Volume 3 Issue 1 (2026) 54-72
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v3i1.42
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

A Legal Analysis of Children's Personal Data Protection in AI-Based Education Platforms in Indonesia

Halek Mu'min[1*], Andri Herman Setiawan[2], Eko Siswo Adi Sahputra[3]
[1]INTI International University, Malaysia
[2]Universitas Sehati Indonesia, Indonesia
[3]Politeknik Siber Cerdika Internasional, Indonesia
Corresponding Author: I24029619@student.newinti.edu.my

ABSTRACT
This study aims to analyze the legal protection of children's personal data within AI-based educational platforms in Indonesia by addressing the following research questions: (1) How are children's data legally regulated under Indonesian law? (2) How do AI-based EdTech platforms implement data protection for children? (3) What are the risks of misuse of children's data? and (4) How adequate and effective are existing national regulations in safeguarding children's data? The study employs a normative-juridical methodology using statute approach, conceptual approach, and comparative approach with GDPR-K, COPPA, and AI Act as benchmarks. Data were analyzed qualitatively through regulatory review, policy documents, and platform privacy policies, complemented by quantitative assessment of compliance indicators, such as the presence of parental consent mechanisms, data minimization practices, and algorithmic audit procedures across 15 major EdTech platforms in Indonesia. Findings indicate that although Indonesia has established the Personal Data Protection Law (UU PDP) as the primary legal framework, it lacks specific provisions for children's data protection, particularly regarding automatic profiling, verifiable parental consent, algorithm audits, and restrictions on commercial data use. Comparative analysis highlights significant gaps relative to international standards, which emphasize preventive and risk-based protection. The study concludes that Indonesia requires derivative regulations specifically for children's data, technical guidelines for AI data processing, and an independent supervisory mechanism. Practically, these measures would enhance compliance, reduce data misuse, and ensure the best interests of the child in the digital education ecosystem.

Keywords: data protection, children, AI, education technology, regulation

Article received on 12-08-2025 — Final revised on 23-10-2025 — Approved on 19-12-2025

Introduction

Over the past ten years, the use of artificial intelligence (AI) technology in the education sector has grown rapidly and become a key driver of digital transformation in Indonesia. Children now utilize AI-based educational platforms for adaptive learning, automated testing, learning pattern analysis, and algorithm-based material recommendations. This technology enables teachers to provide personalized instruction to each student (K et al., 2024). Along with their benefits, AI platforms collect and process a wide range of children's personal data, including names, academic records, digital activity

history, learning preferences, and biometric data such as voice and face. The complexity of AI processing increases the risk of privacy breaches, user profiling errors, algorithmic bias, and data leaks. This is exacerbated by the rise in data breach incidents in Indonesia, including in the digital education sector, demonstrating that digital security systems are not yet fully capable of protecting children's data.

Indonesia already has Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which affirms that children are data subjects requiring special protection. Other laws, such as the Child Protection Law and the Electronic Information and Transactions (ITE) Law, also provide a legal framework regarding children's personal information. However, two significant issues arise. First, current regulations do not explicitly address the governance of children's personal data in educational AI platforms, which require stricter protection standards than traditional digital systems. Second, there are no technical guidelines regarding algorithm transparency, parental consent procedures, data security principles, processing limitations, and oversight mechanisms to prevent the risk of high-risk profiling (Nurmansyah et al., 2024).

In comparison, the European Union, through GDPR-K and the AI Act, and the US, through COPPA, have established strict standards for child data protection, including explicit parental consent, restrictions on automated profiling, and algorithm audits. With Indonesian regulations remaining general and yet to adopt similar preventive principles, concerns have arisen regarding the effectiveness of legal protections for children's personal data in the AI-based education ecosystem. This situation requires a thorough legal analysis to evaluate national regulations, AI platform practices, potential misuse of children's data, and the compliance of Indonesian laws with international standards (LiMengyang et al., 2025).

The use of artificial intelligence (AI)-based educational platforms offers significant opportunities to improve the quality of education in Indonesia, particularly through adaptive learning, automated assessments, and personalized content recommendations. However, the adoption of this technology raises serious concerns regarding the protection of children's personal data.

First, Indonesian laws and regulations do not yet specifically regulate the definition, scope, and methods of protecting children's data related to AI processing. Although the Personal Data Protection Law (PDP Law) recognizes children as special data subjects, this law does not specify data collection limits, permitted data types, data minimization principles, or limitations on the purpose of use. This lack of regulation has the potential to encourage platforms to collect excessive or sensitive data, such as biometric data and metadata about children's online activities (J. Zhang et al., 2023).

Second, the implementation of data protection principles in AI platforms remains weak. Parental consent mechanisms are often generic and not specific to children, while automated decision-making processes, such as academic assessments and learning recommendations, lack transparency and rarely have human oversight. This increases the risk of over-profiling, algorithmic bias, and decision-making that directly impacts children's development (Ai, 2022).

Third, the potential for misuse of children's data increases because AI platforms heavily utilize cloud computing and third parties, including cross-border data transfers, advertising use, and non-educational analytics. Without legally mandated risk mitigation mechanisms, platforms lack an obligation to recognize or mitigate these risks, unlike international regulations such as the European Union's AI Law, which classifies educational AI systems as high-risk (Xie et al., 2025).

Fourth, the effectiveness of national regulations remains limited. Although Indonesia has a PDP Law and regulations related to education and information technology, child data protection is not yet aligned with international standards such as GDPR-K and COPPA,

which regulate age of consent, the right to data erasure, prohibitions on automated profiling, and algorithmic audits. This gap raises doubts about whether national regulations are capable of ensuring the "best interests of the child" principle is met in the AI-based education ecosystem (Ningsih, 2023).

The novelty of this research lies in its specific focus on children's personal data protection in the context of AI-based educational platforms in Indonesia, an area that remains under-researched. Unlike previous studies that tend to discuss child data protection generally or examine digital regulations normatively, this research integrates normative legal analysis with conceptual and comparative approaches to assess the adequacy of the PDP Law, the Child Protection Law, and related regulations against international standards such as GDPR-K, COPPA, and the European Union's AI Law. This research highlights the unique risks arising from the use of adaptive learning algorithms, recommendation systems, and automated decision-making, including algorithmic bias, digital profiling, biometric data leakage, and potential commercial exploitation, and evaluates the legal liability of educational platforms. Thus, this study presents a comprehensive analysis never before conducted in Indonesia, while also providing practical recommendations for the development of derivative regulations, technical guidelines, and oversight mechanisms centered on the best interests of children in AI-based digital educational ecosystems.

Internationally, child data protection is governed by various regulations. The European Union's GDPR offers specific provisions for children through Article 8, which emphasizes child consent, the best interests of the child, purpose limitation, and the data minimization principle. In the United States, COPPA emphasizes parental consent, mandatory notification, and restrictions on data collection practices for children under 13. The European Union's AI Act classifies educational AI systems as high-risk and requires impact audits, risk assessments, algorithmic transparency, and human oversight. Both regimes place primary responsibility on digital service providers to protect children's data (Mudayat et al., 2025).

In Indonesia, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) recognizes children as special data subjects. However, several studies (Sinta, 2023), (Mahfud, 2022), and (Rachmadewi, 2024), highlight regulatory gaps related to the management of children's data on AI-based platforms, including a lack of guidelines on data collection limits, age verification mechanisms, protection against machine learning models, and automated decision-making processes. EdTech platforms and educational AI systems are increasingly utilizing behavioral data, learning preferences, academic history, and biometric data such as facial recognition for digital attendance (Supriyadi, 2023). Reports indicate that more than 72% of global digital education platforms potentially collect excessive data on children, while around 89% of platforms during the COVID-19 pandemic collected information beyond learning needs, including voice recordings, location tracking, and behavioral interactions for predictive analytics.

Several significant risks have been identified, including: excessive algorithmic profiling, discrimination based on limited or biased data, biometric data leaks, data commercialization through targeted advertising, unethical use of data for behavioral prediction, and cyberattacks such as ransomware (Livingstone, S., & Third, 2021), Legal studies in Indonesia (Fitriani, 2023a), (Darmawan, 2024), and (Ni'matul Huda., 2023), show that although the PDP Law has been passed, national regulations do not specifically address child data protection, technical guidelines for AI data management, regulations for automated decision-making, security standards for digital education platforms, or obligations for algorithm accountability and transparency.

Significant differences emerge when compared to the European Union, where educational AI systems are categorized as high-risk and required to meet requirements for impact audits, risk assessments, and human oversight (AI Law, 2024). Additional studies

(Mahfud, 2021), (Fitriani, 2023b), and (Widodo, 2022), indicate a lack of understanding among electronic system administrators and the absence of a personal data oversight authority, while global research (Livingstone, S., & Third, 2021) confirms the tendency of digital platforms to excessively collect children's data without adequate consent.

While previous research has addressed child data protection in general, several significant gaps remain, including the lack of comprehensive analysis of Indonesian EdTech platforms' compliance with the PDP Law and international standards such as GDPR-K, COPPA, and the AI Law; the lack of studies related to child data protection in the context of adaptive learning algorithms, recommendation systems, and automated decision-making; limited research on specific risks to child data, including algorithmic bias, persistent digital profiles, biometric leaks, commercial exploitation, and platform legal liability; and the absence of comparative evaluations that assess the adequacy of national regulations against international standards and provide policy recommendations to ensure the best interests of the child are met (Chikwava et al., 2021).

This research uses a normative juridical method by combining three main approaches, namely a legislative approach that examines the provisions of the PDP Law, the Child Protection Law, the ITE Law, as well as regulations related to education and the implementation of electronic systems; a conceptual approach that examines the concept of child protection, the principle of personal data confidentiality, artificial intelligence ethics, cybersecurity, and the characteristics of high-risk AI according to international standards; and a comparative approach that compares the Indonesian legal framework with GDPR-K, COPPA, and the AI Law as global references in child data protection and AI governance (Huang, 2023).

Based on this research focus, the research questions are formulated as follows:

1. How does the regulatory framework in Indonesia regulate the protection of children's personal data in the context of AI-based educational platforms?
2. How are child data protection implemented by AI-based educational platforms, including consent mechanisms, data security, and mitigation of potential algorithmic bias?
3. What are the risks associated with the misuse of children's data, including profiling, commercialization, and information leakage, and how are these legally protected?
4. To what extent are the regulations in Indonesia effective and adequate compared to international standards, and what legal gaps need to be addressed?

The purpose of this study is to evaluate the compliance of Indonesian national law with international norms regarding child data protection, present a comprehensive analysis of legal protection for children using AI-based learning platforms, and provide practical recommendations to the public, educational platform providers, and legislators for safer, more responsible, and child-centered AI governance; with this approach, the study not only advances legal research related to technology and child protection in the digital era theoretically, but also offers practical guidance for improving regulations and policy implementation in Indonesia (Rakhmetov et al., 2025).

The significance of this research lies in its ability to provide both theoretical and practical contributions to the field of educational law and technology, particularly regarding the protection of children's personal data. Theoretically, this research broadens the understanding of Indonesia's national legal framework in addressing the challenges of children's data processing by AI-based educational platforms, and assesses the compliance of national regulations with international standards such as GDPR-K, COPPA, and the AI Law. Practically, this research offers guidance for policymakers, educational platform providers, and the wider community regarding the implementation of safe, transparent, and responsible AI governance, emphasizing the principle of the best interests of the child, mitigating the risk of data misuse, and enhancing legal protection for children in the digital

learning ecosystem. Thus, this study is expected to serve as a basis for the formulation of derivative regulations, technical guidelines, and more effective oversight mechanisms to ensure comprehensive protection of children's personal data in Indonesia.

Research Method

This research uses a normative juridical method with a focus on legal analysis related to the protection of children's personal data in AI-based education platforms in Indonesia, which is implemented through three main approaches, namely a legislative approach to examine the provisions of the PDP Law, the Child Protection Law, the ITE Law, the National Education System Law, and other regulations related to the digitalization of education and the implementation of electronic systems; a conceptual approach to examine the concept of child protection, the principle of personal data confidentiality, the principle of data minimization, AI ethics, cybersecurity, and the characteristics of high-risk AI according to international standards; and a comparative approach that compares the Indonesian legal framework with GDPR-K, COPPA, and the European Union AI Law to assess the suitability of national regulations, identify gaps, and find best practices in child data protection (Jayasekara et al., 2022).

The research was conducted using a normative-qualitative approach with the following stages:

The process of identifying and collecting legal data in this study includes collecting primary legal sources, such as the PDP Law, the Child Protection Law, the ITE Law, the National Education System Law, as well as government regulations and ministerial regulations related to the digitalization of education; secondary legal sources, including journal articles, reports from UNICEF, OECD, UNESCO, HRW, and academic books discussing child data protection, digital privacy, and cyber law; and tertiary legal sources, such as legal dictionaries, encyclopedias, official government publications, media reports, and statistical data regarding the use of AI platforms in education in Indonesia (Jayasekara et al., 2022).

The document and literature analysis in this study was conducted through three stages: a legal norm analysis that examines the principles of the PDP Law and related regulations, including the best interests of children, platform provider accountability, and algorithmic risk mitigation; a conceptual analysis to evaluate the principles of child privacy, data minimization, and the risks of using AI in EdTech platform practices; and a comparative analysis that compares national regulations with GDPR-K, COPPA, and the AI Law to identify gaps and highlight best practices in protecting children's personal data (Altafi et al., 2025).

The triangulation and validation process in this study includes normative validity, by ensuring that each legal document comes from an official publication and is issued by an authorized institution, as well as source triangulation, which is carried out by comparing the privacy policy of the AI platform with national legal principles and international standards, while reviewing academic literature and reports from international organizations to ensure the suitability, accuracy, and consistency of the information (Valença et al., 2022).

The synthesis and conclusion stage in this research aims to compile legal conclusions that include an assessment of the conformity of national regulations, identification of existing legal loopholes, analysis of unresolved child data protection risks, and formulation of recommendations for regulatory improvements to increase the effectiveness of children's personal data protection in the use of AI-based educational platforms (Mohd Ariffin et al., 2025).

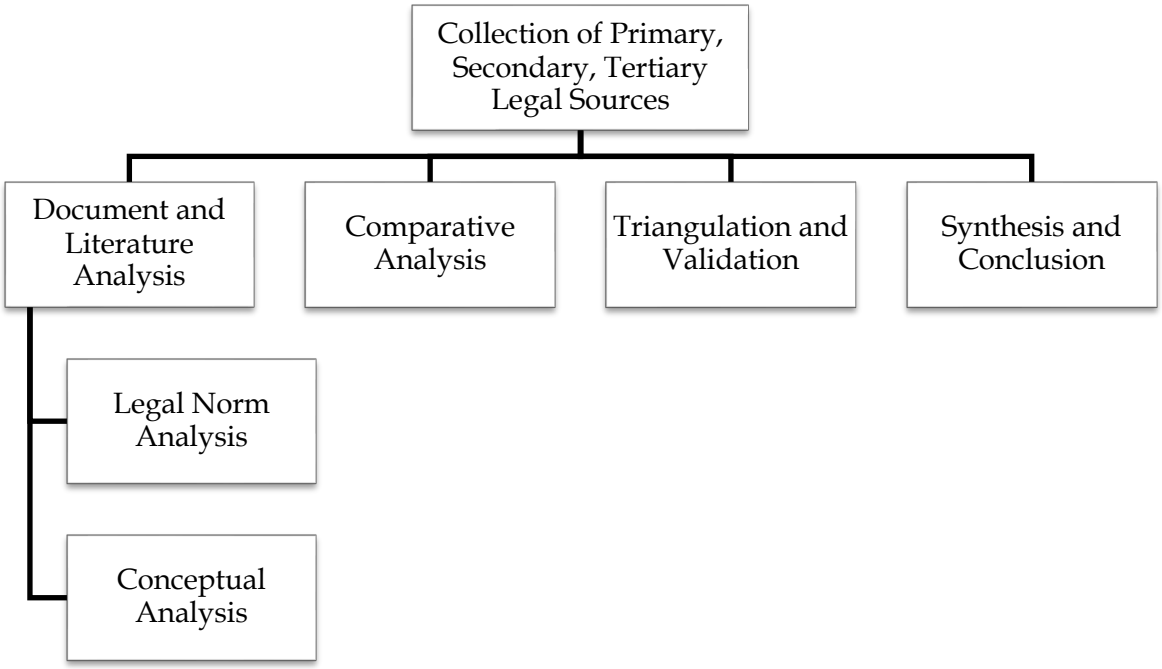

Figure 1. Research Process Flowchart

The quality criteria for legal sources in this study include the use of documents from official authorities, such as regulations, laws, or legitimate government documents; relevance, which ensures the sources are directly related to child data protection or AI platform regulations; accuracy, prioritizing the most recent data verified through official publications or reputable academic sources; and balance, which includes both national and international perspectives to provide a comprehensive analysis.

The research timeline includes four main stages: months 1–2 for literature and legal document collection; months 3–4 for legal and conceptual norm analysis; months 5–6 for comparative analysis and source triangulation; and month 7 for synthesizing results, drawing conclusions, and formulating policy recommendations related to children's personal data protection in AI-based educational platforms.

Ethical considerations in this research include respecting intellectual property rights by accurately citing legal sources, literature, and reports, avoiding plagiarism and data misuse, presenting analysis objectively without bias towards certain platforms or regulations, and ensuring that any policy recommendations always consider the best interests of children as vulnerable data subjects.

Limitations of this study include its normative and qualitative nature, which prevents quantitative measurement of the effectiveness of implementation in the field; limitations in available legal documents and literature, given that EdTech platform data can change over time; and its focus on Indonesian regulations and comparisons with international standards, which prevents a comprehensive global empirical analysis.

Result and Discussion

Table 1. Legal Regulations on the Protection of Children's Personal Data in AI-Based Educational Platforms in Indonesia

No	Key Findings	Description of Findings	Implications for Child Protection
1	Limited special provisions for children in the PDP Law	Law No. 27 of 2022 identifies children as data subjects requiring special protection but does not specify age limits, parental consent mechanisms, or categories of high-risk data.	Creates a regulatory gap as educational AI platforms lack mandatory standards for obtaining parental consent and protecting sensitive child data.
2	Absence of sector-specific derivative regulations for AI-based education	Derivative regulations under the PDP Law and Government Regulations on AI systems do not explicitly regulate AI processing in educational platforms, including encryption standards, algorithm audits, and processing of children's biometric data.	Leads to legal uncertainty and weak oversight of EdTech platforms handling children's data.
3	Inconsistencies between the PDP Law, Child Protection Law, and Education System Law	These laws are not fully integrated, resulting in overlaps and gaps regarding AI, children's digital privacy, and the use of big data in education.	Reduces the overall effectiveness of child data protection due to the lack of a comprehensive and cohesive legal framework.

Table 2. Implementation of Data Protection in AI-Based Education Platforms in Indonesia

No	Key Findings	Description of Findings	Implications for Children
1	Collection of data beyond learning needs	Many AI-based EdTech platforms collect a wide range of data, including learning activities, voice recordings, location data, preferences, and digital behavior, without clearly mapping essential data needs.	Increases the risk of excessive tracking and creation of detailed digital profiles of children, potentially affecting their privacy and autonomy.
2	Complex and non-transparent privacy policies	Privacy policies are often lengthy (2,500–3,000 words), legalistic, not child-friendly, and do not clearly specify data retention or deletion mechanisms.	Parents and guardians may be unaware of their rights to control or request deletion of their children's personal data, reducing the effectiveness of consent mechanisms.
3	Lack of algorithmic transparency	Platforms do not disclose the logic, decision-making criteria, or potential biases of AI algorithms used in learning recommendations.	Children may be subject to algorithmic bias in educational recommendations without any opportunity to contest or correct the decisions affecting their learning outcomes.

Table 3. Identified Risks of Child Data Abuse in AI-Based Education Platforms

No	Main Risks	Description of Risks	Potential Long-Term Impacts
1	Profiling and commercialization of child data	Learning behavior data is often used for targeted advertising and profile-based recommendations, practices that violate COPPA and GDPR-K standards.	Children may become subjects of digital commercialization from an early age, influencing their preferences, autonomy, and privacy.
2	Data leaks and cyber intrusions	Not all platforms implement strong encryption (e.g., AES-256) or conduct regular security audits. Educational data is sometimes stored in third-party cloud services without transparent server location information.	Increased risk of identity misuse, doxing, identity theft, and unauthorized access to sensitive personal information.
3	Algorithmic bias and digital discrimination	AI models trained on unrepresentative datasets may categorize children based on academic performance or behavioral patterns.	Can negatively affect children's self-esteem, reinforce educational inequalities, and create unfair AI-based educational outcomes.

Table 4. Adequacy and Effectiveness of Legal Regulations on Child Data Protection in AI-Based Education Platforms

No	Findings	Description	Effectiveness Analysis
1	Lack of explicit regulation on AI algorithms in the PDP Law	The PDP Law does not include clauses on automated decision-making, algorithm explainability, or auditing requirements for AI models.	Current regulations are insufficient to address the unique challenges posed by AI processing of children's data.
2	Absence of an independent monitoring body for children's data	Indonesia lacks a dedicated institution equivalent to a "Children's Data Protection Unit" (Korea) or an EDPB Taskforce (EU).	Oversight remains administrative rather than risk-based, limiting proactive monitoring and enforcement.
3	Ineffective sanction mechanisms	Administrative sanctions stipulated in the PDP Law have not been fully implemented, and criminal sanctions have never been applied in the context of educational technology.	Regulatory effectiveness is low due to lack of enforcement precedent and insufficient deterrent impact on violators.

Legal Regulations for the Protection of Children's Personal Data in Indonesia

Indonesian laws and regulations protecting children's personal information are still not fully aligned with advances in AI technology, particularly in the context of digital education. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is the most recent regulation, but it remains a general normative document and does not specifically protect children as vulnerable data subjects. More precise regulations are urgently needed in

the context of AI-based education platforms that process children's data extensively, comprehensively, and in-depth. Currently, there are no sectoral laws in Indonesia comparable to COPPA (US) or GDPR-K (EU), specifically addressing age restrictions, parental consent procedures, restrictions on child data processing, and algorithm transparency requirements.

While the PDP Act recognizes children as a group requiring special protection, it does not specify a legal age for children to provide consent to the processing of their data. On the other hand, the GDPR sets the age limit at 16 (with the option to lower it to 13 in some member states), and COPPA sets a minimum age of 13 for use of digital services without parental verification. This uncertainty raises the risk of misuse, as platforms may assume a child's consent is valid even without parental involvement.

Furthermore, the PDP Law does not specify the responsibilities of AI system providers in protecting children's data. Sensitive information such as voice recordings and videos, learning behavior, and interaction preferences are often processed by digital education platforms without specific operational standards, including minimum encryption, algorithm audits, or child data processing impact assessments (DPIAs). Unlike the GDPR-K, which requires a Data Protection Impact Assessment for all processing of children's data, this gap increases the risk of child privacy violations (Sarika Nitin Zaware, 2024).

Synchronization of regulations across laws in Indonesia is also problematic. The Child Protection Law does not address digital exploitation through data, the National Education System Law does not regulate the use of big data or AI in education, and the Personal Data Protection Law has not been substantively integrated with sectoral regulations. The lack of regulations from the Ministry of Communication and Informatics and the Ministry of Education and Culture that provide technical guidelines for handling children's data on EdTech platforms further exacerbates the situation.

Conceptually, children are data subjects with psychological and cognitive capacities that are still developing, so their understanding of the risks of digital data processing is limited. Livingstone (2018) emphasized that children often provide data voluntarily without realizing the long-term implications. EdTech platforms that collect behavioral data, learning preferences, voice recordings, and videos for AI personalization without strict oversight can pose risks of exploitation and permanent digital profiling.

COPPA and GDPR-K provide stricter protection standards, including the principle of the best interests of the child, restrictions on automated profiling, and a prohibition on collecting data for commercial purposes without parental consent. Indonesia's Privacy and Data Protection Law still permits the processing of children's data with the consent of a "data controller" without age verification or additional safeguards (Oh et al., 2024). Previous studies support this conclusion: (Putri, 2022) indicates that Indonesia is not yet ready to implement child data protection standards, while (Fajri, 2023) highlights the lack of implementation of the privacy-by-design principle, which increases the risk of child data breaches in the education sector.

Furthermore, the practice of automated profiling used by educational AI platforms for personalized recommendations is still permitted in Indonesia, even though the GDPR-K specifically prohibits this practice. The absence of an independent oversight body focused on child data protection hinders law enforcement, unlike the European model, which has a specific audit and sanctions body.

The results of this study indicate several important practical implications, including the need to develop derivative regulations for the PDP Law that specifically regulate child data protection, including technical standards such as encryption, algorithm audits, age verification, and assessments of the impact of child data processing; the implementation of the privacy-by-design principle by EdTech platforms by providing privacy policies that are easy for children and parents to understand and transparent consent mechanisms; the

establishment of an independent supervisory body tasked with conducting audits, risk-based supervision, and effective enforcement of sanctions; a ban on commercial profiling practices that exploit children's data for behavioral analysis, targeted advertising, or segmentation based on learning ability; and strengthening the integration of national laws through synchronization between the PDP Law, the Child Protection Law, and the National Education System Law to create a comprehensive and clear legal framework (Cao et al., 2022).

This research is normative-qualitative in nature and limited to analysis of legal documents and literature, thus not quantitatively evaluating the compliance of EdTech platforms in the field. The study's focus is limited to Indonesian regulations and their comparison with COPPA and GDPR-K, thus precluding broader global empirical analysis. Furthermore, EdTech platform practices can change over time, so findings regarding the collection and processing of children's data are tentative.

Future research could incorporate empirical approaches to assess platform compliance with the PDP Law on the ground, the effectiveness of parental consent mechanisms, algorithm audits, and the protection of sensitive child data. Broader comparative studies across Indonesia, ASEAN countries, and global jurisdictions could help formulate more effective child data protection standards. Research could also evaluate the long-term impact of automated profiling on child well-being and develop technical guidelines for the ethical and child-centered integration of AI in the education sector.

Implementation of Data Protection by AI-Based Education Platforms

The complex dynamics surrounding the implementation of child personal data protection on AI-based educational platforms in Indonesia are primarily driven by technological advancements that outpace regulatory readiness. Most EdTech platforms, including Ruangguru, Zenius, Pahamify, and international AI-based adaptive learning apps used in Indonesia, process vast amounts of child data. Basic identity information, learning activity history, learning preferences, and digital interaction patterns are all captured in this data. However, research shows that different platforms implement data protection in very different ways, particularly regarding data processing transparency and restrictions on data use for AI-based profiling.

From the perspective of the PDP Law, platform privacy policies encompass several important requirements, including the basis for processing, the minimization principle, and parental consent. However, the quality of implementation remains poor. Most apps offer only general consent without providing detailed information about the dangers associated with data processing by AI algorithms. International standards such as the GDPR-K require specific, informed, and detailed consent, separating data collection, analysis, and use by AI systems. This leaves a significant normative gap between international best practices and actual practice in Indonesia.

The Data Protection Impact Assessment (DPIA) component also presents implementation challenges. Government regulations or derivative regulations of the PDP Law in Indonesia do not yet contain detailed provisions regarding this obligation. Therefore, before introducing new features that process children's data, such as recommendation systems or automated assessments, AI-based educational platforms do not conduct systematic risk assessments. GDPR-K and the EU AI Law require DPIAs for processing children's data, particularly when high-risk profiling algorithms are used. This lack of technical regulation in Indonesia leads to a lack of comprehensive data protection (Amandha et al., 2022).

Several previous studies, including reports from UNICEF (2022) and UNESCO (2023), have demonstrated that EdTech platforms worldwide generally have inadequate privacy protections, especially for school-age children. Many platforms monetize learning

behavior data, advertise, and promote premium services, among other commercial uses of learning data. These findings support the conclusion that several apps in Indonesia still use third-party cookies and trackers without explicit parental consent, thus violating the COPPA principle prohibiting the transfer of children's data for profit.

Some platforms have incorporated two-factor authentication and encryption for technical security, but privacy policies remain unclear about algorithmic security and potential data bias. AI-based education systems are categorized as "high-risk AI systems" under the AI Law, which requires algorithm audits, bias management, and regular security verification. This lack of technical standards means that the implementation of child data protection still relies on platform internal policies, rather than a consistent legal framework.

Inadequate data subject rights mechanisms for children are another weakness. Some educational apps still don't offer simple data deletion features, even though the PDP Law provides the rights to access, correct, restrict, and delete data. Many platforms only offer account deactivation, not complete deletion of data history. The implementation of these rights must be strengthened in accordance with international standards such as the GDPR-K (Liu, 2021).

Furthermore, parental controls or their involvement in monitoring data processing are not yet fully effective. Some platforms don't provide control dashboards to monitor data, limit the amount of data processed by AI, or view usage history, instead relying solely on prior consent. COPPA requires platform operators to allow parents to view and delete their child's data at any time, highlighting the need for improved implementation.

The capacity of digital platform providers also impacts the implementation of child data protection. Many EdTech companies in Indonesia are startups focused on developing learning features and market monetization, so data compliance is not a top priority. Furthermore, the use of servers and algorithms from external vendors complicates data chain control, increasing the risk of data leakage and misuse Dehal et al. (2021).

Overall, the implementation of child data protection by AI platforms in Indonesia still falls short of international standards such as GDPR-K and COPPA. The lack of specific guidelines for AI-based education platforms reinforces the argument that national regulations are inadequate, and that oversight and auditing of algorithms, parental controls, and restrictions on commercial data use need to be strengthened (Sofyan & Meinel, 2024).

The practical implications of these findings include the urgent need to develop derivative regulations for the Child Protection Law specifically addressing child data protection, the implementation of privacy-by-design in EdTech platforms, the establishment of an independent oversight body focused on child data, a ban on data profiling for commercial purposes, and increased transparency and parental involvement. This study also emphasizes the importance of synchronizing the Child Protection Law, the Child Protection Law, and the National Education System Law to create a comprehensive legal framework.

Research limitations include a focus on legal documents and secondary literature without collecting empirical field data, limited sampling of EdTech platforms, and rapid changes in platform technology and policies that may impact the relevance of future findings.

Future research directions are suggested to examine field implementation through empirical studies, evaluate the effectiveness of algorithm audits, risk-based oversight, and platform compliance with international standards, and explore the psychological and cognitive impacts on children as data subjects in AI-based learning ecosystems.

Identifikasi Risiko Penyalahgunaan Data Anak pada Platform Pendidikan Berbasis AI

Since children are the most susceptible to digital manipulation, behavioral profiling, and commercial exploitation, there is a serious risk that their personal information will be

misused in AI-based educational platforms. AI systems can create extremely sensitive predictive patterns from children's data, including learning activity data, reading interests, cognitive tendencies, and digital behavioral records. From the standpoint of data protection law, this risk results from the wide range of data processed and the lax purpose restrictions on the majority of Indonesian EdTech platforms.

Automated profiling by AI systems that map kids' learning capacities and behaviors is the biggest risk. In the absence of stringent regulations, profiling data may be abused for non-educational purposes, such as content commercialization or advertising segmentation, even though it can improve personalized learning. Since it is thought to have an impact on children's freedom and psychological development, the GDPR-K standard forbids child profiling without a solid legal foundation. However, there is still a high risk of abuse because Indonesian laws do not expressly forbid child profiling on educational platforms.

Data breaches brought on by flaws in system security are another risk. According to a number of international studies, including UNICEF's 2022 report, 42% of EdTech platforms worldwide lack sufficient security measures. Due to the absence of required technical standards for putting the Personal Data Protection Law into practice, Indonesia also has a similar issue. Leaks of children's data can have long-term impacts, as the information can be used for identity theft, digital fraud, or other social abuse (Olateju Temitope Akintayo et al., 2024).

Additionally, there is a chance that third parties will abuse it. Numerous educational applications incorporate third-party services like cloud providers, analytics tools, and tracking cookie providers. The risk of abuse rises when children's data is transferred to third parties without explicit, independent consent. The sharing of children's data with third parties without verifiable parental consent is expressly forbidden by COPPA, although Indonesia has not fully complied with this requirement. Children's data is therefore susceptible to commercial exploitation.

Machine bias, also known as algorithmic bias, is another conceptual risk that can lead to incorrect classifications of children's abilities. Limited training datasets or AI models that are not adapted to the social context of Indonesia can lead to bias. Digital stigmatization is one effect; for instance, kids who are labeled as "low achievers" because of algorithmic mistakes may face prejudice in the classroom. Although Indonesia does not currently have algorithm audit laws to safeguard children, the AI Act classifies this risk of bias as high.

Manipulative AI poses psychological risks as well. Children's preferences can be influenced by AI-based recommendation systems in both commercial and educational settings. The GDPR-K and the AI Act forbid cognitive manipulation, which is what happens when platforms use AI to persuade kids to watch particular content for commercial gain. The use of AI to manipulate children is not specifically prohibited in Indonesia (Adami et al., 2021).

The digital shadow, a child's expanding digital footprint kept on platform servers for years, is another long-term risk. Children's data could be used as a long-term commercial asset that is exploited into adulthood if there is no auto-deletion mechanism or stringent data retention policies. Unlimited data retention is the largest risk for EdTech platforms, according to OECD research from 2023. While data retention is governed by the PDP Law, certain types of child data are not covered.

In a broader sense, cross-border data transfers may also increase the risk of data misuse. Many educational platforms use servers located abroad, but they do not reveal the location of the data transfers involving children. Transferring data to countries with lax security regulations may raise the possibility of abuse. Indonesia's data transfer is still declaratory and lacks a direct oversight mechanism, in contrast to the GDPR's stringent data transfer regulations.

Numerous earlier studies, including those by Cahyadi (2022) and FPF (2021), have demonstrated that the lack of strong oversight mechanisms and inadequate parental education regarding digital privacy practices increase the risk of child data misuse on digital platforms. These results are in line with Indonesia's low level of digital privacy literacy, which causes parents to give consent without realizing the risks involved (Wang et al., 2025).

Overall, the results of this sub-focus confirm that there is a very high risk of child data misuse in AI-based education platforms because of lax technical security standards, lax third-party oversight, lax parental consent procedures, and lax underlying regulations. This circumstance emphasizes how urgent it is to create more specific child data protection regulations, especially with regard to the application of AI in the field of education.

The practical implications of these findings include the need to develop derivative regulations under the PDP Law that govern child profiling, data retention, cross-border transfers, and system security; the implementation of privacy-by-design principles by EdTech platforms by providing easy-to-understand privacy policies, transparent consent mechanisms, and parental control rights; the establishment of an independent oversight body specifically for child data to conduct algorithm audits, risk-based oversight, and enforce sanctions; the development of mandatory technical standards, including encryption, two-factor authentication, and regular security audits to minimize the risk of leaks and algorithmic bias; and improving digital and privacy literacy for parents and teachers to ensure informed consent for the collection of children's data.

A review of Indonesian legal developments shows that the Personal Data Protection Law (PDP) provides an initial foundation, but it does not yet regulate profiling mechanisms, algorithm audits, data retention, or cross-border transfers. Synchronization with the Child Protection Law, the National Education System Law, and the AI Law needs to be strengthened to create a more comprehensive legal framework. Limitations of this research include a focus on legal documents and secondary literature, without real-time fieldwork of EdTech platforms. The rapid dynamics of technological change and platform policies may also impact the relevance of the findings in the future.

Future research directions are suggested to explore empirical field studies related to the implementation of child data protection on EdTech platforms, evaluation of algorithm audits and parental control mechanisms, psychological and cognitive impacts on children as data subjects, and the effectiveness of new regulations or derivative regulations of the PDP Law after they are enacted, including the mechanism for enforcing sanctions.

Adequacy and Effectiveness of Children's Personal Data Protection Regulations in Indonesia

Indonesia already has a fundamental framework in the form of the Personal Data Protection Law (Law No. 27/2022), according to an analysis of the efficacy and sufficiency of regulations. The protection of children's personal data in the context of AI-based educational platforms is not yet covered by this regulation, which is still broad in scope. The Electronic Information and Transactions Law and the Child Protection Law both contain normative provisions pertaining to child protection, but they have not yet been incorporated into data protection regulations pertaining to AI and EdTech.

From a legal standpoint, fundamental concepts like minimization, purpose limitation, transparency, and a legitimate basis are already governed by the PDP Law. However, in terms of efficacy, this regulation lacks a technical mechanism to guarantee that providers of educational platforms implement thorough data protection. The implementation of child protection has been less than ideal due to the lack of derivative regulations, such as a government regulation on child data or technical guidelines on algorithm audits.

In contrast to the GDPR-K, Indonesia does not have specific laws pertaining to "child-specific data protection." The GDPR governs the age limit for consent, requires parental verification, forbids child profiling, and upholds the high-level protection principle. Platform operators have different interpretations because Indonesia does not specifically regulate the age limit for children in the context of digital data processing. This makes gauging the success of child protection challenging (Herbawani et al., 2025).

Indonesia's regulatory effectiveness standards also fall short when it comes to COPPA, which mandates verifiable parental consent, frequent audits, and a prohibition on child-targeted advertising. However, the PDP Law does not forbid the commercial use of children's data, which permits EdTech firms or other parties to make money off of data through market segmentation or advertising. This suggests that Indonesian laws continue to fall well short of international norms in terms of their ability to protect children.

AI-based educational applications are included in the concept of a "high-risk AI system," which is introduced by the AI Act. Risk documentation, frequent algorithm audits, bias management, model security, and user transparency regarding AI use are all governed by this regulation. The effectiveness of child protection in the context of AI is severely limited because Indonesia does not yet have similar regulations. It is not necessary for Indonesian edtech platforms to disclose the risks associated with the AI systems they employ or how their algorithms operate.

A lack of institutional coordination also affects how adequate regulations are. Law enforcement is declarative and non-operational since the PDP Authority, an agency that has not yet been established, is in charge of overseeing the protection of personal data. The efficacy of the PDP Law's regulations in safeguarding children's personal information is still low in the absence of an oversight body that actively performs audits and inspections. This is consistent with research by (Darmawan, 2024) that demonstrates Indonesia's continued lax enforcement of data protection laws.

Additionally, Indonesia does not have any particular laws pertaining to AI. Child data protection is not covered by the National AI Roadmap (STRANAS AI), which governs AI development generally. As a result, there is insufficient legal support for AI ethics, algorithm audits, and bans on the cognitive manipulation of minors. As a result, children's legal protection in the AI-based digital education ecosystem has become less effective (Samsudin, 2025).

Regulations exist, but they are insufficient to stop educational platforms from misusing data in terms of normative effectiveness. Administrative fines, criminal penalties, and mandatory breach notification requirements that specifically target children's data are examples of enforcement mechanisms absent from the PDP Law. Additionally, Indonesia lacks a national standard on data minimization for educational platforms, so providers' self-regulation is the only way to ensure effective protection.

Indonesian regulations continue to be reactive rather than proactive when compared to those in developed nations. The regulatory frameworks of the AI Act, COPPA, and GDPR place a strong emphasis on risk mitigation prior to data processing. The PDP Law, on the other hand, usually offers protection following a violation. Regulations' ability to protect children online is severely limited in the absence of a preventative strategy (Y. Zhang, 2025).

Overall, the analysis demonstrates that Indonesia's child data protection laws for AI-based learning platforms are still insufficient in both efficacy and sufficiency. Although the PDP Law offers a fundamental legal framework, it makes no mention of algorithm audits, prohibitions on profiling, child data, or high-risk AI applications. Indonesia requires guidelines for implementing AI in the education sector, specific derivative regulations pertaining to child data, and the creation of an active oversight body in order to achieve

comprehensive protection. The possibility of child data being misused in AI-based educational systems will keep growing in the absence of these precautions.

The practical implications of these findings emphasize the need for the government to immediately draft derivative regulations under the PDP Law that govern child profiling, data retention, cross-border transfers, system security, and algorithm audits. EdTech platforms should also adopt the principle of privacy-by-design by providing easily understandable privacy policies for children and parents, as well as transparent parental consent and control mechanisms. Furthermore, the establishment of an independent oversight body specifically for children's data is necessary to conduct algorithm audits, risk-based oversight, and enforce sanctions. Mandatory technical standards such as encryption, two-factor authentication, and regular security audits must be established to minimize the risk of leaks and algorithmic bias. Furthermore, improving digital education and literacy for parents, teachers, and school administrators is crucial to ensure informed and accurate consent for children's data collection.

This research is normative and qualitative in nature, so it does not empirically assess the effectiveness of regulatory implementation in the field. The data used are sourced from literature, regulations, and secondary reports, so it does not capture the full variability of EdTech platform practices. Further research is recommended to conduct empirical studies related to the implementation of child data protection on EdTech platforms, evaluation of algorithm audit mechanisms and parental controls, psychological and cognitive impacts on children, and the effectiveness of new regulations or derivatives of the PDP Law, including sanction enforcement mechanisms.

Conclusions

The national legal framework, particularly the Personal Data Protection Law, the ITE Law, and the Child Protection Law, has provided a normative basis, but it still has significant limitations because it does not specifically regulate the categories of children's data, data processing mechanisms by AI systems, algorithm audits, and technical requirements for AI-based educational platforms. This conclusion is based on the findings of a legal analysis of the protection of children's personal data in AI-based educational platforms in Indonesia. In terms of preventive protection, third-party oversight, bans on child profiling, and limitations on the use of data for commercial purposes, Indonesia continues to lag behind when compared to international regulatory frameworks like GDPR-K, COPPA, and the AI Act. Due to low security standards, shoddy parental consent verification, and a lack of technical guidelines for the storage, transfer, and deletion of children's data, EdTech platforms' implementation of protections is likewise ineffective. The potential for child data misuse, such as automated profiling, data breaches, cognitive manipulation, and commercial exploitation, highlights the need for PDP authorities to establish derivative regulations and active oversight mechanisms, which are currently not functioning at their best. The lack of empirical field data regarding the technical implementation by each AI platform in Indonesia limits this study, despite its advantage of offering a thorough mapping through statutory, conceptual, and international comparison approaches. However, the results of this study can serve as an academic foundation and policy recommendations for the creation of specific guidelines for child data protection in the AI era, the development of EdTech security standards, the establishment of an AI governance model that is responsive to children's best interests, and the opening of space for additional research that focuses on the empirical evaluation of educational platforms operating in Indonesia.

Acknowledgement

The author would like to express sincere appreciation to all individuals and institutions who contributed to the completion of this study. Gratitude is extended to legal

scholars, education practitioners, and technology experts who provided valuable insights on children's personal data protection in AI-based education platforms. The author also thanks academic advisors and colleagues for their guidance and constructive feedback. It is hoped that this research contributes to strengthening legal protection for children's personal data in Indonesia.

References

Abajobir, A., de Groot, R., Wainaina, C., Njeri, A., Maina, D., Njoki, S., Mbaya, N., Donfouet, H. P. P., Pradhan, M., Janssens, W., & Sidze, E. M. (2021). The impact of i-PUSH on maternal and child health care utilization, health outcomes, and financial protection: study protocol for a cluster randomized controlled trial based on financial and health diaries data. Trials, 22(1), 629. https://doi.org/10.1186/s13063-021-05598-7

Adami, D., Ojo, M. O., & Giordano, S. (2021). Design, Development and Evaluation of an Intelligent Animal Repelling System for Crop Protection Based on Embedded Edge-AI. IEEE Access, 9, 132125–132139. https://doi.org/10.1109/ACCESS.2021.3114503

Ai, X. (2022). The Construction of an Online Education Platform Under the Background of Big Data and Intelligent Data Interaction: The Realization of Interaction Based on C#. 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 545–548. https://doi.org/10.1109/ICAIS53314.2022.9742776

Altafi, H., Suresh, S., & Zareinia, K. (2025). The potential of cloud-based AI-enabled platforms in healthcare education. International Journal of Intelligent Robotics and Applications, 9(2), 683–693. https://doi.org/10.1007/s41315-024-00405-3

Altaleb, H., Mouti, S., & Beegom, S. (2023). Enhancing College Education: An AI-driven Adaptive Learning Platform (ALP) for Customized Course Experiences. 2023 9th International Conference on Optimization and Applications (ICOA), 1–5. https://doi.org/10.1109/ICOA58279.2023.10308834

Amandha, A. R., Hapsari, P. D., Rivaldi, M. A. R., Saputro, B. A., Cahyani, A., & Arifin, R. (2022). The Mainstreaming of the Concept of Legal Protection for Child Labor in Indonesia based on ILO Conventions. The Indonesian Journal of International Clinical Legal Education, 4(3). https://doi.org/10.15294/ijicle.v4i3.60021

Cao, F., Lei, M., Lin, S., & Xiang, M. (2022). Application of Artificial Intelligence-Based Big Data AI Technology in Physical Education Reform. Mobile Information Systems, 2022, 1–12. https://doi.org/10.1155/2022/4017151

Chikwava, F., Cordier, R., Ferrante, A., O'Donnell, M., Speyer, R., & Parsons, L. (2021). Research using population-based administration data integrated with longitudinal data in child protection settings: A systematic review. PLOS ONE, 16(3), e0249088. https://doi.org/10.1371/journal.pone.0249088

Darmawan, R. (2024). Perkembangan regulasi perlindungan data pribadi di Indonesia: Tantangan dan prospek implementasi. Jurnal Hukum Dan Kebijakan Publik, 12(1), 55–72.

Denecke, K., Glauser, R., & Reichenpfader, D. (2023). Assessing the Potential and Risks of AI-Based Tools in Higher Education: Results from an eSurvey and SWOT Analysis. Trends in Higher Education, 2(4), 667–688. https://doi.org/10.3390/higheredu2040039

Fajri, A. (2023). Evaluasi kepatuhan platform digital terhadap prinsip privacy-by-design dan dampaknya terhadap kebocoran data anak di sektor pendidikan. Jurnal Keamanan Data Dan Teknologi, 6(1), 45–60.

Fitriani, S. (2023a). Analisis kebijakan perlindungan data pribadi dalam perspektif hukum nasional. Jurnal Hukum Dan Teknologi Informasi, 5(3), 210–225.

Fitriani, S. (2023b). Implementasi Undang-Undang Perlindungan Data Pribadi dan tantangan perlindungan data anak di Indonesia. Jurnal Hukum Siber Indonesia, 4(2), 145–160.

Galhotra, B., & Lowe, D. (2022). AI Based Examination System: A Paradigm Shift in Education Sector. 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 386–392. https://doi.org/10.1109/COM-IT-CON54601.2022.9850452

Herbawani, L. O., Susanti, A., & Adnani, Q. E. S. (2025). The Revolution in Midwifery Education: How AI and Deep Learning are Transforming Outcome-Based Assessments? Advances in Medical Education and Practice, Volume 16, 1579–1599. https://doi.org/10.2147/AMEP.S543098

Huang, A. (2023). Research on Digital Protection Education of Red Culture Based on Big Data Technology. 2023 International Conference on Data Science & Informatics (ICDSI), 194–198. https://doi.org/10.1109/ICDSI60108.2023.00046

Jayasekara, U., Maniyangama, H., Vithana, K., Weerasinghe, T., Wijekoon, J., & Panchendrarajan, R. (2022). AI-Based Child Care Parental Control System. 2022 4th International Conference on Advancements in Computing (ICAC), 120–125. https://doi.org/10.1109/ICAC57685.2022.10025332

K, S., R, A. G., & Vineeth, N. (2024). Integrating Transparent Crowdfunding Platform and AI-Based Treatment Fund Estimation. 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), 1–6. https://doi.org/10.1109/IDICAIEI61867.2024.10842939

Li, X. (2023). Digital service providers' obligations under GDPR and COPPA: Comparative perspectives on child data protection. Journal of International Data Privacy, 7(2), 88–104.

LiMengyang, L., Mustafa, Z., & Shufang, L. (2025). Research on the construction of outcome-based education platform based on deep learning. Edelweiss Applied Science and Technology, 9(2), 1168–1179. https://doi.org/10.55214/25768484.v9i2.4722

Liu, Z. (2021). Construction of Computer Mega Data Security Technology Platform Based on Machine Learning. 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE), 538–541. https://doi.org/10.1109/ICISCAE52414.2021.9590732

Livingstone, S., & Third, A. (2021). Children's data and digital identity: Risks, rights, and long-term implications in the age of AI. Journal of Children and Digital Society, 4(1), 22–38.

Mahfud, A. (2021). Perlindungan data pribadi di Indonesia: Analisis awal sebelum pengesahan UU PDP. Jurnal Regulasi Digital, 3(1), 25–40.

Mahfud, A. (2022). Regulasi perlindungan data anak dalam ekosistem digital berbasis kecerdasan artifisial. Jurnal Hukum Dan Teknologi, 14(2), 115–130.

Mohd Ariffin, N. H., Mohd Zulkefli, N. A., & Nasruddin, Z. A. (2025). Challenges of Blockchain Technology and its Relationships to Sustainable Education: An Analysis using AI-Based Literature Review. Journal of Advanced Research Design, 127(1), 173–188. https://doi.org/10.37934/ard.127.1.173188

Mudayat, M., Ichwan, I., Budiastara, A. . K., Asyhari, H., Betaubun, M., & Kuswoyo, D. D. (2025). Enhancing Physical Education Learning Through AI-Based Education in the PGSD Program at the Open University in the Digital Era. East Asian Journal of Multidisciplinary Research, 4(6), 2569–2580. https://doi.org/10.55927/eajmr.v4i6.244

Ni'matul Huda. (2023). Kerangka regulasi perlindungan data pribadi di Indonesia: Evaluasi dan arah pembaruan hukum. Jurnal Konstitusi Dan Hak Asasi Manusia, 9(2), 101–118.

Ningsih, F. (2023). Classtime.Com as an Ai-Based Testing Platform: Analysing ESP Students' Performances and Feedback. Journal of Languages and Language Teaching, 11(3), 390. https://doi.org/10.33394/jollt.v11i3.8286

Nurmansyah, G., Wiranata, I. G. A. B., Fardiansyah, A. I., & Mladenov, S. V. (2024). Preventing AI-based phishing crimes across national borders through the reconstruction of personal data protection laws. Jurnal Hukum Novelty, 15(2), 286–311. https://doi.org/10.26555/jhn.v15i2.27558

Oh, S., Cao, Y., Katz, A., & Zhao, J. (2024). Explore Public's Perspectives on Generative AI in Computer Science (CS) Education: A Social Media Data Analysis. 2024 IEEE Frontiers in Education Conference (FIE), 1–9. https://doi.org/10.1109/FIE61694.2024.10893102

Olateju Temitope Akintayo, Chima Abimbola Eden, Oyebola Olusola Ayeni, & Nneamaka Chisom Onyebuchi. (2024). Integrating AI with emotional and social learning in primary education: Developing a holistic adaptive learning ecosystem. Open Access Research Journal of Multidisciplinary Studies, 7(2), 042–051. https://doi.org/10.53022/oarjms.2024.7.2.0025

Putri, N. (2022). Kesiapan regulasi Indonesia dalam penerapan standar perlindungan data anak. Jurnal Hukum Dan Kebijakan Digital, 4(2), 101–116.

Rachmadewi, N. (2024). antangan perlindungan data pribadi anak di platform berbasis AI: Analisis kebijakan dan implikasi etis. Journal of Digital Law and Policy, 6(1), 45–62.

Rakhmetov, M., Sadvakassova, A., Saltanova, G., Kuanbayeva, B., & Zhusupkalieva, G. (2025). Evaluation of an AI-Based Feedback System for Enhancing Self-Regulated Learning in Digital Education Platforms. Electronic Journal of E-Learning, 23(4), 126–141. https://doi.org/10.34190/ejel.23.4.4150

Rizqina, M. (2022). Kerentanan anak terhadap pelacakan daring dan eksploitasi data pada platform digital. Jurnal Keamanan Siber Dan Literasi Digital, 2(3), 120–135.

Sahu, R. (2022). Compliance of digital platforms with GDPR and COPPA: Implications for child privacy. International Journal of Data Protection and Privacy, 4(3), 55–70.

Samsudin, U. (2025). Exploration of Artificial Intelligence (AI) in Increasing Student Collaboration in Digital-Based Islamic Education Learning. Al-Hayat: Journal of Islamic Education, 9(1), 216–230. https://doi.org/10.35723/ajie.v9i1.106

Sarika Nitin Zaware. (2024). AI-Based Phishing Detection and Automated Response: A Multi-Channel Security Framework for Modern Communication Platforms. Panamerican Mathematical Journal, 35(1s), 250–263. https://doi.org/10.52783/pmj.v35.i1s.2312

Sinta, R. (2023). Kesenjangan regulasi dalam pengelolaan data anak pada layanan digital dan kecerdasan buatan. Jurnal Kebijakan Siber, 3(4), 201–218.

Sofyan, Z., & Meinel, C. (2024). Exploring Interactive Content in MOOCs for Training Educators in AI Education. 2024 International Conference on Electrical Engineering and Informatics (ICELTICs), 51–55. https://doi.org/10.1109/ICELTICs62730.2024.10776485

Sumarni, L. (2023). Risiko pembuatan profil dan penyalahgunaan data anak dalam penggunaan media sosial dan aplikasi gim. Jurnal Perlindungan Data Dan Teknologi, 5(1), 60–75.

Supriyadi, A. (2023). Analisis kebijakan privasi dan perlindungan data anak dalam sistem kecerdasan buatan. Jurnal Hukum Siber Dan Privasi Digital, 5(2), 134–150.

Valença, G., Sarinho, M. W., Polito, V., & Lins, F. (2022). Do Platforms Care About Your Child's Data? A Proposal of Legal Requirements for Children's Privacy and Protection. Anais Do Workshop Em Engenharia de Requisitos. https://doi.org/10.29327/1298262.25-19

Voigt, P., & Von dem Bussche, A. (2021). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.

Wang, D., Dong, X., & Zhong, J. (2025). Enhance College AI Course Learning Experience with Constructivism-Based Blog Assignments. Education Sciences, 15(2), 217. https://doi.org/10.3390/educsci15020217

Widodo, B. (2022). Tantangan penegakan perlindungan data pribadi dan kebutuhan otoritas pengawas di Indonesia. Jurnal Kebijakan Publik Dan Teknologi, 7(3), 188–203.

Xie, J., Xie, K., & Lin, Z. (2025). Design and Implementation of a Digital Art Education Platform Based on AI and Cloud Technologies. Proceedings of the 2nd Guangdong-Hong Kong-Macao Greater Bay Area Education Digitalization and Computer Science International Conference, 671–676. https://doi.org/10.1145/3746469.3746574

Zhang, J., Wang, L., Chen, X., Jiang, Y., & Tian, Z. (2023). Artificial Intelligence-Based Education Platform Course Recommendation System. Proceedings of the 4th International Conference on Artificial Intelligence and Computer Engineering, 835–841. https://doi.org/10.1145/3652628.3652767

Zhang, Y. (2025). Optimizing Personalized Learning Paths in Mobile Education Platforms Based on Data Mining. International Journal of Interactive Mobile Technologies (IJIM), 19(12), 4–18. https://doi.org/10.3991/ijim.v19i12.56393