Law and Judicial Review

e-ISSN: 3108-9534

Vol 01 (2) 2025 p. 109-126



**Corresponding author**:
Navis Nailil Munna
Email: naililnavis@gmail.com

*Received 26 September 2025;*
*Accepted 3 October 2025;*
*Published 4 October 2025.*



**Conflict of interest statement**:
The author (s) reported no conflict of interest

DOI: http://doi.org/10.70764/gdpu-ljr.2025.1(2)-09

# LEGAL CONSTRUCTION OF CHILD AND ADOLESCENT PRIVACY PROTECTION IN THE DIGITAL AGE: THE DILEMMA BETWEEN CYBER PROTECTION AND INFORMATION ACCESS IN SCHOOLS

**Navis Nailil Munna**[1]

[1] *Universitas Muria Kudus, Indonesia*

## ABSTRACT

**Objective**: This study aims to analyze the legal construction of child and adolescent privacy protection in Indonesia in the digital age, particularly addressing the dilemma between the need for cybersecurity and the right to access information in schools.

**Research Design & Methods**: This study uses a qualitative method with a normative juridical approach through a literature review of laws, scientific literature, and related legal sources, which are analyzed descriptively and qualitatively to identify normative gaps and provide recommendations for the protection of children's privacy in the digital age.

**Findings:** The findings reveal that Indonesia's legal framework on child privacy protection is still fragmented, with overlapping regulations, a lack of specific norms, and a lack of standard protocols for managing personal data in educational institutions. Compared to the GDPR and COPPA, Indonesian regulations are still less comprehensive, especially in terms of monitoring, law enforcement, and parental consent requirements. Schools face a significant dilemma in balancing cybersecurity measures with ensuring students' rights to access information as part of their learning process.

**Implications & Recommendations:** This study emphasizes the importance of strengthening child privacy regulations in Indonesia through implementing specific norms, data management standards in schools, the principle of Privacy by Design, and increased digital literacy for all stakeholders to create a safe and inclusive digital education ecosystem.

**Contribution & Value Added:** This research strengthens the discourse on child data privacy protection in Indonesia by critically comparing it with international regulations and emphasizing the importance of balancing cybersecurity and the right to information as a legal and educational necessity in the digital age.

**Keywords: Child Privacy, Data Protection, Digital Education**

JEL codes: K36, K38, I28
**Article type:** research paper

## INTRODUCTION

The digital age has fundamentally changed the way children and teenagers interact with the world, especially in the context of education. The massive penetration of information and communication technology has presented enormous opportunities in the form of easy access to unlimited data, enriching learning experiences, and encouraging the transformation of learning methods from conventional to more interactive, collaborative, and technology-based. Through various digital platforms, children and teenagers can acquire knowledge quickly, hone their critical

thinking skills, and connect with the global community, so the learning process is no longer limited to the physical classroom.

Schools today increasingly rely on various digital products to support the educational process, delivery of material, and administrative services. Many educational technology (edtech) platforms promote themselves with the primary goal of improving the quality of education for children and adolescents through innovative features, such as personalized learning tailored to student needs, more interactive and practical content delivery, the use of automated systems in administrative decision-making, and the provision of detailed reports on student performance and engagement (Bayne, 2015). In practice, the education sector has become a relatively more open space for applying automated data collection logic, as personal monitoring and supervision are considered an integral part of the learning process. This condition demonstrates the potential of edtech in creating efficiency and effectiveness and raises new challenges related to data protection, privacy, and the ethics of using technology in education.

Despite offering various benefits, many edtech providers are involved in practices that potentially undermine and even endanger children's rights, particularly the right to privacy (Han, 2022). Personal data now encompasses not only basic identifiers such as name, address, or date of birth, but also extends to more complex digital footprints, including user behavior preferences, social media interaction patterns, real-time location tracking, search history, and other online activity records, all of which can be tracked, analyzed, profiled, and even monetized by third parties for various commercial and non-commercial interests (Sianipar et al., 2025). In the context of education, this is evident in the practice of collecting and utilizing large amounts of data that often far exceed the basic needs of service provision, opening up opportunities for the data to be used for other purposes, including commercial purposes that specifically target children, adolescents, and their families. This situation becomes even more complex given that children occupy a unique position as legal subjects with limited capacity to give valid consent to the processing of personal data, thus requiring stricter protection and effective oversight mechanisms.

Meanwhile, society now lives in an increasingly open digital space, where various social media platforms, e-commerce, and other digital services require users to share their personal information as a prerequisite for access, thereby blurring the boundaries between private and public spaces and increasing the risk of data leaks and misuse. Many users, including educators and students, still have low digital literacy and therefore do not fully understand how their data is used, processed, or the hidden risks that accompany it. Research by Akraman et al., (2018) shows that most internet users in Indonesia do not understand the long-term consequences of granting access to their personal data to digital applications or platforms.

Schools have an essential responsibility to assess the pedagogical quality and educational benefits of the edtech they use and recommend, while also bearing a legal and moral obligation to protect the digital privacy of teachers and students, consistently placing the best interests of students as the top priority. This responsibility goes beyond formal compliance with legal regulations; it requires further efforts because consent-based privacy protection mechanisms still have severe limitations. In Indonesia, this challenge is even more apparent as schools must balance aggressive edtech marketing and promises with the real needs of the educational community and the protection of teachers' and students' rights. The complexity, ambiguity, and power imbalance in data processing practices often make it difficult for schools to transparently ascertain what types of information are collected by edtech platforms and how that data is managed and utilized. This situation underscores the need for institutional capacity, digital literacy, and stronger regulations so that schools are not merely passive users but also active guardians of privacy rights in the era of digital education.

This study aims to analyze the legal framework for protecting the privacy of children and adolescents in the digital age, particularly in the dilemma between the need for cyber protection and access to information in schools. This study will examine the existing legal framework through a normative legal approach, identify normative gaps, and formulate recommendations to strengthen the protection of children's privacy in the digital age. The urgency of this research is increasingly apparent, given that schools, as the main space for education, now face the challenge of balancing

the need for cyber protection to protect students' personal data with the demand to continue providing broad access to information as part of their rights in the learning process. Thus, this study is expected to provide a theoretical and practical basis for formulating a balanced privacy protection strategy, so that children's best interests are guaranteed without hindering the use of digital technology in education.

## LITERATURE REVIEW

### The Concept of Child Privacy Protection from a Legal Perspective

Child privacy protection is multidimensional because it encompasses legal, psychological, and technological aspects. Solove (2008) emphasizes that child privacy is not merely a matter of securing personal data, but is also related to fulfilling children's rights to build their identity and gradually develop their autonomy in accordance with their level of maturity. This issue has become increasingly complex in the digital age because children leave digital traces that can be recorded and accessed in the long term, potentially affecting their future lives regarding freedom of expression, protection from exploitation, and social and professional opportunities.

Milkaite et al., (2021) and Stoilova et al., (2021) highlight that children's privacy in the digital context cannot be equated with adult privacy, because children are still in the process of cognitive, emotional, and social development, which makes them more vulnerable to various forms of online risks. Children are not yet fully capable of understanding the long-term consequences of their digital actions, such as when uploading photos, sharing personal information, or giving consent on digital platforms, which can impact their reputation, safety, and future opportunities. Therefore, stricter protection is needed to prevent data misuse and protect them from potential dangers such as harassment, exploitation, and cyberbullying. On the other hand, children also have the fundamental right to participate in digital life, as the digital space can be an essential means for them to learn, express themselves, build their identity, and establish social relationships. The challenge that arises is how to design a digital ecosystem that is both inclusive and safe, namely by introducing policies, regulations, and technological practices that can balance children's right to participate with the need to protect their privacy.

The concept of child privacy protection from a legal perspective has become a significant concern as the widespread use of digital technology has directly impacted children's lives. The European Union, through the General Data Protection Regulation (GDPR), has introduced a comprehensive legal framework that explicitly emphasizes the need for special protection of children's personal data. This regulation affirms that children have the same privacy rights as adults and recognizes their limitations in understanding digital risks, necessitating additional protection. The GDPR, for example, sets a specific age limit for granting consent to data processing and emphasizes the principle of the best interests of the child in all data collection and use activities (Macenaite, 2017).

The international legal framework increasingly emphasizes protecting children's privacy by highlighting their vulnerability in the digital space. Regulations developed in various countries seek to strike a balance between supporting technological innovation and protecting children's rights, particularly about managing personal data. This effort is evident in how privacy laws adapt to new challenges arising from technological advances such as artificial intelligence, predictive algorithms, and big data analysis, which can potentially increase risks to children's rights and freedoms (Bygrave, 1998; Singla, 2024). These legal dynamics reflect a sustained global commitment to building a digital ecosystem that promotes technological progress and protects children as the most vulnerable group, so that they can grow and participate in the digital society with a sense of security.

### Personal Data Protection Regulations in the Digital Age

Personal data protection regulations have become increasingly important in the digital age as technological advances continue changing how data is collected, processed, and used globally. Various jurisdictions have established robust frameworks to protect individual privacy rights while balancing innovation and privacy protection. In Indonesia, similar efforts have been realized by developing a personal data protection regulatory framework, in which the Personal Data Protection Law (PDP Law) serves as an important legislative measure to guarantee privacy rights and personal

data security amid the rapid growth of information technology and digital services.

The Personal Data Protection Law (PDP Law) provides a comprehensive regulatory framework that regulates various important aspects, ranging from data protection principles and the classification of personal data types to governance and security mechanisms in data management. In addition, this law also mandates the establishment of a data protection commission that has a strategic role in enforcing the law, overseeing the implementation of regulations, and handling various cases of data violations. The existence of this legal framework not only serves as an essential foundation for strengthening the protection of individual privacy rights but also plays a crucial role in building public trust in the digital ecosystem, thereby supporting the sustainable growth of Indonesia's digital economy (Mayasari, 2023; Prastyanti & Sharma, 2024).

Indonesia's digital economy, now the largest in Southeast Asia, faces serious challenges related to data breaches, which continue to occur, especially in vital sectors such as e-commerce and financial technology-based lending services (peer-to-peer lending). These incidents underscore the need to implement more comprehensive and effective data protection policies. Compared to other countries in the region, such as Hong Kong and Malaysia, Indonesia has made progress in developing a regulatory framework. However, there are still significant weaknesses, particularly in terms of establishing more stringent laws and the existence of independent institutions or special commissions that consistently monitor and enforce personal data protection rules to respond to the complexity of risks in the ever-evolving digital era (Shahrullah et al., 2024; Sudarwanto & Kharisma, 2022).

### Theoretical Approach: Privacy by Design

Privacy by Design (PD) is an approach that emphasizes the importance of integrating privacy protection from the initial planning and development stages of a system or technology, rather than as an additional solution after the system is already in operation. In other words, privacy is viewed as a fundamental element that must be embedded in technology's architecture, mechanisms, and processes to prevent potential privacy violations early on (Schaar, 2010). This approach was born in response to the rapid development of technology, which often presents complex privacy risks that are difficult to address if only considered after the system has been implemented.

The theoretical basis of Privacy by Design (PbD) emphasizes integrating privacy aspects into technical and organizational measures from the early stages of system and process design. This approach requires the early identification of potential privacy risks. It ensures that privacy protection features are embedded directly into the system architecture, rather than added later as a temporary solution. Its implementation requires cross-disciplinary collaboration involving legal experts, system architects, and software developers to design systems that respect users' privacy rights and comply with data protection laws. Such interdisciplinary collaboration is key to balancing technical and legal dimensions, while supporting compliance with global regulations such as the General Data Protection Regulation (GDPR) (Rommetveit & van Dijk, 2022; Schaar, 2010; Sion et al., 2019).

Privacy by Design (PbD) plays a vital role in developing a framework capable of responding to the challenges of enormous data complexity and social data mining practices by embedding privacy principles directly into data processing technology. Through this approach, privacy protection is not treated as an obstacle, but rather as an integral part of the system that enables a balance between personal data security and the optimization of large-scale data utilization. Integrating privacy protection from the outset of system design is crucial, as it minimizes potential privacy violations without reducing opportunities for exploring new knowledge contained in massive data analytics (Monreale et al., 2014).

Privacy by Design, as proposed by Ann Cavoukian, emphasizes that privacy protection must be proactively designed from the conception stage of a system, rather than added later. This can be achieved by integrating privacy elements such as automatic privacy settings (privacy by default), transparency, and data management throughout its life cycle into the school's curriculum and technological infrastructure. For example, through the implementation of a learning design framework that allows students to control their data, the use of privacy-centric

analytics, and educational consent mechanisms and privacy interfaces so that privacy protection is not only a technical obligation but an integral part of an ethical and data-aware learning experience (Hoel & Chen, 2016).

The seven key principles of Privacy by Design outlined in Cavoukian (2010) research are highly relevant in education, particularly in schools. These principles include a proactive rather than reactive approach, the application of privacy as the default setting, the integration of privacy protection into system design from the outset, ensuring full functionality without compromising data protection, the application of comprehensive end-to-end security, the enforcement of visibility and transparency in data management, and consistent respect for the privacy rights of each user. The implementation of these principles requires a comprehensive strategy that not only focuses on technical aspects but also involves close collaboration between educators, school administrators, policymakers, parents, and even students themselves, to create an educational ecosystem that is safe, transparent, and oriented towards the protection of personal data.

## METHODS

This study uses a qualitative method with a normative juridical approach, as the study focuses on analyzing legal constructs and identifying normative gaps in protecting children's privacy in the digital age. The normative juridical approach is carried out through a review of literature and secondary data, which includes primary, secondary, and tertiary legal materials. Primary legal materials include legislation such as the 1945 Constitution, Law Number 23 of 2002 concerning Child Protection as amended by Law Number 35 of 2014, and Law Number 27 of 2022 concerning Personal Data Protection. Secondary legal materials include scientific literature, legal journals, research results, and academic articles. In contrast, tertiary legal materials are legal dictionaries and encyclopedias that explain primary and secondary legal materials. Data collection techniques were carried out through a literature study by searching for relevant regulations, court decisions, and literature, which were then analyzed descriptively and qualitatively through the stages of inventory, classification, substantive review, identification of gaps and conflicts in norms, and assessment of compliance with international standards such as the Convention on the Rights of the Child (CRC). Data validity is maintained through source triangulation by comparing various legal literature and verifying the validity and currency of the laws and regulations used, so that the research results can provide recommendations for legal constructs that are more responsive to the needs of child privacy protection in the digital age.

A qualitative method with a normative legal approach was chosen as the most appropriate method for this study because it allows researchers to conduct an in-depth analysis of legislation, legal doctrines, and legal principles relevant to the protection of children's privacy in the digital age. This approach emphasizes understanding existing legal constructs and identifying normative gaps or loopholes that may arise due to the rapid development of digital technology, which is often not fully regulated. Using this method, researchers can systematically examine primary, secondary, and tertiary legal materials, including academic literature, jurisprudence, and policy documents, to produce comprehensive and contextual legal interpretations. In addition, the normative legal approach allows research to not only describe legal phenomena, but also evaluate the effectiveness of existing norms, assess the compatibility between legal principles and practices in the field, and provide recommendations for improving or strengthening regulations that are more responsive to digital challenges.

## RESULT

### Analysis of the Legal Framework for Child Privacy Protection in Indonesia

The legal framework in Indonesia that primarily regulates the protection of children's privacy is contained in the Personal Data Protection Law (PDP Law) (Sihabudin, 2023). This regulation provides a comprehensive and systematic legal basis for maintaining the security and confidentiality of personal data, including children's data, from unlawful collection, use, and processing practices. The PDP Law emphasizes the importance of explicit consent as a key requirement before data controllers or processors can process personal data. Specifically for children, who are considered a vulnerable group, the consent mechanism cannot be carried out directly. Still, it must be done through their parents or legal guardians who have legal responsibility (Shahrullah et al., 2024).

The legal framework for child privacy protection in Indonesia can be considered comprehensive, as it is regulated through various complementary regulations. Not only is it enshrined in the constitution, which guarantees the fundamental rights of every citizen, but this protection is also reinforced through the Child Protection Law and the Personal Data Protection Law (PDP Law). The PDP Law itself is designed as a special legal instrument that focuses on protecting personal data, requiring all parties involved in collecting, using, and storing data to comply with strict guidelines. In addition, the PDP Law also contains provisions on sanctions for violations, thereby emphasizing the importance of maintaining data security and confidentiality, especially for children's data as a group that is vulnerable to the risk of misuse (Shahrullah et al., 2024).

The Indonesian legal framework explicitly emphasizes the importance of protecting children's privacy through various levels of complementary regulations. Constitutionally, the 1945 Constitution guarantees every child the right to protection, including the right to privacy, which is the fundamental basis for all derivative policies and regulations. The Child Protection Law then affirms these rights by stipulating the obligations of the state, family, and community to protect children from all forms of abuse, exploitation, and disclosure of personal data that could endanger their development and safety. Furthermore, the Personal Data Protection Law provides specific technical mechanisms, such as the principles of lawful data collection, restrictions on use, access rights, and data control obligations, which are directly relevant to regulating the management of children's information in both digital and non-digital environments. This combination of constitutional, substantive, and technical regulations reflects a multi-layered approach that not only protects children's rights legally but also ensures their practical application in everyday life, including in the fields of education, digital services, and online media, thereby establishing a solid legal foundation for comprehensively protecting children's privacy and data security.

The existence of this key legislation encompasses a range of complementary legal instruments that seek to protect children's privacy, from laws governing the protection of personal data to regulations that specifically emphasize child protection. Each regulation is explained not only based on its main provisions—such as children's rights to information, data manager obligations, and oversight mechanisms—but also in terms of its practical relevance in the context of child privacy protection, for example, how the rules are applied in schools, digital services, or online platforms. With this systematic approach, it is clear that the state is striving to provide multi-layered protection that is not only normative but also operational, ensuring that children's rights to privacy and data security are effectively protected in various aspects of life, while preventing the misuse of personal data that could potentially harm children's development and safety.

Table 1. Legal Basis for Child Privacy Protection in Indonesia

| Legal Basis | Main Provisions | Relevance to Child Privacy Protection |
|---|---|---|
| Law No. 27 of 2022 concerning Personal Data Protection (PDP) | It regulates principles, data subject rights, and data controller obligations, including the special category of children's data as sensitive data. | It will become the main instrument for regulating children's privacy, requiring parental/guardian consent to process children's data. |
| 1945 Constitution Article 28G & 28I | It guarantees everyone's right to protection for themselves, their family, honor, dignity, and a sense of security. | Forms the constitutional basis for children's right to privacy, including protecting their personal data and dignity. |
| Law No. 23 of 2002 concerning Child Protection (in conjunction with Law No. 35 of 2014 and Law No. 17 of 2016) | Affirms the right of children to protection from abuse in the mass media, including personal identity, in the best interests of the child. | Protects children from exploitation of personal identity, such as the dissemination of photos/names in legal cases. |
| Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) (Law No. 19 of 2016) | Regulates personal data protection, prohibits personal information distribution without consent, and imposes sanctions for violations. | It provides a legal basis for protecting children's privacy in digital spaces such as social media and online applications. |
| Law No. 14 of 2008 on Public Information Disclosure | Regulates exempted information, including information that may reveal personal secrets. | Protects children's identity information from being disclosed to the public, especially in legal or medical cases. |
| Regulations of the Minister of Women's Empowerment and Child Protection (e.g., Regulation of the Minister of Women's Empowerment and Child Protection No. 8 of 2014 concerning Child Protection Policy) | Develop technical guidelines for child protection in various aspects, including privacy in the mass media. | Provide practical guidance on implementing child privacy protection by institutions, schools, the media, and families. |

The implementation of laws on personal data protection, especially those related to children, cannot be optimized without close collaboration between various stakeholders, including government agencies, the private sector, and civil society, each of which plays a vital role in promoting the enforcement of regulations and raising public awareness (Mayasari, 2023). With the rapid development of digital technology presenting new challenges, continuous legislative reform is crucial to ensure that regulations remain relevant and adaptive to the dynamics of the times. In this context, applying the principles of Privacy by Design and Privacy by Default must be the primary foundation, as these two principles ensure that privacy protection, especially for children, is automatically integrated into every data management process. Thus, protecting children's privacy is reactive to violations and proactive in preventing risks from the early stages of policy and digital system design (Mayasari, 2023).

Although the legislative framework provides a strong legal basis for protecting privacy, additional measures are still needed to ensure its effectiveness. These efforts include conducting periodic impact assessments to evaluate compliance with regulations, while identifying new gaps or risks that may arise with technological developments. In addition, there is a need for clear and standardized ethical guidelines as a reference for all stakeholders in managing personal data, so that potential implications for human rights, particularly privacy violations, can be prevented and addressed appropriately (Zuwanda et al., 2024).

### Regulatory Disharmony and Normative Vacuum

Analysis of the legal framework in Indonesia in the field of child personal data protection still faces serious problems in the form of overlapping and normative vacuums between the Child Protection Law, the Electronic Information and Transaction Law (EIT Law), and the Personal Data Protection Law (PDP Law). These three regulations have definitions, scopes, and protection mechanisms that are not yet harmonized, and often overlap and give rise to different interpretations. This situation creates fundamental legal uncertainty, especially for educational institutions that must develop comprehensive and consistent privacy policies. As a result, schools must navigate unsynchronized legal requirements, so that the practice of protecting children's personal data in the educational environment has the potential to be suboptimal or even contradictory. In this context, regulatory harmonization is an urgent need to protect children's privacy effectively and not be hampered by the fragmentation of existing norms (Uribe, 2020).

Overlapping regulations in protecting children's personal data are particularly evident in the fundamental differences in defining personal data and regulating protection mechanisms. Each law, such as the Child Protection Law, the ITE Law, and the PDP Law, sets different rules regarding consent, processing procedures, and the obligations and responsibilities of data controllers. These differences confuse institutions trying to comply with all provisions simultaneously, as no single guideline can be used as a reference. This situation creates legal uncertainty and slows down and complicates protecting children's personal data, especially in the education sector, where protecting children's rights should be a top priority (Oguejiofor et al., 2023).

The absence of specific norms governing oversight mechanisms and sanctions for privacy violations in the education sector poses serious problems for protecting children's data. Without clear regulatory guidelines and enforcement instruments, educational institutions often face difficulties in implementing personal data protection standards consistently and effectively. This situation not only weakens the protection of children's rights in the digital space but also can open up opportunities for inconsistent practices and even data abuse due to a lack of accountability (Kadir et al., 2025). Therefore, the urgency to develop a more comprehensive and harmonious policy framework is becoming increasingly clear, especially by including specific regulations and proportional sanctions. Thus, legal gaps can be closed, and protecting children's data in educational environments can be ensured to run more optimally and fairly.

### Personal Data Management Practices in Schools

In Indonesian schools, managing children's personal data still faces serious challenges due to the absence of standard protocols that comprehensively regulate data governance. Many schools only collect and store basic administrative data, such as names, addresses, and student academic records, but do not have adequate digital security systems. This situation makes children's personal data more vulnerable to leakage and misuse. This vulnerability is exacerbated by the use of online learning applications that often involve third-party services. In practice, the involvement of third parties has the potential to open up loopholes for data leaks or exploitation without the knowledge or explicit consent of the school or parents, creating a new dilemma in protecting children's privacy in the field of education (Jose, 2024).

Integrating digital technology, particularly artificial intelligence (AI), in educational settings increases the complexity of risks to children's privacy and data security. Although AI offers great potential to transform learning processes and improve the effectiveness of education, its use also presents serious challenges related to personal data management. This creates an urgent need to develop a robust protection framework and strategy to maintain the integrity and confidentiality of student data. Currently, school data management practices do not yet implement comprehensive security standards, such as data encryption, strict access controls, and routine security audits, even though these measures are essential to protect sensitive information from potential leaks or misuse (Jose, 2024).

The issue of personal data management in schools is not only technical in nature, but is also influenced by gaps in understanding and awareness of privacy among educators and administrators. Several studies show that many school staff do not yet have adequate competence

to recognize the risks associated with the collection, storage, and processing of student data, making it difficult to minimize potential privacy violations. The absence of clear operational guidelines and specific training programs on data governance further exacerbates this situation, as staff are not equipped with standard procedures or policy frameworks that can be used as a reference in managing sensitive information. Marín et al., (2023) emphasize that efforts to address this issue require coordination among stakeholders, including the government, educational institutions, and other relevant parties, in formulating data governance policies that are relevant and contextual to the academic environment.

In the current digital era, managing students' data in schools is an important aspect that must be considered to protect privacy and information security. Schools not only collect and store basic administrative data, but also use this data for various academic and non-academic purposes. Improper data management practices can lead to risks of leaks, misuse, or violations of student privacy rights. Therefore, it is essential to understand standard personal data management practices in schools and implement best practices that ensure security, transparency, and compliance with personal data protection principles. The following table presents examples of personal data management practices in schools, explanations, and recommendations for best practices.

Table 2. Examples of Personal Data Management Practices in Schools

| Aspect | Practical Examples in Schools | Explanation | Best Practices |
|---|---|---|---|
| Data Collection | Student registration forms contain full name, national identification number, address, religion, medical history, and parental data. | This data is required for administration and educational services, often without an explanation of the purpose of use. | Provide clear information about the purpose of data collection, request parental/student consent, and collect only relevant data. |
| Data Storage | Student data is stored in physical archives (folders) and the school's digital system. | Manual methods are prone to loss; digital systems are often unencrypted. | Store data digitally with encryption, perform regular backups, and secure physical archives in a locked location. |
| Use of Data | Data is used for class placement, grade reports, scholarship applications, or academic competitions. | Often, without explicit consent from parents or students for use beyond the original purpose | Use data for its original purpose and request additional consent if it is used for other purposes. |
| Data Distribution | Data is shared with third parties such as learning application providers, book publishers, or scholarship institutions. | There is a high potential for leaks without a data protection agreement. | Create a written agreement with third parties, including data protection, access restrictions, and regular audits. |
| Data Security | Some schools use passwords on digital report card applications or local servers. | Passwords are often easy to guess, and data is not adequately backed up. | Use strong passwords, two-factor authentication (2FA), data encryption, and access monitoring systems. |
| Data Access | Teachers, homeroom teachers, and administrators have full access to student data. | Without straightforward access controls, data is vulnerable to misuse. | Implement role-based access so that each staff member only accesses data as needed. |
| Data Deletion | After students graduate, records are kept indefinitely. | Irrelevant data remains stored, potentially subject to misuse. | Perform data deletion or anonymization once it is no longer relevant, in accordance with data retention policies. |

By emphasizing the development of consistent security and privacy standards and increasing institutional awareness and capacity, schools can build a sustainable data protection system that is in line with national regulations and international standards. These efforts include not only the formulation of internal policies, but also the strengthening of technical mechanisms through the implementation of best practices such as end-to-end data encryption, multi-factor authentication (MFA), role-based access control, regular data backups with separate storage, and the use of firewall-protected servers.

Governance-wise, schools need to develop clear data protection SOPs (Standard Operating Procedures), including procedures for data collection, storage, use, and distribution. Any form of data processing should always be based on informed consent from parents or guardians, with a transparent explanation of the purpose of use. To strengthen institutional capacity, schools can conduct regular training for teachers and staff on digital security awareness, data management ethics, and how to respond to information leaks.

Regular security audits and the implementation of privacy principles from the digital system design stage (privacy by design) need to be a reference from the planning stage to the implementation of digital systems in schools so that personal data management is more effective. This means that every learning application, administration platform, and database system must be designed with built-in security features and not just as an afterthought. Periodic security audits will help identify security gaps as early as possible, so that corrective measures can be taken immediately. With this comprehensive approach, schools can make optimal use of digital technology and online learning platforms while maintaining the privacy and security of children's information in an increasingly complex digital age.

### Comparison with International Regulations

The legal framework for child privacy protection in Indonesia is still relatively limited compared to more established regulations at the international level, such as the European Union's GDPR and the United States' COPPA. The GDPR, which came into effect in 2016, is widely recognized as the global standard in data protection, as it sets strict requirements regarding parental consent before the personal data of children under the age of 16 can be processed. This regulation protects children's data through detailed technical measures and ensures adequate oversight mechanisms and strict penalties for violators. Previous studies show that the GDPR approach includes proactive protection of children's rights in the digital world, including the obligation for service providers to be transparent about data collection and use, as well as clear legal responsibility for violators (Corning, 2024; Macenaite & Kosta, 2017). In comparison, Indonesian regulations still need to be strengthened to keep pace with developments in digital technology and the need for child protection in schools and online platforms.

Along these lines, COPPA in the United States, which has been in effect since 2000, is designed to provide exceptional protection for children's privacy in the digital world, especially for those under 13. This law requires every online service provider to obtain verifiable parental consent before collecting personal information from children. In addition, COPPA establishes strict compliance monitoring mechanisms and enforcement procedures for violators, thereby creating a comprehensive legal framework to prevent illegal data collection and misuse. This regulation also emphasizes the responsibility of service providers to be transparent in their use of children's data, gives parents the right to access and delete their children's information, and encourages proactive data security practices (Anderson, 2024; Reyes et al., 2018).

Conversely, Indonesia currently does not have specific regulations that explicitly govern the protection of children's privacy in the digital realm. They do not have clarity and enforcement mechanisms comparable to the GDPR in the European Union or COPPA in the United States. The existing legal framework tends to be general and does not provide detailed technical guidelines or procedures to ensure compliance by various parties managing children's data effectively. This situation creates a significant gap in protecting children's privacy, as no standards govern the safe collection, use, and storage of children's data. In addition, the lack of a comprehensive approach makes Indonesia face challenges in dealing with evolving digital risks, including potential data misuse, unauthorized access, and children's exposure to unsafe content, thus reinforcing the

urgency to develop regulations that are more holistic and responsive to the needs of child protection in the digital age (Corning, 2024).

To balance this regulatory gap, Indonesia must adopt stricter policies that align with international best practices as applied in the GDPR and COPPA. These efforts include strengthening clearer and verifiable parental consent mechanisms before children's data is processed, implementing special protection measures to maintain the confidentiality and security of children's data, and strict law enforcement against violators. In addition, Indonesia also needs to develop a comprehensive technical framework, including operational guidelines for schools, digital platforms, and online service providers, so that the protection of children's privacy is not only normative but can be implemented in practice. Thus, national regulations will be able to provide more effective security, strengthen public trust, and prepare a child-friendly digital ecosystem that is safe from potential data misuse.

## DISCUSSION

### Imbalance between Regulations and Practices in Schools

The imbalance between school regulations and practices, particularly in terms of data privacy protection, is a crucial issue that has various implications for education governance. Existing rules are often normative and abstract, failing to provide clear technical guidance and practical implementation guidelines for schools. As a result, educational institutions usually face confusion in translating legal provisions into daily operational procedures, especially those related to managing, storing, and distributing students' personal data. Several studies confirm the gap between the formal legal framework and actual practices in the field, where schools often rely on internal initiatives or ad-hoc policies without an adequate regulatory basis (Ghorashi et al., 2023; Hoel & Chen, 2018; Ismail, 2024). This situation highlights the need for more contextual, practical, and adaptive regulations to bridge the gap between data protection needs and the operational realities of education.

For example, although international regulations such as the General Data Protection Regulation (GDPR) explicitly emphasize the importance of protecting individual privacy, these regulations often do not provide specific and contextual technical guidelines for educational institutions. The absence of detailed operational guidelines leaves schools vulnerable, as they must interpret general rules themselves without a clear framework for implementation. As a result, many schools find it challenging to translate the normative provisions of the GDPR into concrete procedures, for example, regarding parental consent mechanisms, methods of storing and encrypting student data, and procedures for sharing information with third parties. This situation shows that without the support of more applicable technical instruments, regulations only function at the principle level. At the same time, schools continue to face significant challenges in maintaining the security and privacy of student data in their daily educational activities (Ghorashi et al., 2023).

In the education sector, issues related to data use consent are pretty complex. Existing policies are generally based on formal legal frameworks that often do not prioritize consent, especially when there are legitimate interests of educational institutions themselves (Hoel & Chen, 2018). This situation creates vulnerability, as the rights of students and parents to control their personal data can be marginalized by schools' administrative and operational needs. Therefore, privacy policies in education must be based not only on legal obligations but also on educational values that emphasize respect for individual rights, transparency, and the active participation of all parties.

Implementing artificial intelligence (AI) in education, while bringing various benefits such as personalized learning and increased administrative efficiency, simultaneously complicates data privacy and ethics issues. This technology operates by collecting, processing, and analyzing data on a large scale, including sensitive data on student behavior, academic performance, and even psychological aspects, which poses new risks not fully anticipated by the existing regulatory framework (Ismail, 2024). Current regulations cannot provide comprehensive protection against the ethical and technical impacts that arise, creating gaps in educational data governance. Therefore, academic institutions need to immediately develop more detailed, transparent, and

adaptive internal policies to ensure that the use of AI remains in line with privacy protection principles. At the same time, policymakers are also required to dynamically update regulations to respond to the new complexities arising from the use of AI, including accountability, data security, and the protection of students' rights.

To solve the increasingly complex challenges related to data privacy in the era of AI implementation, it's necessary to apply comprehensive and layered data governance policies. These policies should include not only formal rules, but also practical mechanisms that schools can consistently implement. In addition, educators need to be equipped with special training on the ethical, legal, and technical implications of AI use and data privacy management, so that they have sufficient capacity to maintain the security of student information in their daily practices (Ismail, 2024; Ismail & Aloshi, 2024). Furthermore, data literacy needs to be integrated into the education curriculum so that students develop critical awareness about how their data is collected, used, and protected. With clear technical guidelines and translating regulations into practical steps, schools can improve the protection of children's privacy and build a safer, more transparent, and responsible digital culture in the educational environment.

### The dilemma of cyber protection and information access rights

Schools currently face complex challenges in maintaining a balance between cybersecurity protection and fulfilling students' rights to access information. On the one hand, the increasing intensity and sophistication of cyber threats have prompted educational institutions to tighten their digital defense systems to protect students' and educators' personal data and sensitive information. However, overly strict security measures often limit students' access to various digital learning resources essential for their academic development (Watini et al., 2024). Conversely, if access is too relaxed, the risk of privacy violations, data leaks, and exploitation of personal information will be even higher. This situation highlights the urgency for schools to formulate data management strategies that focus on protection and ensure fair and proportional accessibility, so that security needs and the right to information can be balanced.

The key to addressing the dilemma between data protection and access to information lies in formulating policies that provide maximum protection without limiting students' fundamental right to knowledge. The world of education has unique characteristics that make it vulnerable to cybersecurity threats, including theft and leakage of personal data, phishing practices targeting teachers and students, and malware attacks that have the potential to damage digital learning infrastructure (Watini et al., 2024). These threats disrupt the smooth running of the teaching and learning process and pose a serious risk to system integrity and individual privacy. Therefore, a comprehensive solution is needed that combines cutting-edge protection technologies, such as implementing advanced encryption to secure data transmission, using multi-factor authentication to strengthen system access, and cybersecurity literacy and awareness training programs specifically designed for the educational context.

Educational institutions must develop proactive strategies emphasizing security technology and include a balanced policy framework to guarantee the right to access information and protect privacy (Mijwil et al., 2023). This approach is essential because increasingly dynamic digital threats require adaptive responses, not static rules. By utilizing cutting-edge technologies such as Artificial Intelligence (AI) and Machine Learning (ML), schools can perform early detection and predict cyberattack patterns, for example, identifying suspicious activities before they develop into serious violations. Implementing this AI and ML-based framework enables security systems to be reactive and preventive, thereby minimizing risks without sacrificing open access to the digital resources needed by students and teachers. Thus, a safe, inclusive digital education ecosystem is created to support the learning process oriented towards optimal use of technology (Bhardwaj & Kaushik, 2022).

A collaborative approach involving various stakeholders, from educational institutions to cybersecurity experts to policymakers, is a crucial strategic step in building a secure and inclusive digital education ecosystem. This cross-sector collaboration enables the formulation of more comprehensive protection strategies, as each party brings different perspectives, expertise, and experiences to address the complexity of cyber threats that are increasingly diverse and specific

to the school environment (Belmabrouk, 2023). In practice, efforts to balance protection needs with the principle of open access to education require in-depth analysis of new technological developments, such as cloud computing, the Internet of Things (IoT), and Artificial Intelligence, which are now widely integrated into learning systems. In addition, the resulting policies must also consider the real needs of stakeholders, including students, teachers, parents, and administrators, so that privacy protection and access to information can run harmoniously.

Schools can strengthen protection against cyber threats while ensuring open access to information by implementing a holistic and layered cybersecurity framework. This includes integrating the latest security technologies with adaptive governance and capacity building through regular training programs designed to meet the practical needs of educators, staff, and students. In addition, internal policies must be formulated flexibly to adapt to the dynamics of technological developments without compromising established security standards. This balanced approach enables the creation of a digital education ecosystem that is resilient in the face of potential cyber attacks and continues to support students' rights to broad access to information, so that the benefits of digital learning can be optimally realized in a safe and trusted environment.

### The Importance of Implementing Privacy by Design in Education

Implementing the Privacy by Design (PbD) principle in the context of digital education plays a crucial role in building a safe, transparent, and student rights-oriented online learning ecosystem. This concept emphasizes that privacy should not be an afterthought but integrated from the early stages of digital learning system design. Thus, every feature, data collection process, and student data management is proactively designed to comply with personal data protection standards, reduce the risk of information leaks, and strengthen trust between schools, students, and parents. Furthermore, implementing PbD can also improve digital literacy in terms of privacy, provide a strong foundation for developing an information security culture in the educational environment, and support the creation of ethical and sustainable learning technology innovations.

One of the fundamental principles of Privacy by Design is the application of default settings that prioritize personal data protection from the outset. Every online learning platform must be designed to automatically apply the highest privacy standards without waiting for user intervention. With this strategy, the potential risk of data leaks or misuse can be minimized because the system only collects and stores genuinely relevant information necessary for learning purposes. This approach strengthens digital security and builds trust between users and education service providers, as students, parents, and educators feel more protected in their online learning activities. In addition, default privacy configurations also serve as a form of proactive prevention against unauthorized access, in line with the recommendations of Robol et al., (2017), while encouraging educational institutions to be more responsible in data governance.

Parental involvement in the consent process is essential in implementing Privacy by Design in the digital education environment. Schools must establish open, transparent, and accessible communication mechanisms with parents and guardians to obtain comprehensive information about how their children's personal data is collected, processed, stored, and protected from potential misuse. This transparency not only serves to comply with regulations that require parental consent before children's data is processed, but also serves as a strategic means of strengthening public trust in educational institutions. Through active parental involvement, schools can create better control over data flows, provide space for parents to ask questions or raise objections, and ensure that all data management practices are ethical and responsible. This approach emphasizes that protecting children's privacy is a legal obligation and a moral and social responsibility for educational institutions (Robol et al., 2017).

Another crucial aspect in implementing Privacy by Design is maintaining a high level of transparency in every data management practice in the educational environment. Educational institutions are required to openly explain the procedures used in the collection, processing, storage, and destruction of personal data, as well as to develop privacy policies that are not only comprehensive but also easily accessible and understandable to all stakeholders, including students, parents, teachers, and academic staff. This transparency must include detailed explanations of how data may be shared with third parties, the purposes for which the data will

be used, and assurances that all parties receiving the data operate according to strict data protection standards. By providing clear, consistent, and communicative guidance, educational institutions ensure compliance with regulations and build a sense of security and trust within the academic community. In line with the perspective of Asghar et al., (2019) and Robol et al., (2017), this practice emphasizes that openness in data governance is the primary foundation in creating a digital learning system that is ethical, accountable, and oriented towards protecting individual privacy rights.

### The Urgency of Digital Literacy for the Education Ecosystem

Digital literacy plays a crucial role in building a healthy and competitive education ecosystem, as these skills are relevant not only for students but also for teachers and parents as key stakeholders. Mastering digital literacy enables them to understand, evaluate, and utilize technology and information appropriately in the context of learning and everyday life. Amidst the rapid development of technology increasingly integrated into the education system, digital literacy is the foundation for ensuring that the teaching and learning process is interactive, collaborative, and safe.

Teachers play a central role in integrating digital literacy into the learning process because the successful application of technology in education depends heavily on their competence in mastering and utilizing digital devices. Teachers' digital skills enrich teaching methods and open opportunities for students to develop 21st-century skills, such as critical thinking, problem solving, creativity, and collaboration. The findings of Temirkhanova et al., (2024) confirm that teachers with good digital literacy can create a learning ecosystem that is more dynamic, interactive, and relevant to the needs of the times. Such a learning environment has been proven to improve students' technical abilities in using technology while stimulating their creative capacity to produce innovative works.

For students, digital literacy plays a very strategic role in shaping learning and life skills relevant to the demands of the times. Mastery of digital literacy not only supports them in understanding and using technology effectively but also fosters the ability to learn independently, adapt to change, and take advantage of the opportunities offered by the digital ecosystem. Schools that systematically integrate technological tools and digital literacy strategies into their curriculum contribute significantly to equipping students with special educational needs to manage the learning process more autonomously and inclusively (Temirkhanova et al., 2024). Furthermore, these skills form an essential foundation for developing students' capacity to critically, creatively, and ethically interact with digital content. This improves the quality of learning and serves as a key safeguard in protecting students' personal data, privacy, and psychological well-being as they face various challenges in the ever-evolving digital world.

For parents, a deep understanding of digital literacy is just as important as it is for students and teachers, as it enables them to support their children's education more effectively and continuously. With adequate digital literacy, parents can understand the dynamics of technology use in learning, recognize the benefits and risks that may arise, and guide their children to use digital devices wisely and responsibly. Comprehensively designed digital literacy strategies also help parents realize their rights and responsibilities in digital citizenship, including aspects of privacy protection, data security, and ethics of interacting in the virtual world. This understanding not only strengthens support for children's academic development but also equips families with the ability to create a safe, healthy, and productive digital environment, so that modern education can run in harmony with the protection of children's welfare in the technological era.

Increasing digital literacy among various education stakeholders requires a systematic and sustainable approach, which involves developing training programs to meet their needs. These adaptive and contextual programs help educators strengthen their technical and pedagogical competencies and encourage the creation of cross-role collaboration spaces between teachers, parents, and students (Palacios-Rodríguez et al., 2024). This collaborative approach reduces the digital skills gap while strengthening synergies in building educational practices relevant to the dynamics of the digital age. Furthermore, with intensive collaboration, the

education community can more easily adapt to rapid technological changes and ensure that the learning strategies implemented remain inclusive and effective (Grosseck et al., 2023).

## CONCLUSION

The digital age has brought significant changes in how children and adolescents interact with the world, particularly in education, where schools increasingly rely on digital products and services to support the learning process. However, the presence of various edtech providers poses a serious risk to children's privacy protection because there are still many data management practices that are prone to violating their rights. This study analyzes the legal framework for protecting the privacy of children and adolescents in Indonesia, highlighting the dilemma between the need for cyber protection and the fulfillment of the right to access information in schools. The study results show that Indonesia's legal framework still faces several problems, such as overlapping regulations, normative gaps, and the absence of standard protocols in the practice of personal data management in the educational environment. Compared to international regulations such as the GDPR in the European Union and COPPA in the United States, Indonesia still lags behind in strengthening norms, oversight mechanisms, and law enforcement. On the other hand, schools are in a difficult position to balance maintaining student data security with providing them with their right to access information as part of the learning process. Therefore, the application of the Privacy by Design principle in the development of digital education systems, accompanied by increased digital literacy for teachers, students, and parents, is key to building a safe, inclusive, and equitable education ecosystem in the digital age.

## REFERENCES

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi dan Privasi pada Pengguna Smartphone Android di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 115. https://doi.org/10.21456/vol8iss2pp115-122

Anderson, H. (2024). The Guardian of the Digital Era: Assessing the Impact and Challenges of the Children' s Online Privacy Protection Act. *Law and Economy*, *3*(2), 6– 10. https://doi.org/10.56397/LE.2024.02.02

Asghar, M. N., Kanwal, N., Lee, B., Fleury, M., Herbst, M., & Qiao, Y. (2019). Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective. *IEEE Access*, *7*, 111709– 111726. https://doi.org/10.1109/ACCESS.2019.2934226

Bayne, S. (2015). Teacherbot: Interventions in Automated Teaching. *Teaching in Higher Education*, *20*(4), 455– 467. https://doi.org/10.1080/13562517.2015.1020783

Belmabrouk, K. (2023). *Cyber Criminals and Data Privacy Measures* (pp. 198– 226). https://doi.org/10.4018/979-8-3693-1528-6.ch011

Bhardwaj, A., & Kaushik, K. (2022). Predictive Analytics-Based Cybersecurity Framework for Cloud Infrastructure. *International Journal of Cloud Applications and Computing*, *12*(1), 1– 20. https://doi.org/10.4018/IJCAC.297106

Bygrave, L. (1998). Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, *6*(3), 247– 284. https://doi.org/10.1093/ijlit/6.3.247

Cavoukian, A. (2010). Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society*, *3*(2), 247– 251. https://doi.org/10.1007/s12394-010-0062-y

Corning, G. P. (2024). The Diffusion of Data Privacy Laws in Southeast Asia: Learning and the Extraterritorial Reach of the EU' s GDPR. *Contemporary Politics*, *30*(5), 656– 677. https://doi.org/10.1080/13569775.2024.2310220

Ghorashi, S. R., Zia, T., Bewong, M., & Jiang, Y. (2023). An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing. *Applied Sciences*, *13*(23), 12727. https://doi.org/10.3390/app132312727

Grosseck, G., Bran, R. A., & Ț îru, L. G. (2023). Digital Assessment: A Survey of Romanian Higher

Education Teachers' Practices and Needs. *Education Sciences*, *14*(1), 32. https://doi.org/10.3390/educsci14010032

Han, H. J. (2022). How Dare They Peep into My Private Life? *Human Rights Watch*. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Hoel, T., & Chen, W. (2016). Privacy-driven Design of Learning Analytics Applications – Exploring the Design Space of Solutions for Data Sharing and Interoperability. *Journal of Learning Analytics*, *3*(1). https://doi.org/10.18608/jla.2016.31.9

Hoel, T., & Chen, W. (2018). Privacy and Data Protection in Learning Analytics Should be Motivated by an Educational Maxim—Towards a Proposal. *Research and Practice in Technology Enhanced Learning*, *13*(1), 20. https://doi.org/10.1186/s41039-018-0086-8

Ismail, I. A. (2024). *Protecting Privacy in AI-Enhanced Education* (pp. 117– 142). https://doi.org/10.4018/979-8-3693-0884-4.ch006

Ismail, I. A., & Aloshi, J. M. (2024). *Data Privacy in AI-Driven Education* (pp. 223– 252). https://doi.org/10.4018/979-8-3693-5443-8.ch008

Jose, D. (2024). Data Privacy and Security Concerns in AI-Integrated Educational Platforms. *Recent Trends in Management and Commerce*, *5*(2), 87– 91. https://doi.org/10.46632/rmc/5/2/19

Kadir, A., Stevens, A. J., Takahashi, E. A., & Lal, S. (2025). Child Public Health Indicators for Fragile, Conflict-Affected, and Vulnerable Settings: A Scoping Review. *PLOS Global Public Health*, *5*(3), e0003843. https://doi.org/10.1371/journal.pgph.0003843

Macenaite, M. (2017). From Universal Towards Child-specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, *19*(5), 765–779. https://doi.org/10.1177/1461444816686327

Macenaite, M., & Kosta, E. (2017). Consent for Processing Children's Personal Data in the EU: Following in US Footsteps? *Information & Communications Technology Law*, *26*(2), 146–197. https://doi.org/10.1080/13600834.2017.1321096

Marín, V. I., Carpenter, J. P., Tur, G., & Williamson-Leadley, S. (2023). Social Media and Data Privacy in Education: An International Comparative Study of Perceptions Among Pre-Service Teachers. *Journal of Computers in Education*, *10*(4), 769–795. https://doi.org/10.1007/s40692-022-00243-x

Mayasari, H. (2023). A Examination on Personal Data Protection in Metaverse Technology in Indonesia: A Human Rights Perspective. *Journal of Law, Environmental and Justice*, *1*(1), 64–85. https://doi.org/10.62264/jlej.v1i1.4

Mijwil, M., Omega John Unogwu, Youssef Filali, Indu Bala, & Humam Al-Shahwani. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of CyberSecurity*, *2023*, 57–63. https://doi.org/10.58496/MJCS/2023/010

Milkaite, I., De Wolf, R., Lievens, E., Leyn, T. De, & Martens, M. (2021). Children's Reflections on Privacy and the Protection of Their Personal Data: A Child-Centric Approach to Data Protection Information Formats. *Children and Youth Services Review*, *129*, 106170. https://doi.org/10.1016/j.childyouth.2021.106170

Monreale, A., Rinzivillo, S., Pratesi, F., Giannotti, F., & Pedreschi, D. (2014). Privacy-by-Design in Big Data Analytics and Social Mining. *EPJ Data Science*, *3*(1), 10. https://doi.org/10.1140/epjds/s13688-014-0010-4

Oguejiofor, B. B., Omotosho, A., Abioye, K. M., Alabi, A. M., Oguntoyinbo, F. N., Daraojimba, A. I., & Daraojimba, C. (2023). A Review on Data-Driven Regulatory Compliance in Nigeria. *International Journal of Applied Research in Social Sciences*, *5*(8), 231–243. https://doi.org/10.51594/ijarss.v5i8.571

Palacios-Rodríguez, A., Llorente-Cejudo, C., Lucas, M., & Bem-haja, P. (2024). Macroassessment of Teachers' Digital Competence. DigCompEdu Study in Spain and Portugal. *RIED-Revista*

*Iberoamericana de Educación a Distancia*, *28*(1). https://doi.org/10.5944/ried.28.1.41379

Prastyanti, R. A., & Sharma, R. (2024). Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. *Journal of Human Rights, Culture and Legal System*, *4*(2), 354–390. https://doi.org/10.53955/jhcls.v4i2.200

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018). "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies*, *2018*(3), 63–83. https://doi.org/10.1515/popets-2018-0021

Robol, M., Salnitri, M., & Giorgini, P. (2017). *Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework* (pp. 236–250). https://doi.org/10.1007/978-3-319-70241-4_16

Rommetveit, K., & van Dijk, N. (2022). Privacy Engineering and the Techno-Regulatory Imaginary. *Social Studies of Science*, *52*(6), 853–877. https://doi.org/10.1177/03063127221119424

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x

Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Review*, *10*(1), 1. https://doi.org/10.20956/halrev.v10i1.5016

Sianipar, K. R. D., Rahmayanti, R., & Gultom, A. (2025). Protection of Privacy Rights in The Digital Era Between Cybersecurity and Freedom of Information. *International Journal of Law and Society*, *2*(3), 247–252. https://doi.org/10.62951/ijls.v2i3.701

Sihabudin, S. (2023). Expanding the Limitations of the Protection and Processing of Children's Personal Data: An Overview of Current Regulations, Challenges, and Recommendations. *Brawijaya Law Journal*, *10*(1), 59–71. https://doi.org/10.21776/ub.blj.2023.010.01.04

Singla, A. (2024). The Evolving Landscape of Privacy Law: Balancing Digital Innovation and Individual Rights. *Indian Journal of Law*, *2*(1), 1–6. https://doi.org/10.36676/ijl.v2.i1.01

Sion, L., Dewitte, P., Van Landuyt, D., Wuyts, K., Emanuilov, I., Valcke, P., & Joosen, W. (2019). An Architectural View for Data Protection by Design. *2019 IEEE International Conference on Software Architecture (ICSA)*, 11–20. https://doi.org/10.1109/ICSA.2019.00010

Solove, D. J. (2008). The End of Privacy? *Scientific American*, *299*(3), 100–106. https://doi.org/10.1038/scientificamerican0908-100

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's Understanding of Personal Data and Privacy Online – A Systematic Evidence Mapping. *Information, Communication & Society*, *24*(4), 557–575. https://doi.org/10.1080/1369118X.2019.1657164

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0193

Temirkhanova, M., Abildinova, G., & Karaca, C. (2024). Enhancing Digital Literacy Skills Among Teachers for Effective Integration of Computer Science and Design Education: A Case Study at Astana International School, Kazakhstan. *Frontiers in Education*, *9*. https://doi.org/10.3389/feduc.2024.1408512

Uribe, D. (2020). Privacy Laws, Non-Fungible Tokens, and Genomics. *The Journal of The British Blockchain Association*, *3*(2), 1–10. https://doi.org/10.31585/jbba-3-2-(5)2020

Watini, S., Davies, G., & Andersen, N. (2024). Cybersecurity in Learning Systems: Data protection and privacy in educational information systems and digital learning environments. *International Transactions on Education Technology (ITEE)*, *3*(1), 26–35. https://doi.org/10.33050/itee.v3i1.665

Zuwanda, Z. S., Lubis, A. F., Solapari, N., Sakmaf, M. S., & Triyantoro, A. (2024). Ethical and Legal Analysis of Artificial Intelligence Systems in Law Enforcement with a Study of Potential Human

Rights Violations in Indonesia. *The Easta Journal Law and Human Rights*, *2*(03), 176–185. https://doi.org/10.58812/eslhr.v2i03.283