The Easta Journal Law and Human Rights
Vol. 3, No. 01, October 2024, pp. 20 - 29
ISSN: 2985-7112, DOI: 10.58812/eslhr.v3i01

An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia

Loso Judijanto[1], Nuryati Solapari[2], Irman Putra[3]
[1] IPOSS Jakarta
[2] Universitas Sultan Ageng Tirtayasa
[3] Sekolah Tinggi Hukum Militer AHM-PTHM

Article Info

Article history:

Received Oct, 2024
Revised Oct, 2024
Accepted Oct, 2024

Keywords:

Data Protection
Indonesia
Juridical Normative Analysis
Personal Data Protection Law
Right to Privacy

ABSTRACT

This paper analyzes the gap between data protection regulations and the implementation of the right to privacy in Indonesia from a juridical normative perspective. Despite the enactment of the Personal Data Protection (PDP) Law in 2022, significant challenges remain in ensuring the protection of personal data. These challenges include vague legal definitions, limited enforcement mechanisms, and insufficient provisions for regulating emerging digital technologies such as artificial intelligence and big data. Additionally, public awareness of privacy rights remains low, further exacerbating the ineffective implementation of the law. Through a comparative analysis with international frameworks like the GDPR, this paper highlights key areas for improvement in Indonesia's data protection landscape. Recommendations include establishing a centralized data protection authority, enhancing legal provisions for technological advancements, and increasing public engagement to ensure the effective protection of privacy rights in the digital age.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

The swift progression of digital technology has revolutionized numerous facets of life, encompassing communication, business, education, and governmental services. The digital revolution presents significant prospects for economic growth and social progress, yet it has also presented new difficulties concerning data protection and privacy rights [1], [2]. The proliferation of online platforms, digital transactions, and social media in Indonesia has markedly augmented the quantity of personal data amassed, retained, and processed by both commercial and state organizations [3], [4]. Consequently, apprehensions regarding the security and privacy of personal information have become paramount.

The right to privacy is a fundamental human right, codified in multiple international legal documents, including the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), to which Indonesia is a signatory [5]–[7]. Indonesia has acknowledged the significance of privacy at the national level through its Constitution and the implementation of the Personal Data Protection Law, which seeks to govern the

collection, processing, and utilization of personal data [7]–[9].Nonetheless, despite the presence of this legal framework, a substantial disparity persists between the regulatory stipulations and their practical execution.

The enforcement of data protection legislation in Indonesia encounters numerous obstacles. The issues encompass ambiguous legislative definitions, inadequate enforcement methods, insufficient public knowledge of data privacy rights, and the dynamic nature of digital threats [9], [10]. Moreover, Indonesia's regulatory framework frequently fails to align with technological improvements, resulting in discrepancies in the safeguarding of people' personal data [11], [12]. The implementation of the Personal Data Protection Law represents progress; yet, concerns persist about its efficacy in safeguarding privacy rights in the digital era.

This study aims to examine the disparity between data protection rules and the actual enforcement of the right to privacy in Indonesia from a normative legal standpoint. Normative juridical analysis examines legal norms and principles to assess the adequacy of existing legislation in safeguarding private rights and their application in practical contexts. This paper examines the legislative framework of data protection in Indonesia to identify deficiencies in the existing regulatory structure and offer ideas for enhancing the enforcement of privacy laws.

This research is significant due to its potential to enhance the debate on data protection and privacy in Indonesia. The advancement of digital technology in Indonesia necessitates robust legal protection for personal data to secure citizens' rights and uphold public faith in the digital framework. This document will examine the subsequent critical inquiries: What are the primary discrepancies between data protection legislation and the right to privacy in Indonesia? In what manner do these discrepancies influence the effective enforcement of privacy rights? What improvements are necessary to enhance privacy protection inside the digital economy?

2. LITERATURE REVIEW

2.1 The Concept of Privacy and Data Protection

Privacy is a fundamental human right, essential for protecting personal autonomy and freedom. It encompasses control over personal information, protection of personal space, and confidentiality of communications, allowing individuals to decide what information is shared and with whom. [13], [14] defined privacy as the ability to control personal information boundaries and avoid unwarranted intrusions. International legal instruments like Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) enshrine this right, forming the basis for national data protection laws. As digital technologies evolve, stronger data protection frameworks are needed to address risks related to data collection and processing, with scholars emphasizing the balance between information flow and privacy rights [13], [15], [16]. Theories like Westin's and Solove's taxonomy of privacy issues, including information collection, processing, and dissemination, shape the legal frameworks protecting privacy in the digital age [16].

2.2 The Global Landscape of Data Protection Regulations

Data protection laws have significantly evolved in response to growing privacy concerns in the digital age, with the European Union's General Data Protection Regulation (GDPR) being one of the most prominent frameworks. Implemented in 2018, the GDPR sets a high standard for data protection, emphasizing transparency, accountability, and the rights of data subjects, including access,

rectification, erasure (the "right to be forgotten"), and data portability, which have become benchmarks for other nations' privacy laws [17]–[19]. In the United States, data protection follows a sectoral approach, with specific laws like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the Children's Online Privacy Protection Act (COPPA) for children's online data. However, the U.S. lacks a comprehensive federal data protection law like the GDPR, relying instead on state-level laws such as California's Consumer Privacy Act (CCPA) to fill federal regulatory gaps [14], [20]. Other countries, including Canada, Australia, Japan, and Singapore, have developed their own comprehensive data protection laws, which share common elements like personal data protection, consent requirements, and secure data processing measures.

2.3 Data Protection and Privacy in Indonesia

Indonesia has recognized the importance of data protection in the face of increasing digitalization and privacy risks, with the Personal Data Protection Law, enacted in 2022, serving as its primary legal framework. Modeled after the GDPR, this law outlines the rights of data subjects, obligations for data controllers and processors, and enforcement mechanisms. However, despite its comprehensive scope, significant gaps in implementation persist. [21] highlights issues such as unclear legal definitions and weak enforcement mechanisms, while [7] points to challenges in regulating large tech companies that handle vast amounts of personal data. One of the key obstacles is enforcing privacy regulations in a rapidly evolving digital environment, with [22] noting that limited resources and technical expertise hinder the government's ability to monitor compliance, leading to data breaches and a lack of accountability. Public awareness of the law is another issue, as many Indonesians remain unaware of their data privacy rights, reducing the likelihood of holding organizations accountable for violations [23]. Additionally, the law struggles to keep pace with technological advancements like AI and big data analytics, raising concerns about consent and data processing, as [16] emphasizes the need for more specific provisions to address these emerging technologies and ensure privacy protection in the digital age.

3. RESEARCH METHODS

3.1 Research Design

The research adopts a juridical normative design, focusing on the systematic review and analysis of legal norms, statutes, regulations, and policies related to data protection and privacy rights in Indonesia. This approach is well-suited for evaluating the effectiveness of Indonesia's legal framework in safeguarding privacy and ensuring data protection, especially in the face of emerging digital threats. The study will utilize primary legal materials, including Indonesia's Constitution, the Personal Data Protection Law (2022), and the Electronic Information and Transactions (ITE) Law, which collectively provide the legal foundation for privacy protection. Secondary legal materials, such as legal commentaries, academic papers, reports, and case studies, will offer additional insights into the interpretation and practical application of these laws. To complement the juridical normative approach, descriptive analysis will be used to identify and describe gaps between legal norms and their enforcement, emphasizing the

discrepancies between the protections intended by law and their real-world implementation.

3.2 Data Collection

The data for this study is derived from both legal documents and scholarly literature. The sources of data are categorized as follows:

a. Primary Legal Materials

The study will analyze several key legal frameworks related to data protection and privacy in Indonesia, starting with the Indonesian Constitution, which provides the foundational provisions for the right to privacy. Central to the analysis is the Personal Data Protection Law (2022), which will be thoroughly examined to evaluate its provisions on data protection, individual privacy rights, and the obligations of data controllers and processors. Additionally, the Electronic Information and Transactions (ITE) Law, which governs online activities, including privacy, data misuse, and cybercrime, will be reviewed for its relevance to digital data protection. The study will also consider other relevant laws and government regulations, particularly those imposing specific privacy obligations on certain industries.

b. Secondary Legal Materials

The study will review a variety of sources to provide a comprehensive analysis of Indonesia's data protection framework. Legal commentaries and academic papers will be examined to offer critical perspectives and expert opinions, situating Indonesia's legal provisions within broader global trends and addressing local enforcement challenges. Government reports and policy papers, particularly from agencies such as the Ministry of Communication and Information Technology, will be analyzed to understand the government's approach to privacy rights and the enforcement of data protection regulations. Additionally, case studies and court rulings on privacy violations and data breaches will be reviewed to assess how Indonesian courts interpret and apply data protection laws, offering practical insights into the real-world implementation of these legal norms.

3.3 Data Analysis

The data analysis will be conducted in two stages: normative legal analysis and comparative analysis, which together will offer a comprehensive understanding of Indonesia's current legal framework and its gaps. The normative legal analysis will examine legal norms, principles, and rules governing personal data protection and privacy rights, focusing on the content of the Personal Data Protection Law and related regulations, assessing their alignment with international standards like the GDPR. It will also evaluate the legal obligations of data controllers and processors, and how these are enforced, alongside the rights of data subjects, such as access, correction, and erasure of personal data, identifying areas where the framework may be inadequate, particularly in enforcement and public awareness. The comparative analysis will contrast Indonesia's data protection laws with other countries, particularly the European Union's GDPR, to identify best practices and differences in legal definitions, enforcement mechanisms, and penalties for non-compliance. This will provide a global perspective on the effectiveness of Indonesia's data protection measures and offer

recommendations for enhancing its legal framework.

4. RESULTS AND DISCUSSION

4.1 Results

1. Gaps in the Legal of the Personal Data Protection Law (PDP Law)

Analysis of Indonesia's Personal Data Protection Law (PDP Law) revealed several key areas where it fails to provide comprehensive protection of personal data and ensure the right to privacy. These gaps were identified as follows:

a. Unclear Definitions and Scope While the PDP Law sets out general principles for data protection, certain key terms remain unclear. For example, the concept of 'personal data' lacks specificity, especially when discussing new types of data generated by new technologies such as artificial intelligence (AI) and the Internet of Things (IoT). This creates ambiguity in determining what data is covered by the law and limits its applicability to the modern digital environment. In addition, the scope of the law does not clearly outline the responsibilities of all actors in the digital ecosystem, including third-party processors and international data transfer practices.

b. Another significant gap in the PDP Law is the absence of strong enforcement mechanisms. While the law outlines penalties for non-compliance, there is no clear guidance on how these penalties will be enforced. The lack of a dedicated data protection authority (DPA) with the power to monitor, investigate, and enforce the law has resulted in weak oversight. This shortcoming has been highlighted in several data breach cases where organizations were not held accountable due to regulatory inaction or lack of resources for enforcement.

c. Inadequate Provisions for Technological Advancements the PDP Law struggles to keep pace with the rapid advancements in digital technology. Provisions related to data consent, collection, and processing are inadequate when considering technologies such as machine learning, big data analytics, and AI, which often rely on the collection and analysis of large amounts of data. The law does not address the nuances of how these technologies may intrude on individuals' privacy, especially in cases where data is passively collected or aggregated from multiple sources without explicit consent.

d. Lack of Public Awareness and Data Subject Empowerment Public awareness of privacy rights under the PDP Law is low in Indonesia. This is particularly concerning given the increasing number of data breaches and privacy violations. Many people are unaware of their rights to access, correct, or delete their personal data, and this lack of knowledge weakens the efficacy of the law. In addition, there are no established channels for individuals to report

breaches or seek assistance, which limits the empowerment of data subjects in exercising their rights.

These results show that, Indonesia's Personal Data Protection Law (PDP) has been criticised for its shortcomings in providing comprehensive data protection and ensuring privacy rights. The definition and scope of the law is ambiguous, especially regarding new types of data generated by AI and IoT, which complicates its application in the digital era [23], [24]. In addition, the absence of strong enforcement mechanisms, including a dedicated data protection authority, weakens oversight and accountability, as seen in cases of data breaches where organisations avoid punishment due to regulatory inaction [25], [26] . The law also struggles to keep pace with technological advances, lacking provisions for consent and data processing in the context of machine learning and big data analytics, which often involve passive data collection without explicit consent [26]. In addition, public awareness of privacy rights under the PDP Law is still low, limiting the empowerment of data subjects to exercise their rights and report violations [27].

2. ***Implementation Challenges***

This study also found several challenges related to the implementation of the PDP Law, which further contribute to the gap between the legal provisions and the practical protection of privacy rights:

1. Fragmentation of Regulatory Bodies Data protection in Indonesia is regulated by multiple bodies, including the Ministry of Communications and Information Technology (Kominfo) and other sectoral regulators. This fragmented approach leads to inconsistencies in the enforcement of privacy regulations. For example, financial institutions may be subject to different privacy requirements compared to e-commerce platforms, creating confusion and regulatory overlap. The absence of a central authority to oversee data protection across sectors exacerbates this problem.
2. Weak Data Security Standards Enforcement of data security standards under the PDP Law is inconsistent. Many organisations lack the technical infrastructure and knowledge to implement adequate security measures to protect personal data. This has resulted in frequent data breaches, including high-profile incidents involving financial institutions and large technology companies. The lack of clear guidelines on data breach reporting and incident response further hinders regulators' ability to respond to privacy breaches in a timely manner.
3. Indonesia's legal framework lacks comprehensive rules for cross-border data transfers, which is a critical issue in today's global digital economy. The PDP Law does not provide clear criteria for the transfer of personal data to foreign entities, nor does it mandate the same level of protection for data processed outside Indonesia. This creates vulnerabilities, as personal data can be transferred to jurisdictions

with weaker privacy laws, increasing the risk of abuse.

The implementation of the Personal Data Protection Law (PDP) in Indonesia faces several challenges that contribute to the gap between legal provisions and practical privacy protection. These challenges include regulatory fragmentation, weak enforcement of data security standards, and inadequate rules for cross-border data transfers. The fragmented regulatory landscape, with various bodies such as the Ministry of Communications and Informatics (MOCI) and sectoral regulators, leads to inconsistencies in the enforcement of privacy rules, causing confusion and overlap across sectors such as finance and e-commerce [9], [22]. Weak enforcement of data security standards under the PDP Act is another important issue. Many organisations lack the necessary technical infrastructure and expertise to implement robust security measures, resulting in frequent data breaches. The absence of clear guidelines on data breach reporting and incident response further complicates regulatory efforts to address privacy breaches promptly [2], [11]. In addition, Indonesia's legal framework lacks comprehensive rules for cross-border data transfers, which is a critical issue in the global digital economy. The PDP Law does not provide clear criteria for transferring personal data to foreign entities, nor does it ensure equal protection for data processed outside Indonesia, increasing the risk of misuse [28].

3. *Data Privacy Breach Case Studies*

This study examined several data privacy breach case studies in Indonesia to illustrate the gaps in the legal framework and its implementation. The case studies of data privacy breaches in Indonesia highlight significant gaps in the legal framework and its implementation[29], especially regarding the enforcement of the Personal Data Protection Law (PDP). A 2020 data breach involving Tokopedia, a major e-commerce platform, exposed the personal data of 91 million users, yet the company faced only minimal repercussions due to weak enforcement mechanisms[9], [12], [30]. Similarly, unauthorized access to government databases, which leaked the personal information of 102 million Indonesian citizens, underscored vulnerabilities in government IT infrastructure and the need for stronger regulatory oversight [31]. These cases illustrate broader challenges in Indonesia's legal system regarding privacy and data protection[9].

4.2 Discussion

The gaps identified in Indonesia's PDP Law reflect the broader challenges faced by many countries in regulating data protection in the digital age. Comparisons with global best practices, such as the European Union's General Data Protection Regulation (GDPR), highlight important areas where Indonesia's legal framework can be strengthened. The GDPR provides a clear definition of personal data, imposes strict penalties for non-compliance, and gives data protection authorities the power to act decisively against breaches. In addition, the GDPR addresses the challenges of new technologies through principles such as data minimisation, purpose limitation, and accountability. In contrast, Indonesia's PDP Law lacks strong enforcement mechanisms and adaptability to technological developments, making it less effective in protecting privacy in the rapidly evolving digital landscape. A potential solution is to establish an

independent data protection authority with powers similar to the European Data Protection Supervisor, which can monitor compliance, sanction, and provide guidance on emerging privacy issues [27][26][23].

Another key issue highlighted by this research is the lack of public awareness regarding privacy rights in Indonesia. Without an informed public, even the most robust data protection laws will be ineffective. Indonesia could benefit from public awareness campaigns such as those implemented in countries with mature data protection frameworks, which can educate the public about their rights, encourage the exercise of those rights, and provide avenues to seek recourse in cases of privacy breaches. In addition, organisations should be required to provide more transparent information on how they collect, use and protect personal data, which will not only empower data subjects, but also increase trust between consumers and businesses in the digital economy [11], [28], [32].

As digital technologies evolve, the need for a dynamic legal framework becomes increasingly important, yet Indonesia's current data protection regulations do not fully address the implications of big data, AI, and IoT. These technologies often rely on the continuous collection and analysis of personal data, which raises privacy concerns. To address this, Indonesia could introduce specific legal provisions governing these technologies, such as requiring organizations to conduct privacy impact assessments before implementing data-intensive technologies. The introduction of stricter rules regarding data consent, collection and processing could also help bridge the gap between the legal framework and technological advancements. By adopting principles such as privacy by design, Indonesia can ensure that new technologies are developed with privacy protections integrated into their core functions [12], [30], [31].

4.3 Recommendations to Improve Data Protection and Privacy in Indonesia

Based on the findings of this study, several recommendations can be made to improve the protection of privacy rights and the implementation of data protection laws in Indonesia:

1. Indonesia should establish a dedicated data protection authority with the power to enforce data protection laws, investigate violations, and impose fines. This authority would provide clear guidance to businesses and ensure uniform enforcement across the sector.
2. The PDP Law should be updated to address emerging technologies such as AI and IoT. Specific regulations for data-intensive technologies should be introduced, to ensure that these technologies respect the privacy rights of individuals.
3. The government should launch a public awareness campaign to educate citizens about their privacy rights. This could include workshops, online resources, and outreach programmes aimed at increasing public engagement with data protection laws.
4. Clearer guidelines for data breach reporting, stronger penalties for non-compliance, and regular audits of organisations handling personal data are needed to ensure accountability and prevent breaches.

5. Indonesia can benefit from adopting best practices from international frameworks such as the GDPR. This includes imposing stricter consent requirements, ensuring data portability, and protecting against unauthorised cross-border data transfers.

5. CONCLUSION

This research examined the gap between Indonesia's data protection regulations and the practical implementation of privacy rights, focusing on the newly enacted Personal Data Protection (PDP) Law. While the PDP Law is an important advance, challenges such as unclear legal definitions, weak enforcement, and inadequate provisions for digital technologies such as artificial intelligence, big data, and the Internet of Things (IoT) hinder its implementation. Low public awareness of privacy rights also limits individuals' ability to assert their rights. The lack of a centralised data protection authority and fragmented oversight add to the complexity of enforcement. Compared to the EU General Data Protection Regulation (GDPR), Indonesia's legal framework still needs improvement in the aspects of cross-border data transfer, consent, and accountability. The establishment of a specialised data protection authority with clear enforcement powers, stronger legal provisions and public awareness campaigns is recommended. Adapting international best practices to the Indonesian context can improve privacy protection and promote sustainable growth of the digital economy.

REFERENCES

[1] F. Balaguer Callejón, "Data protection and the transformation of rights in the digital society: Francisco Balaguer Callejón," *UNIO–EU Law J.*, vol. 10, no. 1, pp. 4–16, 2024.

[2] V. Pyrohovska, K. Rezvorovych, I. Pavlichenko, Y. Sushytska, and V. Ostashova, "Human rights protection in the context of information technology development: Problems and future prospects," *Futur. Econ.*, vol. 4, no. 1, pp. 38–51, 2024.

[3] C. Nyst and T. Falchetta, "The right to privacy in the digital age," *J. Hum. Rights Pract.*, vol. 9, no. 1, pp. 104–118, 2017.

[4] D. Adams, "Managing the challenges of leveraging technology and data advances to improve social protection," 2024.

[5] R. S. Shahrullah, J. Park, and I. Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Rev.*, vol. 10, no. 1, pp. 1–20, 2024.

[6] N. Rianarizkiwati, "Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia," *J. Huk. Sasana*, vol. 8, no. 2, pp. 324–341, 2022.

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

[8] H. Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," *J. Yuridis*, vol. 7, no. 1, pp. 105–119, 2020.

[9] S. Syahwami and H. Hamirul, "The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia," *Enigm. Law*, vol. 2, no. 2, pp. 75–84, 2024.

[10] N. A. P. Adytia, S. Z. S. Wachdin, and S. Said, "The Legal Framework for Personal Data Protection in the Digital Era as Fulfillment of Privacy Rights in Indonesia," *KnE Soc. Sci.*, pp. 692–700, 2024.

[11] O. Reis, N. E. Eneh, B. Ehimuan, A. Anyanwu, T. Olorunsogo, and T. O. Abrahams, "Privacy law challenges in the digital age: a global review of legislation and enforcement," *Int. J. Appl. Res. Soc. Sci.*, vol. 6, no. 1, pp. 73–88, 2024.

[12] F. A. Salsabila and A. A. IImih, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektlf Hukum Siber," *ALADALAH J. Polit. Sos. Huk. dan Hum.*, vol. 2, no. 4, pp. 176–181, 2024.

[13] A. Pokhrel, "Harmonizing public health with individual liberties: exploring the interplay of right to health, privacy, and autonomy during recent and future pandemics," *Int. J. Hum. Rights Healthc.*, 2024.

[14] S. M. R., "Digital Data Privacy Laws: An Outlook," *Issue 2 Indian JL Leg. Rsch.*, vol. 5, p. 1, 2023.

[15] Y. Zhu, "Legal Challenges and Countermeasures for Data Privacy Protection," *Int. J. Educ. Sci. Theory*, vol. 3, no. 5, pp. 21–24, 2024.

[16] R. Natamiharja and I. Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law J.*, vol. 7, no. 1, pp. 233–251, 2024.

[17] O. O. Amoo, A. Atadoga, F. Osasona, T. O. Abrahams, B. S. Ayinla, and O. A. Farayola, "GDPR's impact on cybersecurity: A review focusing on USA and European practices," *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 1338–1347,

2024.

[18] S. S. Bakare, A. O. Adeniyi, C. U. Akpuokwe, and N. E. Eneh, "Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 528–543, 2024.

[19] B. Ehimuan, O. Chimezie, O. V. Akagha, O. Reis, and B. B. Oguejiofor, "Global data privacy laws: A critical review of technology's impact on user rights," *World J. Adv. Res. Rev.*, vol. 21, no. 2, pp. 1058–1070, 2024.

[20] M. C. Compagnucci, "The EU-US Data Privacy Framework: Is the Dragon Eating its Own Tail?," *arXiv Prepr. arXiv2407.17021*, 2024.

[21] V. M. Azza and H. Hartana, "Application of Personal data protection on electronic signatures in Indonesia," *J. Indones. Sos. Teknol.*, vol. 5, no. 5, pp. 2430–2439, 2024.

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

[23] S. W. Attidhira and Y. S. Permana, "Review of Personal Data Protection Legal Regulations in Indonesia," *Awang Long Law Rev.*, vol. 5, no. 1, pp. 280–294, 2022.

[24] E. A. P. Manurung, "The right to privacy based on the Law of the Republic of Indonesia number 27 of 2022," *J. Digit. Law Policy*, vol. 2, no. 3, pp. 103–110, 2023.

[25] G. D. Kuh, "Assessing what really matters to student learning inside the national survey of student engagement," *Chang. Mag. High. Learn.*, vol. 33, no. 3, pp. 10–17, 2001.

[26] S. D. Rosadi, A. Noviandika, R. Walters, and F. R. Aisy, "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?," *Int. Rev. Law, Comput. Technol.*, vol. 37, no. 1, pp. 78–90, 2023.

[27] E. Fauzy and N. A. R. Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Lex Renaiss.*, vol. 7, no. 3, pp. 445–461, 2022.

[28] S. Yuniarti, A. M. Ramli, S. D. Rosadi, and D. Budhijanto, "The New Chapter Of Indonesia's Data Protection On Digital Economy Perspective," *J. Southwest Jiaotong Univ.*, vol. 58, no. 3, 2023.

[29] A. Angelia, F. S. Oeijono, and D. Limbong, "Legal Protection of Paylater Users on E-Commerce Platforms for Personal Data Leakage," *Amnesti J. Huk.*, vol. 6, no. 2, pp. 174–185, 2024.

[30] I. T. Almeyda and E. Prasetyawati, "Consumer Protection for The Hacking of Personal Data of Tokopedia Marketplace Users," *J. Evid. Law*, vol. 3, no. 2, pp. 93–106, 2024.

[31] R. Sahatatua, Y. Gusmaria, I. K. Astawa, A. M. Suherman, T. Setiady, and W. D. Tinambunan, "Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum," *J. Multidiscip. Acad. Pract. Stud.*, vol. 2, no. 3, pp. 217–221, 2024.

[32] I. Bondarenko, T. Shulga, V. Kapustnyk, S. Hotsuliak, and P. Duravkin, "Directions for the implementation of regulatory means for the application of tax benefits in the general system of regulatory regulation of technology support means," *Eastern-European J. Enterp. Technol.*, vol. 1, no. 13, p. 121, 2023.