



Protection of Children's Privacy Rights in the Digital Era: Legal Challenges to Social Media Use

Hanna Ade Ningtiyas ^{1*}, Budiyo¹

¹ Faculty of Law, Universitas Jenderal Soedirman, Purwokerto, Jawa Tengah, Indonesia

*Corresponding author: hanna.ningtiyas@mhs.unsoed.ac.id

Article History

Revised: 2026-08-15

Accepted: 2026-10-24

Published: 2026-10-31

Abstract: This study analyses the legal framework for the protection of children's privacy rights in social media use, focusing on Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law) and Indonesia's obligations under UNCRC General Comment No. 25 of 2021. Employing a normative legal approach that integrates statutory, comparative, case-based, and conceptual methods, the study identifies five structural weaknesses in the PDP Law: inconsistent age definition for children (Article 6), absence of an explicit algorithmic profiling prohibition (Article 57), lack of operationalised age-verification standards, weak child data-erasure rights (Article 36), and institutional vacuum in supervisory authority (Article 58). A three-jurisdiction comparative analysis Indonesia, the European Union, and the United States places Indonesia in the weakest position across eight protection dimensions. Jurisprudential analysis of Irish DPC v. TikTok (€345 million, 2023) and FTC v. YouTube/Google (USD 170 million, 2019) empirically demonstrates a "two-tier privacy standard" applied by global platforms owing to Indonesia's weak enforcement environment. Curriculum analysis reveals that the Merdeka Curriculum has not integrated digital privacy rights within formal human rights education. This study introduces the "Digital Child Privacy Protection Pyramid" as a novel analytical framework integrating four complementary layers: strong regulation, independent oversight, platform accountability, and literacy-education-empowerment.

Keywords: Personal Data Protection; Children's Privacy Rights; Social Media.

Introduction

In the framework of international law, the normative foundation for privacy protection is established by Article 12 of the 1948 Universal Declaration of Human Rights (UDHR) and Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR). These provisions are then specifically applied to children through Article 16 of the 1989 UN Convention on the Rights of the Child (CRC), an instrument that has been ratified by 196 countries, including Indonesia, through Presidential Decree Number 36 of 1990.

Article 16 of the CRC emphasizes two fundamental rights: no child should be subjected to arbitrary interference with their private life, and children have the right to legal protection against such interference. This provision creates a positive obligation for the state to take legislative, administrative, and other measures to make this protection real and responsive to changing contexts, including the digital context.

In response to massive digitalization, the UN Committee on the Rights of the Child issued General Comment No. 25 of 2021 on the Rights of the Child in the Digital Environment, the most authoritative soft law instrument interpreting children's rights in the digital age. This General Comment explicitly requires countries to implement age-appropriate consent mechanisms for processing children's data, protect children from commercial profiling and monitoring, mandate privacy by design and privacy by default in platform architecture, ensure children's digital privacy literacy, and guarantee children's rights to effective remedies when their privacy is violated.

Under Indonesia's national legal framework, child privacy protection is based on several pillars: Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, Law Number 35 of 2014 on Child Protection, Law Number 27 of 2022 on Personal Data Protection (PDP Law), and Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Information and Electronic Transactions (ITE Law). Normatively, this framework reflects Indonesia's commitment to protecting children's privacy, including in digital spaces.

Despite the existing normative framework, the real-world situation shows a pretty significant gap. The EU Kids Online 2020 report, which surveyed 25,000 children across 19 countries, found that one in three kids reported negative experiences online, with privacy risks being one of the most common issues (Smahel et al., 2020).

Indonesia, with more than 185 million internet users and 167 million of them actively using social media in 2023, presents a digital ecosystem that's highly vulnerable for children. Global platforms like TikTok, with 113 million Indonesian users (the third largest in the world), and YouTube operate without significant regulatory hurdles, while the data protection authority hasn't even been established more than two years after the PDP Law was passed. The gap between the high number of child users and weak law enforcement is a situation that can't be allowed to continue.

Concrete cases of child privacy violations by global platforms give a very clear picture. The Federal Trade Commission (FTC) slapped a historic \$170 million fine on Google/YouTube in September 2019 for collecting data on children under 13 without parental consent. In 2023, the Irish Data Protection Commission (DPC) fined TikTok €345 million for GDPR (The General Data Protection Regulation) violations in handling children's data, including unsafe default privacy settings. These cases empirically show that child privacy violations by global platforms are not a theoretical risk, but a real, large-scale threat.

The phenomenon of sharenting adds a layer of irony where the threat to privacy actually comes from the parents themselves. On average, a child has 1,300 photos of themselves posted by their parents on social media before they turn 13 years old (Steinberg, 2017). Lupton and Williamson (2017) warn that the era of dataveillance creates a permanent 'digital dossier' for children even before they can give consent, a reality that fundamentally conflicts with a child's right to control their own digital footprint (Lupton & Williamson, 2017).

The gap identified in this study reflects a systemic failure in the transmission of digital values and norms to the younger generation. The current Merdeka Curriculum includes an Informatics subject that formally covers digital security topics; however, content analysis of the curriculum conducted by the team's members shows that the aspect of digital privacy rights as part of human rights is barely articulated in the existing competency standards. Learning about digital safety tends to focus solely on technical-operational aspects, such as how to create a strong password and how to avoid viruses. As a result, the human rights dimension and the legal dimension that form the foundation of digital ethics are left completely untouched. Consequently, students may know how to technically use privacy features, but do not understand why privacy matters as a fundamental right protected by law. This is what is referred to as "digital skills without digital rights literacy" — digital skills without digital rights literacy (Livingstone et al., 2018).

A systematic search of Indonesian legal literature reveals several significant research gaps. First, no study has yet conducted a systematic article-by-article analysis of the PDP Law's provisions concerning children and directly linked it to Indonesia's obligations under UNCRC General Comment No. 25 of 2021. Second, a comparative study of three jurisdictions combined with analysis of concrete jurisprudence such as Irish DPC v. TikTok (2023) and FTC v. YouTube/Google (2019) has never previously been conducted within the context of Indonesian law. Third, the dimension of sharenting as a privacy violation originating from parents has been very rarely examined from the perspective of Indonesian children's rights law. Fourth, no study has yet integrated the perspective of formal education—particularly curriculum analysis and teacher capacity—into the legal study of digital children's privacy protection in Indonesia. A purely legal-centric approach produces recommendations

that are difficult to operationalize because it disregards the reality of the education ecosystem as the front line in building children's rights awareness. This study directly fills that gap through the contribution of team members from the field of education.

This research covers three fundamental aspects. First, it provides the first analytical mapping that systematically examines five specific structural weaknesses of PDP Law No. 27 of 2022 from Indonesia's obligations under UNCRC General Comment No. 25 of 2021. Second, it offers a cross-jurisdictional jurisprudence analysis (*DPC v. TikTok*, €345 million, 2023; *FTC v. YouTube/Google*, USD 170 million, 2019) and connects it with Indonesia's law enforcement context for the first time. Third, it develops a "Digital Child Privacy Protection Pyramid" that integrates international law, national law, platform responsibility, child literacy, and formal education as a new comprehensive framework.

Based on the discussions above, this study aims to: (1) analyze the international and Indonesian legal framework regarding the protection of children's privacy on social media comprehensively, with a special focus on Law No. 27 of 2022 on PDP and UNCRC General Comment No. 25 of 2021; (2) identify and analyze the main legal challenges in enforcing children's privacy protection in the digital era, including through cross-jurisdictional case law studies; (3) integrate the perspectives of education practitioners in analyzing the effectiveness and operationalization of children's privacy rights protection; and (4) formulate detailed, operational, and complementary legal and educational policy recommendations.

Research Methods

This study uses a normative legal research approach, which is research that examines law as a set of norms using library materials as the main data. Normative legal research is the most suitable approach when the main goal of the study is to find coherence truth, whether existing legal rules align with higher norms and are consistent with each other (Marzuki, 2021). This research is descriptive-analytical-prescriptive in nature: it describes the existing normative framework, analyzes it critically, and provides policy recommendations based on the findings of the analysis.

As a methodological innovation, this study adopts an interdisciplinary approach that combines perspectives from law, education, and the experiences of field education practitioners. The integration of these three perspectives is carried out through analytical triangulation, where each finding from legal analysis is tested for its relevance to the educational context and vice versa. This approach responds to criticism that research on children's digital rights, when purely legal-doctrinal, often produces recommendations that are not contextual and difficult to implement (Livingstone & Third, 2017).

This research integrates four legal research approaches in a synergistic way. The statute approach examines all relevant legal instruments from the 1948 UDHR to the 2022 PDP Law. The comparative approach compares the legal framework for child privacy protection in three jurisdictions: Indonesia, the European Union, and the United States. The case approach analyzes the rulings in Irish *DPC v. TikTok* (2023), *FTC v. YouTube/Google* (2019), and *ICO v. TikTok UK* (2023). The conceptual approach looks into concepts like privacy by design, right to erasure, informed consent, algorithmic profiling, and the best interest of the child.

The collection of legal materials was carried out through a systematic literature study using UN Treaty Collection, EUR-Lex, HeinOnline, JDIHN, Google Scholar, Scopus, and SINTA. The analysis was conducted using qualitative analysis techniques that integrate five legal interpretation methods: (1) grammatical, (2) systematic, (3) teleological, (4) comparative, and (5) futuristic. In the education dimension, a content analysis was carried out on the Merdeka Curriculum documents, especially the learning outcomes for Informatics and PPKn, to identify to what extent children's digital privacy rights are accommodated in Indonesia's formal education system.

Results and Discussion

International Legal Framework: A Comparative Normative Analysis

1. Evolution of International Instruments and Their Implications for Indonesia

The protection of children's privacy in international law has evolved in three stages. The first stage (1948–1989) covered general protection through the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). The second stage (1989–2020) was marked by the birth of the Convention on the Rights of the Child (CRC), which specifically addressed children's privacy protection, though it didn't touch on the digital dimension. The third stage (2021–present) is marked by the United Nations Convention on the Rights of the Child (UNCRC) General Comment No. 25 of 2021, which comprehensively regulates children's rights in the digital environment.

A substantive analysis of General Comment No. 25 reveals at least seven positive obligations that directly test the adequacy of Indonesia's PDP Law: (a) paragraphs 67–71 require effective age verification mechanisms for processing children's data; (b) paragraphs 72–74 prohibit algorithmic profiling that exploits children's vulnerabilities; (c) paragraphs 63–66 prohibit commercial monitoring of children without informed consent; (d) paragraphs 80–83 require effective remedies, including data deletion; (e) paragraph 40 mandates privacy by design and by default in platform architecture; (f) paragraphs 31–35 require the state to take an active role in children's digital literacy education; and (g) paragraphs 86–90 require international cooperation between countries in enforcing children's privacy laws. Of these seven obligations, the PDP Law only partially fulfills one obligation through Article 36, while the other six are not accommodated.

This raises the question of whether General Comment No. 25 can realistically be implemented by developing countries like Indonesia, which is still struggling to build basic data protection institutional infrastructure. This normative paradox—the gap between the ambitions of the General Comment and the capacity to implement it—is a structural challenge that can't be solved just by adopting norms; it requires international technical support, technology transfer, and systematic strengthening of institutional capacity. The Committee's analysis in General Comment para. 4 acknowledges the existence of a 'digital divide' between countries, but it doesn't provide concrete mechanisms to address that gap in implementation capacity. This is a substantive weakness of the international soft law instrument that needs to be explicitly identified in legal studies.

UNCRC General Comment No. 25 contains at least 23 paragraphs directly related to the protection of children's privacy, covering data protection (paras. 67–71), protection from surveillance (paras. 63–66), protection from profiling (paras. 72–74), and the right to remedy (paras. 80–83). The depth and breadth of these provisions normatively go far beyond the provisions of Indonesia's PDP Law, a finding that by itself serves as evidence of a significant legal gap that will be analyzed further.

2. GDPR and the Children's Code: A Critical Comparative Analysis

The EU's GDPR is recognized as the gold standard for data protection, and its relevance to Indonesia is twofold: as a comparative model to assess the adequacy of national regulations and as a regulation that directly applies to platforms serving EU citizens, creating an incentive for platforms to implement GDPR standards globally. Article 8 of the GDPR sets the minimum age for independent digital consent at 16, with member states having the flexibility to lower it to 13.

The GDPR still leaves room for member countries to implement certain provisions differently, including those most relevant to children, which creates legal uncertainty for data controllers, parents, and the children themselves (Lievens & Verdoodt, 2018).

However, a critical analysis of the GDPR reveals several limitations that are relevant to the Indonesian context. First, the fragmentation of age limits among member countries (12 countries choosing 16 years, 10 countries choosing 15 years, 5 countries choosing 13 years) creates inconsistencies in protection that platforms could exploit by choosing the jurisdiction with the most

lenient standards. Second, the GDPR's parental consent mechanism assumes the involvement of parents who are digitally savvy and active, an assumption that is quite problematic in Indonesia where parental digital literacy is still very low. Third, the GDPR was designed in the context of a mature legal ecosystem with strong DPAs and an established culture of legal compliance, a situation very different from Indonesia. Adopting the GDPR model can't be done copy-paste style; it needs to go through a contextual adaptation process that considers the existing institutional and social capacity limitations.

The UK's Children's Code (Age Appropriate Design Code), which has been in effect since September 2021, is currently the most innovative regulatory tool because it takes a design approach rather than just a consent-based approach. The fifteen mandatory standards it sets—like putting best interests first (Standard 1), having strong privacy settings by default (Standard 4), minimizing data (Standard 5), and banning dark patterns (Standard 12)—represent a paradigm shift from "tell and consent" to "design for safety."

The "design for safety" approach adopted by the UK's Children's Code resonates strongly with experiences on the ground. Children actively seek ways to circumvent platform restrictions, such as changing their date of birth, using a parent's account, or creating a new account when one is blocked. This shows that protection approaches relying on children's active compliance (opt-in protection) are not effective. Furthermore, it is more effective when protection is built directly into platform design, so that children are automatically protected without needing to take active action. In educational terms, this is analogous to the difference between "discipline by punishment" (disciplining through punishment after a violation occurs) and "discipline by design" (designing an environment that structurally minimizes violations). Indonesia needs to adopt a "privacy by design" philosophy, not only in platform regulation, but also in the design of digital environments used in schools.

3. Comparative Analysis of Three Jurisdictions

Here's a systematic comparison of eight aspects of child privacy protection in three jurisdictions studied in this comparative research. This analysis fills a gap in Indonesian legal literature, which so far has only compared two jurisdictions (Indonesia and the European Union) without including the dimension of actual case law.

Table 1. Systematic Comparison of Child Protection Regulations

Aspect	Indonesia (UU PDP 2022)	Uni Eropa (GDPR + Children's Code)	AS (COPPA 1998)
Child Age Limit	17 yrs old (Art. 6(2)) – inconsistent with the Child Protection Law: 18 yrs old	18 years general; 13–16 years digital consent	13 yrs (digital platform consent)
Consent Mechanism	Parental consent (Art. 6(2)); no technical verification standards	Verifiable parental consent + DPIA required	Verifiable parental consent; detailed technical standards
Profiling Ban	There's no explicit prohibition for children (Ps. 57)	Prohibited without a strong legal basis (Art. 22 GDPR); dark patterns are banned (Children's Code)	Prohibited for children's behavioral advertising
Right to Delete Data	General (Ps. 36); no special priority for children	High priority data is collected during childhood (Ps. 17(1)(f))	Must delete at parents' request anytime
Privacy by Design	Not explicitly regulated	Mandatory (Art. 25 GDPR + 15 standards of the Children's Code)	Not explicitly required
Supervisory Authority	Not formed >2 years after the law was passed	Independent DPA required; cross-border EDPB	FTC with strong enforcement authority
Maximum Penalty	2% of revenue or Rp 60 billion (Art. 57)	4% of global revenue or €20 million	USD 51,744 per day per violation
Child Case Precedent	No precedent yet	DPC v. TikTok: €345 million (2023); ICO v. TikTok: £12.7 million (2023)	FTC v. YouTube/Google: USD 170 million (2019)

The analysis of the table above reveals a consistent pattern: Indonesia systematically occupies the weakest position in five of the eight dimensions of protection. More importantly, it raises the question of why this weakness is systemic in nature. The researchers' argument is that the legislative

process for the PDP Law was carried out without meaningful participation from the education community, child protection practitioners, and representation of children's own interests, so that the structural blind spots in the table are a logical consequence of a non-inclusive process. This finding reinforces the urgency of a public consultation mechanism involving the education community in drafting the PDP Law's implementing regulations. Children's privacy cannot be separated from the misuse of children's personal data by third parties, which constitutes a legal problem (Rohmansyah et al., 2023). This is because personal data encompasses any information that can be used to identify or contact a particular individual, whether that information is collected directly or indirectly through electronic and/or non-electronic methods (Anggen Suari & Sarjana, 2023).

Structural Weaknesses of PDP Law No. 27 of 2022

1. Age Limit Inconsistency (Article 6 Paragraph 2)

Article 6 paragraph (2) of the Personal Data Protection Law states that the processing of children's personal data must obtain consent from parents or guardians. The explanation of this article defines "child" as an individual under 17 years old and/or unmarried. This definition creates a serious inconsistency with Article 1 point 1 of the Child Protection Law No. 35 of 2014, which defines a child as someone under 18 years old, including a child still in the womb. As a result, a 17-year-old teenager, who is still considered a child under the Child Protection Law, no longer gets special protection in the form of mandatory parental consent under the Personal Data Protection Law.

This inconsistency in age limits isn't just a matter of editorial technicalities. From the perspective of children's rights law, having a consistent definition of "child" across all national legal instruments is a fundamental prerequisite for a coherent child protection system. Comparing this with the GDPR shows that the European Union consistently defines a child as anyone under 18 for general protection purposes, while also setting separate rules for digital consent age (13–16 years according to Article 8). The general protection age limit and the digital consent age limit should not be confused. Harmonizing the age limits between the Personal Data Protection Law and the Child Protection Law is an urgent legal necessity.

The inconsistency in age limits between the PDP Law (17 years old) and the Child Protection Law (18 years old) has a direct impact that I can see at school. 12th-grade high school students are usually 17–18 years old. Under the current PDP Law, a 12th grader who is 17 years old is theoretically outside the special child protection of the PDP Law, even though they are still in high school, under the supervision of parents and teachers, and very vulnerable to digital manipulation. Students like this are the most active on social media and are the most exposed to serious privacy risks, such as data collection for job or scholarship recruitment that can involve potential data-based discrimination. The lack of protection for the 17–18 age group is a real gap that needs to be addressed immediately.

Legally, this inconsistency creates a loophole that platforms can exploit. When a platform argues that a 17-year-old user isn't considered a 'child' under the PDP Law, the obligation to get verifiable parental consent doesn't apply, even though the Child Protection Law still classifies them as children in need of protection. This situation creates what legal theory calls 'norm fragmentation,' a misalignment of rules within a single national legal system that weakens the overall protective power of the system.

2. Lack of Explicit Ban on Algorithmic Profiling of Children (Article 57)

Article 57 of the PDP Law only generally regulates that automated decision-making that has a significant impact on data subjects can only be done with explicit consent. This provision does not distinguish between adult and child data subjects and does not include a substantive ban on profiling designed to exploit children's psychological vulnerabilities. Compare this with Article 22 of the GDPR, which substantively prohibits profiling that produces significant effects on children, and the Children's Code, which bans psychological manipulation techniques (dark patterns) against children.

Social media platform algorithms systematically identify and exploit children's psychological vulnerabilities, including their desire for social validation, to maximize engagement that benefits the platform commercially (McDonald & Cranor, 2008). Without an explicit ban, the PDP Law can't prevent such exploitative practices.

Through an umbrella review of 27 studies published between 2019–2021, it was found that the impact of social media use on psychological well-being is very diverse and individual, but psychologically vulnerable teens were shown to experience more significant negative effects, especially from exposure to content curated by algorithms based on user profiles (Valkenburg, 2022).

Algorithmic profiling of children has a dimension that extends far beyond mere privacy risk. It constitutes a fundamental threat to children's developmental autonomy. From an educational psychology perspective, adolescent identity is in a stage of formation that is highly vulnerable to external influence. When algorithms constantly present "curated" content based on a child's psychological profile, reinforcing existing biases, narrowing exposure to a diversity of ideas, and creating echo chambers, it actively intervenes in that identity formation process. Failure at the stage of adolescent identity formation can result in "identity diffusion," which has long-term impacts on mental health. Algorithms that exploit adolescent identity vulnerabilities for the sake of commercial engagement do not merely violate privacy—they have the potential to cause ongoing developmental harm. Indonesian law needs to adopt this concept of "developmental harm" as part of the definition of protected children's privacy violations.

Although most studies find only a small link between digital technology use and teen mental health, the most rigorous research still spots patterns where teens with certain psychological vulnerabilities face clinically meaningful risks, so evidence-based protective regulations are still needed (Odgers & Jensen, 2020).

From a legal perspective, the weakness of Article 57 of the PDP Law causes Indonesia's regulations to get stuck in a consent-based regulation paradigm, where profiling can only be prevented if the data subject (or their parents) actively refuses. This paradigm is not adequate to protect children for two reasons: children do not have the same cognitive capacity as adults to assess the long-term risks of profiling, and 'consent' given under conditions of information asymmetry and digital dependency is not truly free consent. There needs to be a shift to harm-based regulation that bans certain algorithmic techniques proven to harm children's development, regardless of whether consent has been obtained.

3. The Absence of an Operationalized Age Verification Standard

Even though Article 6 paragraph (2) of the PDP Law requires parental consent for processing children's data, the PDP Law doesn't at all regulate how data processors should verify the user's age. Without an effective age verification mechanism, the obligation to get parental consent becomes a norm that's impossible to put into practice—good on paper but not effective in reality.

The issue of age verification is seen as a technical-legal challenge that no jurisdiction has managed to fully solve (Svantesson, 2017). The UK's Children's Code is more advanced, requiring platforms to implement age estimation proportionate to the level of data processing risk, using methods like document verification, machine-learning-based age estimation, or parental credit card confirmation.

The failure of age verification mechanisms is not just a technical issue, because it has very real educational impacts. In Indonesia, it's very common to find middle school students (ages 12-14) who have accounts on platforms that officially prohibit users under 13. They register with fake birth dates, and the platform doesn't perform any meaningful verification. What's more concerning is that some parents actively help their kids sign up with these fake details, using the excuse that 'so their child won't be left behind.' This shows a cultural and social dimension to age verification failures that can't be fixed just with technical regulations. Changing social norms through education is needed to convince parents that platform age restrictions aren't just arbitrary rules, but evidence-based

protections concerning the risks to child development.

4. Weaknesses of Children's Data Deletion Rights (Article 36)

Article 36 of the PDP Law regulates the data subject's right to request the deletion of their personal data. When it comes to children, the PDP Law has a significant weakness because it doesn't provide specific provisions that prioritize deleting data collected when someone was still a child. Article 17(1)(f) of the GDPR explicitly states that data must be deleted if collected in connection with information services for children, giving higher priority to data collected during childhood. Moreover, Article 36 of the PDP Law is subject to very broad exceptions that could make this right ineffective in practice.

Cross-disciplinary analysis reveals a very important dimension of children's right to data deletion that is often overlooked in purely legal studies: its implications for a child's future prospects. Data collected during childhood, impulsive social media posts, online behaviors reflecting developmental stages, and photos exposing vulnerabilities can potentially become a burden that a child carries into adulthood. Employers, colleges, and financial institutions are increasingly using past digital data as considerations in recruitment and selection decisions. Without a strong deletion right, a child who makes a digital mistake at 13 could face the consequences at 25. This isn't just a privacy issue—it's an intergenerational justice issue that the law needs to address by providing stronger and more accessible data deletion protections for kids.

5. Vacancy in the Supervisory Authority Institution (Article 58)

Article 58 of the PDP Law only states that supervision is carried out by an agency under the President; its establishment is regulated through a Presidential Regulation. More than two years after the PDP Law was passed in October 2022, the mentioned supervisory agency still hasn't been set up, which is very different from the GDPR that requires the creation of an independent Supervisory Authority with clear powers for investigation, enforcement, and issuing sanctions.

Without a strong and independent supervisory authority, all of the child privacy protection provisions in the PDP Law become norms that cannot be effectively enforced. The lack of an adequate supervisory institution is one of the main issues in the implementation of Indonesia's PDP Law (Dayang G et al., 2025). The success of Ireland's DPC in imposing a €345 million fine on TikTok was only possible because the DPC has a clear legal mandate, guaranteed independence, sufficient resources, and comprehensive investigative powers—all attributes that the Indonesian supervisory authority, which hasn't even been established yet, does not have.

Child-friendly data processing transparency can only happen if there is a supervisory authority actively pushing platforms to comply through audits, guidance, and consistent enforcement of sanctions, rather than just waiting for complaints from victims (Milkaite & Lievens, 2020).

Cross-Jurisdiction Jurisprudence Analysis and Its Implications for Indonesia

1. Irish DPC v. TikTok (2023): €345 Million and Two-Tier Privacy Standard

Jurisprudence analysis is a crucial dimension for understanding how legal norms are applied and enforced in practice. The Irish Data Protection Commission's (DPC) ruling against TikTok in September 2023 imposed a €345 million fine, one of the largest in the history of global child privacy law enforcement. The violations found included default public privacy settings for accounts of children under 13, the 'Family Pairing' feature that allowed unknown adults to link their accounts with children's accounts, and the failure to implement data protection by design as required by Article 25 of the GDPR.

From the perspective of Indonesian law, the DPC v. TikTok ruling carries highly important analytical implications that have not previously been examined. TikTok, which was fined €345 million in the European Union for violations occurring on its service for European users, is logically very likely to apply the same or even lower standards for Indonesian users, given the absence of GDPR-

equivalent regulation and the absence of any significant threat of sanctions. This reveals what may be called a "two-tier privacy standard," in which platforms apply higher standards in jurisdictions with strong enforcement and lower standards in jurisdictions with weak enforcement. Indonesia, with 113 million TikTok users (the third largest in the world), falls within the group of jurisdictions receiving this lower standard of protection—a condition that directly violates the principle of equality and non-discrimination under the UNCRC. This analysis reinforces the argument that establishing a strong supervisory authority in Indonesia is not merely an administrative necessity, but constitutes a human rights obligation.

2. FTC v. YouTube/Google (2019): USD 170 Million and Platform Denial Strategy

The FTC v. Google LLC and YouTube LLC ruling in September 2019 resulted in a \$170 million fine, the largest in COPPA history. YouTube was found to have collected children's user data through cookies and tracking technologies without verifiable parental consent and used it for personalized ads. From an Indonesian legal perspective, this case directly shows that platforms serving tens of millions of Indonesian child users have been proven to commit serious child privacy violations in a jurisdiction with strong law enforcement—and similar practices are likely to continue in Indonesia without obstacles.

Analytically, the FTC investigation found that YouTube actively marketed itself to advertisers as a platform to 'reach kids' while at the same time claiming to regulators that the platform 'isn't for kids,' a denial strategy that deliberately exploits regulatory gaps. Without proactive oversight authorities conducting investigations, strategies like this are really hard to detect and take action against. This strengthens the urgency of establishing Indonesia's Personal Data Protection Agency with the authority to conduct proactive investigations, not just reactive ones.

3. ICO v. TikTok UK (2023): Consistent Enforcement and Cross-Jurisdiction Deterrence

7 million to TikTok in April 2023 for processing data of children under 13 without proper consent and not complying with the Children's Code. This very significant ICO ruling happened because the violation occurred after a major sanction from the Irish DPC, meaning TikTok continued the same practices even after facing a big penalty in another jurisdiction. This proves that deterrence only works if enforcement is consistent across all the places a platform operates, not just in one jurisdiction.

Across disciplines, these three legal cases reveal a very important insight: platforms won't voluntarily implement higher protection standards than what the law requires. For the education community, this has a very tangible implication where teachers and parents can't rely on the "child-friendly privacy policies" that platforms claim to provide on their own. They need to equip themselves with legal knowledge about what regulations actually require so they can effectively advocate for children's privacy rights. This is where training on the legal side of digital privacy becomes really important—not just technical training on how to use platform security features, but a solid understanding of the rights protected by law and how to enforce them when they're violated.

The comparative analysis above reveals a highly concerning pattern, namely that Indonesia consistently occupies the weakest position across almost all dimensions of protection compared. However, more important than merely identifying the weaknesses is analyzing why these weaknesses occur structurally. The weakness of the PDP Law in protecting children is not merely due to negligence on the part of the legislators, but rather due to a legislative process carried out without meaningful participation from the education community, child protection practitioners, and representation of children's own interests. A law designed without input from those most affected will inherently contain blind spots that are only identified after the regulation has been implemented. This reinforces the argument for the importance of an inclusive public participation mechanism, including consultation with the education community, in the process of drafting the PDP Law's implementing regulations that specifically govern the protection of children.

Specific Legal Challenges: Sharenting, Profiling, and Cross-Border Jurisdiction

1. Sharenting: Analysis of Rights Conflicts and Normative Gaps

Sharenting brings up a conflict between two rights that are both legally protected: a child's right to privacy and parents' right to express themselves. In the context of the CRC, the best interests of the child principle requires that the child's interests be prioritized, even over the parents' interests. However, Indonesia's Child Protection Law doesn't explicitly set limits on what parents can post about their children on social media, creating a significant legal gap.

The practice of sharenting in Indonesia can potentially violate children's privacy rights protected by the Child Protection Law and the Personal Data Protection Law, mainly because parents often don't consider the best interests of the child when sharing photos, videos, or identity information on social media. Right now, there's no legal mechanism that explicitly gives children the right to sue their parents for this kind of privacy violation (Putri et al., 2025).

France offers an interesting model: civil law allows children to sue their parents for violating their personal life if the parents have disclosed information that harms the child's private life. The 'informed parenting' framework distinguishes between sharenting done with the child's best interests in mind (which needs to be educated, not banned) and exploitative or harmful sharenting that should be subject to penalties (Steinberg, 2017).

Sharenting within the school environment has unique dynamics that have not yet been adequately examined in Indonesian legal literature. WhatsApp groups for parents/guardians created by schools have, without anyone realizing it, become highly active sharenting ecosystems. Photos of school activities, videos taken during ceremonies, and even photos taken while exams are in progress are routinely shared in these groups without any consent mechanism from the students being photographed. Furthermore, some parents then repost this content to their own personal social media accounts, which are public in nature. On one hand, this constitutes a violation of students' privacy; on the other hand, there is no clear school policy governing this matter, nor is there any legal framework providing operational guidance for teachers and schools. This is a very real regulatory gap that needs to be filled urgently, not only through national-level legislation, but also through technical guidance for schools on managing student privacy in the digital era. Further information shows that 51% of American teenagers admit it is difficult to stop using social media even though they themselves want to reduce their use, and the majority believe that platform algorithms actively promote content that worsens how they feel about themselves—a finding that reinforces the urgency of regulating profiling based on child protection (Anderson et al., 2023).

The phenomenon of sharenting in schools described above shows an urgent need for a comprehensive and binding school privacy policy. In countries with more advanced data protection systems, every school is required to have a Data Protection Policy that regulates who can take photos of students, how and where photos can be shared, how consent from students and parents must be obtained, and who is responsible for compliance. In Indonesia, regulations need to be developed to require every educational institution to have a digital privacy policy referring to the PDP Law and international standards. Without intervention at the education institution level, even the strongest legal regulations won't effectively change behavior on the ground.

2. Algorithmic Profiling and Its Implications for Child Welfare

Algorithmic profiling allows platforms to deeply analyze children's digital behavior and predict their preferences, psychological vulnerabilities, and even mental health conditions. Social media platform algorithms actively use children's psychological profiles to maximize screen time (McDonald & Cranor, 2008). Under Indonesian law, Law No. 8 of 1999 on Consumer Protection implicitly prohibits misleading advertisements, including those that target children manipulatively, but there are no regulations that specifically ban algorithmic profiling and targeted advertising to children.

A more substantive analysis of algorithmic profiling must question the fundamental assumption underlying current regulation: can algorithmic profiling of children ever be "neutral" or

"beneficial"? Recent neuroscience research shows that the adolescent brain is highly responsive to social rewards (likes, views, followers) and vulnerable to the influence of algorithms optimized for engagement, which in many cases means optimizing for emotional response rather than for children's well-being. Algorithms that detect and exploit children's tendencies toward content about body image, appearance, or social comparison have the potential to actively worsen body image disorders and mental health. From a legal perspective, this means that algorithmic profiling of children should not be regulated solely through a consent-based mechanism, but must instead be regulated through substantive prohibition (harm-based regulation) that bans certain algorithmic techniques proven to harm children's development—regardless of whether consent has been obtained or not.

3. Cross-Border Jurisdiction Challenges

The social media platforms most used by Indonesian kids, TikTok (Cayman Islands/China), YouTube, and Instagram (United States), operate under different legal jurisdictions from Indonesia. When privacy violations occur, Indonesia faces three jurisdictional challenges: determining which law applies (conflict of laws), enforcing decisions against foreign entities without a formal legal presence in Indonesia, and coordinating between regulatory authorities across different jurisdictions. The GDPR's 'marketplace principle,' which requires any entity targeting EU citizens to comply with GDPR regardless of where it is based, is the most effective extraterritorial jurisdiction mechanism (Svantesson, 2017). Indonesia needs to adopt a similar principle: any platform targeting Indonesian users must comply with Indonesia's child protection standards under the PDP Law.

Educational Perspective on Enforcing Children's Privacy Rights: Analysis of Curriculum and Teacher Capacity

Content analysis of the Kurikulum Merdeka documents, especially the Learning Outcomes (CP) for Informatics and PPKn subjects at the high school level (Phase E and F), reveals a critical gap. The 'Digital Security' element in the Informatics CP focuses on technical-operational aspects (account security procedures, identifying cyber threats) without any learning outcomes that explicitly mention digital privacy rights as human rights protected by international and national legal instruments. This situation creates what is called 'digital skills without digital rights literacy' (Livingstone et al., 2018). Students understand how to use security features, but they don't understand that they have legal rights that can be claimed when their privacy is violated.

The gap in children's privacy literacy, where kids can use security features technically but don't understand the underlying laws, is a systemic issue found in many countries and can only be addressed through educational curricula that explicitly integrate human rights dimensions into digital security learning (Stoilova et al., 2021).

The PPKn subject, which formally teaches human rights, hasn't adapted its content to explicitly include children's digital rights. As a result, there's a fragmentation where students learn about human rights in PPKn and about digital technology in Informatics, but they are never explicitly brought together with the understanding that the human rights they learn fully apply in the digital spaces they use every day. This is a curriculum gap that needs to be addressed immediately as part of Indonesia's response to the obligations in General Comment No. 25, paragraphs 31–35.

At the teacher capacity level, field findings reveal that the majority of teachers don't have a proper understanding of the legal framework for protecting children's digital privacy. This isn't an individual fault, but rather a reflection of teacher education programs that haven't incorporated digital human rights law into their curriculum. As a result, when students' privacy is violated at school, teachers respond with informal ethical approaches rather than rights-based approaches, a difference that directly affects whether victims get effective remedies or not.

Digital Child Privacy Protection Pyramid: A New Analytical Framework

Based on all the analysis that has been done, this study tries to build a "Digital Child Privacy

Protection Pyramid" as a new analytical framework that identifies four complementary layers of protection.

The first layer (foundation) is strong regulation, comprehensive legal instruments that are consistent and equipped with effective enforcement mechanisms: the PDP Law along with its derivative regulations specifically governing child protection. The second layer is independent oversight, an independent personal data protection authority with technical expertise and cross-border authority. The third layer is platform responsibility—active obligations for digital platforms to implement privacy by design, age-appropriate design, and compliance mechanisms that can be audited.

The fourth (top) layer in this updated Pyramid framework is literacy, education, and empowerment—which encompasses not only digital education programs for children and parents as found in the previous version, but also: (a) integration of digital privacy rights into the formal education curriculum as a mandatory competency to be achieved, rather than merely supplementary material; (b) capacity building for education practitioners as agents of privacy literacy through continuous professional training programs that integrate legal, pedagogical, and technical dimensions; (c) a requirement for schools to have a binding digital privacy policy; and (d) mechanisms for children's participation in privacy policy processes that concern them. Through the integration of this educational dimension, the Digital Children's Privacy Protection Pyramid becomes a truly comprehensive and operational framework—not only regulating what platforms and the state may and may not do, but also empowering children themselves as active subjects who understand and can advocate for their digital privacy rights.

This Pyramid Framework has important methodological implications: evaluating a country's child privacy protection system shouldn't just measure the strength of its regulations (first layer), but must simultaneously assess all four layers. Indonesia currently has moderate regulations (first layer with five structural weaknesses), no oversight body (second layer), unmonitored platforms (third layer), and an inadequate curriculum with low teacher capacity (fourth layer). Interventions that only focus on improving regulations without strengthening the other three layers won't provide effective protection for children.

Integrated Policy Recommendations: Law and Education

The first and most urgent recommendation is the creation of a Government Regulation on the Protection of Children's Personal Data. This regulation should include harmonizing the definition of 'child' to 18 years old, consistent with the Child Protection Law, an explicit ban on algorithmic profiling that can harm children (not just based on consent), proportional minimum age verification standards referring to the UK's Children's Code model, an obligation for age-appropriate design for platforms, and specific provisions for stronger data deletion rights for data collected during childhood.

The second recommendation is the immediate establishment of an independent Personal Data Protection Agency with a dedicated division for child data protection, staffed with experts in law, child psychology, and digital technology; empowered to proactively investigate platforms that provide services to children, authorize sanctions that have a deterrent effect, and have the capacity for international cooperation with DPAs from other countries.

The third recommendation is the harmonization of regulations, which includes: amending the Child Protection Law to add a specific chapter on child protection in the digital space that accommodates UNCRC General Comment No. 25, adding explicit provisions in the Electronic Information and Transactions Law prohibiting the collection of children's data without consent, and coordinating regulations between the Ministry of Communication and Information, the Indonesian Child Protection Commission, the Ministry of Education and Culture, and data protection supervisory agencies.

The fourth recommendation constitutes an original contribution from the research team's members in the field of education, distinguishing this study from conventional legal research. The team's analysis of the Curriculum documents found that although the Informatics subject includes digital security topics, no learning outcome explicitly refers to digital privacy rights as a human right protected by law. To fill

this gap, revision of the learning outcomes (CP) for the Informatics subject is needed to incorporate competency in understanding digital privacy rights from a human rights perspective, along with the development of cross-subject teaching modules between Informatics and Civics (PPKn) that integrate the human rights legal dimension into digital security learning, the inclusion of digital children's privacy protection material within a comprehensive Digital Citizenship Education program, and the development of assessment instruments that measure not only technical digital skills but also understanding of digital privacy rights and responsibilities.

Another recommendation that likewise constitutes an original contribution from the field of education is the development of teachers as agents of digital privacy literacy. In addition, there is a need to strengthen structured international cooperation. Indonesia needs to actively engage in international forums such as the UN Committee on the Rights of the Child, the Internet Governance Forum (IGF), the Global Privacy Assembly, and the ASEAN Working Group on Data Privacy. Bilaterally, Indonesia needs to develop law enforcement cooperation agreements in the field of children's privacy with the United States and Ireland, the two countries that host the largest social media platforms. A multistakeholder approach involving the education community, civil society organizations, the technology industry, and children's representation must also become an integral component of national child privacy governance.

Conclusion

Based on the comprehensive analysis that has been conducted, a number of conclusions have been produced in this study.

First, with regard to the objective of analyzing the international and national legal frameworks, it was found that although Indonesia has ratified the CRC and issued PDP Law No. 27 of 2022, there is a significant gap between the normative standards of UNCRC General Comment No. 25 of 2021 and the provisions of the applicable PDP Law. Comparative analysis of the three jurisdictions proves that Indonesia consistently occupies the weakest position across the eight dimensions of protection analyzed.

Second, with regard to the objective of identifying legal challenges, this study identifies five critical structural weaknesses in the PDP Law, namely: inconsistency in the age limit (Article 6, paragraph 2), the absence of a prohibition on algorithmic profiling (Article 57), the absence of age verification standards, weaknesses in children's right to data erasure (Article 36), and an institutional void regarding the supervisory authority (Article 58). The jurisprudence of Irish DPC v. TikTok (€345 million, 2023) and FTC v. YouTube/Google (USD 170 million, 2019) empirically proves the existence of a "two-tier privacy standard," in which global platforms apply minimal standards in Indonesia due to the absence of equivalent regulatory barriers.

Third, with regard to the objective of integrating the perspective of education practitioners, curriculum analysis and field observation reveal two critical gaps that have thus far been overlooked in purely legal studies, namely: the education curriculum does not contain learning outcomes that explicitly teach digital privacy rights as human rights, and education practitioners generally do not possess adequate legal understanding to become effective agents of privacy literacy. This condition creates a situation in which millions of children use social media every day without any understanding of the rights that should be protecting them.

Fourth, with regard to the objective of formulating policy recommendations, this study offers a "Digital Children's Privacy Protection Pyramid" framework that integrates four complementary layers strong regulation, independent oversight, platform responsibility, and literacy-education-empowerment along with a number of integrated policy recommendations that are operational and measurable. This package of interventions must be implemented simultaneously to produce real change in the protection of children's privacy rights in the digital era.

Law and education are not two mutually substitutable approaches to protecting digital children's privacy; they are two sides of the same coin. Strong law without meaningful education will produce formal compliance without genuine behavioral change. Good education without adequate legal protection will empower children who then find their rights are not enforced. Only through synergy

between the two can Indonesia move from a condition of "protection on paper" toward "protection in real life."

This study recommends that the formulation of implementing regulations of the PDP Law specifically for child protection and the establishment of an independent supervisory institution be prioritized as an urgent agenda. To the Ministry of Primary and Secondary Education (Kemendikdasmen), it is recommended that regulations on Digital Privacy Policy in Education Units be developed promptly, and that the learning outcomes for Informatics and Civics (PPKn) be revised to incorporate the dimension of digital privacy rights. To the academic community, this study opens up a further agenda, such as empirical studies on the level of digital privacy literacy among high school teachers in Indonesia and comparative studies of sharenting regulations across ASEAN countries.

References

- Anderson, M., Faverio, M., & Gottfried, J. (2023). *Teens, Social Media and Technology* 2023.
- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142. <https://doi.org/10.38043/jah.v6i1.4484>
- Dayang G, S., Lase, S. P. O., & Putri K, A. K. (2025). Urgensi Pembentukan Lembaga Pengawas dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP. *Locus Journal of Academic Literature Review*, 4(2), 106–113.
- Lievens, E., & Verdoodt, V. (2018). Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation. *Computer Law and Security Review*, 34(2), 269–278. <https://doi.org/10.1016/j.clsr.2017.09.007>
- Livingstone, S., Mascheroni, G., & Staksrud, E. (2018). European Research on Children's Internet Use: Assessing the Past and Anticipating the Future. *New Media and Society*, 20(3), 1103–1122. <https://doi.org/10.1177/1461444816685930>
- Livingstone, S., & Third, A. (2017). Children and Young People's Rights in the Digital Age: An Emerging Agenda. In *New Media and Society* (Vol. 19, Issue 5, pp. 657–670). <https://doi.org/10.1177/1461444816686318>
- Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media and Society*, 19(5), 780–794. <https://doi.org/10.1177/1461444816686328>
- Marzuki, P. M. (2021). Metode Penelitian Hukum Edisi Revisi. In *Jakarta: Kencana*.
- McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 540–565.
- Milkaite, I., & Lievens, E. (2020). Child-Friendly Transparency of Data Processing in the EU: from Legal Requirements to Platform Policies. *Journal of Children and Media*, 14(1), 5–21.
- Odgers, C. L., & Jensen, M. R. (2020). Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. In *Journal of Child Psychology and Psychiatry and Allied Disciplines* (Vol. 61, Issue 3, pp. 336–348). <https://doi.org/10.1111/jcpp.13190>
- Putri, S. H., Heriamariaty, H., & Jalianery, J. (2025). Legal Analysis of Sharenting Practices in the Digital Era: Implications for Children's Privacy Rights in Indonesia. *Journal of Law, Politic and Humanities*, 5(4), 3142–3153. <https://doi.org/10.38035/jlph.v5i4.1712>
- Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilisasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAI: Jurnal Hukum Dan Pranata Sosial Islam*, 5(2), 1099–1110. <https://doi.org/10.37680/almanhaj.v5i2.3054>
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. In *EU Kids Online (Issue February)*. <https://doi.org/10.21953/lse.47fdeqj01ofo>
- Steinberg, S. B. (2017). Sharenting: Children's Privacy in the Age of Social Media. *Emory Law Journal*, 66(4), 839–884.

- Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online—a systematic evidence mapping. *Information Communication and Society*, 24(4), 557–575. <https://doi.org/10.1080/1369118X.2019.1657164>
- Svantesson, D. J. B. (2017). Solving the Internet Jurisdiction Puzzle. In *Oxford University Press*. <https://doi.org/10.1093/oso/9780198795674.001.0001>
- Valkenburg, P. M. (2022). Social Media Use and Well-Being: What We Know and What We Need to Know. In *Current Opinion in Psychology* (Vol. 45). <https://doi.org/10.1016/j.copsyc.2021.12.006>