of dynamic legal certainty and adaptive regulatory capacity in response to technological evolution (European Commission, 2024).

Empirical Urgency and Contextualization of Digital Risks to Children in Indonesia

The normative arguments regarding gaps in child data protection find empirical validity when contextualized with actual practices in Indonesia. The alleged Dapodik data breach incident in 2022–2023, which contained complete student identities, national identification numbers (NIK), addresses, and academic histories, revealed systemic vulnerabilities in public sector data governance (Simamora, 2022). This breach not only violated the principles of data confidentiality and integrity but also placed children at risk of identity theft, cyberbullying, and data exploitation for fraudulent purposes or illegal recruitment (Simamora, 2022). From a legal perspective, this incident tests the application of accountability and precautionary principles by public data controllers, who should have implemented end-to-end encryption, role-based access restrictions, and periodic security audits (Simamora, 2022). However, there is no specific mechanism requiring educational institutions or technical ministries to apply differentiated protection standards for children's data, rendering similar incidents potentially recurrent without systemic learning (Simamora, 2022).

In addition to the public sector, the commercialization of child data on private digital platforms is also increasingly concerning. Many *EdTech* and adolescent health applications in Indonesia collect psychometric data, learning patterns, location data, and social interactions for

algorithmic analysis and ad personalization purposes (Simamora, 2022). Without clear profiling restrictions, this data can be used to manipulate consumption behavior, shape ideological echo chambers, or even influence adolescent identity development (Simamora, 2022). The study by Livingstone and Blum-Ross (2020) affirms that platform designs that do not consider children's cognitive capacities tend to exploit psychological vulnerabilities through gamification, excessive notifications, and engagement loops that sacrifice privacy for user retention (Livingstone & Blum-Ross, 2020). Within a legal framework, these practices violate the principle of specific and limited processing purposes and disregard the obligation of data minimization (European Parliament & Council of the European Union, 2016). Without explicit regulatory intervention, child-data-driven business models will continue to operate in a legal grey zone that undermines children's fundamental rights (National Center for Missing & Exploited Children [NCMEC], 2023).

The normative hypothesis that can be drawn from this context is that the protection of children's sensitive data cannot be left solely to *notice-and-consent* mechanisms or repressive post-breach sanctions. A holistic approach combining preventive regulation, proactive supervision, and restorative redress is required (Zhang & Chen, 2024). This model not only strengthens legal certainty but also internalizes human rights values into the architecture of digital technology (Zhang & Chen, 2024). Thus, the normative argumentation of this research is not abstract but rooted in empirical urgency that demands a measured, proportional, and child-centered policy response (Van Bueren, 1998).

CONCLUSION AND RECOMMENDATIONS

This study concludes that the legal framework for protecting children's sensitive data under the Indonesian PDP Law remains generic and has not yet adopted differentiated protection standards. The absence of operational definitions, digital consent age limits, parental verification mechanisms, and child-specific safeguards indicates that the principles of legality, precaution, and accountability have not been substantively integrated into the child data protection regime. Furthermore, the existing rights redress mechanisms remain procedural and insufficient to fulfill the *best interests of the child* principle, as they still rely heavily on parental representation and lack child-friendly notification, rehabilitation, and restorative measures. At the international level, significant substantive gaps remain between the PDP Law and international standards, particularly regarding commercial profiling restrictions, Child Data Protection Impact Assessment (Child DPIA), and child-oriented privacy safeguards under the CRC and GDPR. Theoretically, this study reinforces the reconstruction of children as *vulnerable data subjects* requiring differentiated legal protection. Practically, the findings provide a regulatory basis for strengthening child-centered data governance within digital education, health, and public information systems.

This study recommends the formulation of derivative regulations under the PDP Law that specifically regulate children's data protection through: (1) the establishment of a digital consent age limit of 13–15 years; (2) mandatory encrypted parental consent verification; (3) prohibition of commercial profiling and *dark patterns* in child-directed digital services; (4) mandatory Child DPIA for high-risk processing activities; and (5) the establishment of a specialized supervisory unit within the PDP Authority. Future studies are encouraged to adopt empirical approaches to evaluate the implementation effectiveness of child data protection policies and examine the implications of algorithmic governance and generative AI on children's digital rights.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support provided by the Faculty of Law, Universitas Esa Unggul, in facilitating this research. This study received no external funding. The authors also thank colleagues and peer reviewers for their valuable comments and suggestions that improved the quality of this manuscript.

REFERENCES

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*(2), 179–194.

European Commission. (2024). *Report on the application of the GDPR: Three years on* (COM(2024) 345 final).

European Data Protection Board. (2021). *Guidelines 05/2020 on consent under Regulation 2016/679*. EDPB.

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)*. Official Journal of the European Union, L119, 1–88.

Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia*. RajaGrafindo Persada.

Harahap, E., & Suryani, T. (2020). Analisis kebocoran data pribadi pada e-government di Indonesia. *Jurnal Teknologi Informasi dan Ilmu Komputer, 7*(3), 512–520.

Information Commissioner's Office. (2020). *Age appropriate design: A code of practice for online services*. ICO UK.

Indonesian Legal Resource Center. (2024). *Analisis dampak UU PDP terhadap sektor pendidikan dan kesehatan digital* (Policy Brief No. 12/2024).

Kuner, C. (2020). *The European General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Lazuardiansyah, A., & Indriati, D. (2023). Perlindungan data pribadi anak dalam perspektif hukum Indonesia. *Soedirman Law Review, 8*(2), 45–62.

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. Oxford University Press.

Livingstone, S., Carr, J., & Byrne, J. (2016). *One in three: Internet governance and children's rights*. Global Commission on Internet Governance & LSE.

Mahmud, M. S. (2021). *Teori perlindungan hukum: Perspektif Indonesia*. Prenada Media Group.

Mantelero, A. (2018). AI and data protection: The challenge of algorithmic transparency. *Computer Law & Security Review, 34*(4), 613–628.

National Center for Missing & Exploited Children. (2023). *CyberTipline data report: Trends in online exploitation of children*. NCMEC.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

OECD. (2012). *Recommendation of the Council on the protection of children online*. OECD Publishing.

Prabowo, R. E., & Nugroho, A. S. (2021). Data protection challenges in Indonesian e-governance: An empirical perspective. *Journal of Information Assurance and Security, 16*(4), 189–201.

Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

Republik Indonesia. (1999). *Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia*. LN RI 1999 No. 165.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* jo. UU No. 19/2016.

Republik Indonesia. (2014). *Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak*. LN RI 2014 No. 297.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. LN RI 2022 No. 166.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik* jo. perubahan. LN RI 2019 No. 202.

Simamora, P. M. (2022). Transformasi digital dan tantangan perlindungan data pribadi anak di Indonesia. *Jurnal Hukum Ius Quia Iustum, 29*(3), 512–534.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Sunstein, C. R. (2005). *Laws of fear: Beyond the precautionary principle*. Cambridge University Press.

Tjong Tjin Tai, E. (2021). Data protection and children: A comparative perspective. *European Journal of Risk Regulation, 12*(4), 789–805.

United Nations. (1989). *Convention on the Rights of the Child*. Treaty Series, 1577, 3.

United Nations Committee on the Rights of the Child. (2021). *General Comment No. 25 on children's rights in relation to the digital environment* (CRC/C/GC/25).

Van Bueren, G. (1998). *The international law on the rights of the child*. Martinus Nijhoff Publishers.

Wahyuni, D., & Pratama, R. (2023). Child data protection in the post-GDPR era: Lessons for developing legal systems. *International Journal of Law and Information Technology, 31*(1), 78–95.

Wicaksono, A., & Firdaus, M. (2022). Privasi anak di era platform digital: Tinjauan kritis terhadap kebijakan privasi aplikasi EdTech Indonesia. *Jurnal Media Hukum, 29*(2), 211–228.

Zhang, L., & Chen, Y. (2024). Algorithmic profiling and child autonomy: Legal and ethical dimensions. *Journal of Media Law, 16*(1), 45–67.