

Legal Perspective on Data Privacy Protection as a Human Right in Indonesia

Silvester Magnus Loogman Palit¹, Tumian Lian Daya Purba²

¹ Universitas Cenderawasih

² Universitas Cenderawasih

Article Info	ABSTRACT
Article history: Received Oct, 2025 Revised Oct, 2025 Accepted Oct, 2025 Keywords: Data Privacy; Human Rights; Indonesia; Legal Protection; Normative Juridical Analysis	This study examines the legal perspective on data privacy protection as a human right in Indonesia through a normative juridical approach. The increasing use of digital technology and the proliferation of personal data collection have intensified concerns over the misuse of personal information and inadequate legal safeguards. The research analyzes Indonesia’s constitutional provisions, statutory frameworks—including Law No. 27 of 2022 on Personal Data Protection (PDP Law)—and their alignment with international human rights instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Findings indicate that Indonesia has made substantial progress in establishing a legal foundation for data privacy through the PDP Law, which emphasizes principles of consent, transparency, and accountability. However, implementation challenges remain, particularly in institutional enforcement, public awareness, and regulatory coordination. The study concludes that effective protection of data privacy requires not only strong legal frameworks but also a rights-based approach that upholds human dignity, ensures government accountability, and promotes digital justice in the information age. <i>This is an open access article under the CC BY-SA license.</i> 

Corresponding Author:

Name: Silvester Magnus Loogman Palit
Institution: Universitas Cenderawasih
Email: silvesterpalit@gmail.com

1. INTRODUCTION

The rapid growth of information and communication technology (ICT) has transformed how individuals interact, communicate, and manage data, but it also raises serious legal and ethical issues concerning personal data protection. In Indonesia, data breaches and misuse of personal information have become prevalent, making privacy protection a fundamental human rights concern. The enactment of Law Number 27 of 2022 on Personal Data

Protection (PDP Law) represents a key step toward addressing these issues; however, enforcement challenges persist due to limited infrastructure readiness and business compliance [1], [2]. Existing laws such as the ITE Law and PP PSTE remain fragmented and insufficient to ensure comprehensive data protection [3], [4]. Weak law enforcement and low public awareness further hinder implementation, while many digital businesses fail to uphold data privacy obligations [2]. From a human rights perspective, data privacy aligns with

constitutional rights, necessitating stronger legal safeguards and alignment with global standards such as the GDPR [4].

The right to privacy is a cornerstone of human dignity and autonomy, enabling individuals to control their personal information and protect themselves from intrusive surveillance or exploitation. In Indonesia, privacy rights derive from Article 28G paragraph (1) of the 1945 Constitution, which safeguards personal integrity, honor, and dignity, and are reinforced by the country's ratification of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Despite these normative guarantees and the enactment of the Personal Data Protection (PDP) Law in 2022, privacy protection remains inadequate due to overlapping regulations, weak enforcement mechanisms, and limited institutional capacity [4]–[6]. The fragmented legal framework, including the Electronic Information and Transaction Law (ITE Law), lacks comprehensive safeguards for privacy rights [4], and the absence of a centralized data protection authority further complicates enforcement [5]. Moreover, weak institutional capacity and unclear legal definitions hinder the regulation of emerging technologies like AI and big data [5], creating a “normative vacuum” that limits effective legal recourse [6]. Low public awareness of privacy rights also undermines implementation, emphasizing the need for education and engagement to foster a stronger culture of data protection [5].

To address the growing challenges of data privacy, Indonesia enacted the Personal Data Protection Law (Law No. 27 of 2022), marking a major milestone in aligning its legal framework with international standards such as the European Union's General Data Protection Regulation (GDPR). This law seeks to establish a coherent system for data governance, define the rights of data subjects, and impose obligations on data controllers and processors. However, its effectiveness largely depends on consistent enforcement, strong cross-sectoral coordination, and heightened public awareness of digital rights.

Despite its significance, the PDP Law still lacks comprehensive regulatory mechanisms and an independent supervisory authority—elements essential for effective enforcement—thereby limiting accountability and overall impact [7], [8]. Weak sanctions and oversight further impede its success, as shown by recurring data breaches in major Indonesian companies [8]. Moreover, effective data protection requires coordination among multiple sectors, yet Indonesia's institutional capacity for cross-sectoral collaboration remains underdeveloped, demanding clearer regulations and stronger implementation frameworks [1], [7]. Low public awareness of digital rights also weakens the law's impact, making it vital to enhance citizen education and promote accountability among data controllers [8].

This paper analyzes data privacy protection as a human right in Indonesia through a normative legal approach, focusing on constitutional provisions, statutory regulations, and international human rights obligations to examine the legal foundation, challenges, and future direction of privacy protection. By employing a normative juridical method, it contributes to the discourse on digital human rights and emphasizes the urgency of legal reforms to ensure that privacy protection keeps pace with technological advancements. Fundamentally, safeguarding data privacy is not merely a technical concern but a human rights imperative—essential for maintaining public trust, promoting accountability in digital governance, and ensuring that Indonesia's legal system remains adaptive to the dynamics of the digital era.

2. LITERATURE REVIEW

2.1 *Concept of Data Privacy and Human Rights*

The concept of data privacy is deeply rooted in the broader notion of privacy, which has evolved from physical seclusion to encompass informational privacy in the digital age. This shift underscores the increasing need to protect personal data from unauthorized access and misuse, as reflected in Westin's

definition of privacy as the right to control one's personal information [9]. Historically, privacy discussions began with protecting one's body and home and later evolved toward control over personal information [9]. In the digital era, informational privacy involves both limiting others' access to data and ensuring individual control over personal information [10]. Recognized as a fundamental human right, data privacy safeguards personal information—such as financial and health records—from exploitation and underscores the necessity of robust legal frameworks that balance technological innovation with individual security [11]. Protecting personally identifiable information is essential to prevent violations like unauthorized surveillance or data breaches, while ensuring the preservation of solitude, secrecy, and anonymity as core components of privacy [12].

2.2 Legal Framework of Data Privacy Protection in Indonesia

Indonesia's recognition of privacy as a legal right is deeply rooted in its constitutional framework, specifically Article 28G of the 1945 Constitution, which guarantees personal protection, honor, dignity, and safety, further reinforced by Law No. 39 of 1999 on Human Rights. However, prior to the enactment of the Personal Data Protection Law (Law No. 27 of 2022), Indonesia's data protection regime was fragmented across multiple sectoral regulations, leading to inconsistencies and enforcement challenges. The PDP Law marks a significant step forward by providing a comprehensive framework that defines personal data, establishes data subject rights, and sets obligations for data controllers and processors, incorporating principles such as lawful processing, transparency, purpose limitation, and accountability [13]. It also introduces an independent supervisory authority to oversee compliance and dispute resolution, although its establishment remains pending [8], [13].

Despite these advancements, implementation faces serious challenges, including the absence of a dedicated enforcement institution [13], limited technical expertise, and low public awareness regarding data privacy rights [5], [8]. Furthermore, weak sanctions and oversight mechanisms undermine the law's effectiveness, as reflected in recurring data breach incidents [8]. From a comparative perspective, aligning Indonesia's framework with international standards like the GDPR requires stronger enforcement and greater public engagement to ensure effective protection of personal data [4], [5].

2.3 Data Privacy as a Human Right in the Digital Era

The conceptualization of data privacy as a human right in Indonesia is evolving in line with global trends that view personal data as integral to individual autonomy and dignity. Integrating human rights principles into data protection laws is crucial to ensure technological progress does not erode fundamental freedoms. In Indonesia, this integration is ongoing but not yet fully realized, as legal frameworks continue to develop in alignment with human rights standards while facing persistent implementation gaps [14]. The 1945 Constitution guarantees fundamental rights, including privacy, yet existing regulations such as the ITE Law remain fragmented and lack comprehensive provisions [4]. Key internal challenges include low awareness among data subjects and controllers, complex data processing systems, weak data security, and the absence of an independent authority to enforce data protection [14]. Externally, data interception and eavesdropping—especially within government and financial sectors—further undermine protection efforts [14]. Comparatively, Indonesia's progress is often measured against international standards like the GDPR, which balances privacy and innovation; however, Indonesia faces unique institutional and

supervisory challenges in implementing its Personal Data Protection Act [15]. The enactment of the Personal Data Protection Bill (RUU PDP) is thus emphasized as a vital step toward reinforcing the country's legal foundation for safeguarding data privacy [4].

2.4 Previous Studies and Research Gap

Previous studies on data privacy in Indonesia have largely centered on technical and regulatory aspects, including compliance requirements and enforcement challenges. The absence of an independent supervisory authority has limited the enforcement and accountability of the Personal Data Protection (PDP) Law, contrasting with the GDPR's stronger supervisory model [16], [17]. Indonesia's legal framework also lacks comprehensive mechanisms such as data portability rights and privacy by design principles, which are well-established in the GDPR [7]. Public literacy regarding digital privacy remains low, hindering the effective implementation of data protection laws [16], while weak sanctions and oversight continue to allow recurring data breaches in major companies [8]. To strengthen this framework, the establishment of an independent data protection authority is recommended to enhance enforcement and accountability [7], alongside efforts to increase public education on privacy rights and harmonize domestic regulations with international standards [7], [8]. For instance, earlier analyses have highlighted the fragmented nature and weak enforcement of Indonesia's pre-2022 data protection regime, while others noted that although the new PDP Law structurally aligns with the GDPR, institutional capacity remains a key obstacle. However, limited research has examined the philosophical and human rights dimensions of data privacy in Indonesia. This study addresses that gap by framing data privacy not merely as a regulatory issue but as a core element of human rights protection. Using a normative legal approach, it seeks to

deepen understanding of how Indonesia's legal system conceptualizes and implements data privacy as a human right amid global digital transformation. In summary, existing literature underscores that data privacy is both a legal and moral imperative, requiring comprehensive legal structures, capable institutions, and an informed public to uphold individuals' fundamental rights in an increasingly data-driven society.

3. RESEARCH METHODS

This study employs a normative juridical (legal-normative) approach that focuses on analyzing laws, regulations, legal principles, and doctrines related to data privacy protection as a human right in Indonesia. This method is suitable because the research does not involve empirical fieldwork but emphasizes the coherence and application of legal norms within national and international legal systems. The objective is to understand how Indonesia's existing legal framework protects data privacy and how these protections align with human rights principles, emphasizing the normative relationship between law, technology, and human dignity.

The nature of this research is descriptive-analytical, aiming to describe, explain, and analyze the legal norms governing data privacy protection in Indonesia. It identifies the substance of relevant laws while critically evaluating their consistency with constitutional and international human rights standards. The analysis includes statutory provisions, legal doctrines, and comparative perspectives to assess Indonesia's legal position within the global context of privacy protection. The study relies on secondary legal materials, including primary sources such as the 1945 Constitution (Articles 28G and 28I), Law No. 39 of 1999 on Human Rights, Law No. 27 of 2022 on Personal Data Protection, and relevant international instruments like the UDHR and ICCPR; secondary sources such as academic works by Westin (1967), Solove (2008), Bygrave (2010), and Nasution (2021); and tertiary sources such as legal dictionaries,

government reports, and ASEAN digital governance documents.

Legal materials were gathered through document and literature review, examining statutory provisions, government archives, academic journals, and databases. The analysis employed qualitative and normative legal interpretation across three approaches: the statutory approach (*pendekatan perundang-undangan*), which examines legislative hierarchy and coherence with constitutional norms; the conceptual approach (*pendekatan konseptual*), which explores key legal notions such as privacy, personal data, and human rights to construct a theoretical framework connecting data protection with human dignity; and the comparative approach (*pendekatan komparatif*), comparing Indonesia's laws with international frameworks such as the GDPR and ASEAN data protection regimes. Through these approaches, the research identifies gaps, overlaps, and inconsistencies in Indonesia's data privacy legislation and underscores the philosophical foundation of human rights law to ensure that privacy protection is both legally enforceable and ethically justified.

4. RESULTS AND DISCUSSION

4.1 *Recognition of Data Privacy as a Human Right in Indonesia*

The concept of data privacy as a human right in Indonesia finds its normative foundation in the 1945 Constitution of the Republic of Indonesia (UUD 1945). Article 28G paragraph (1) guarantees the protection of every person's personal integrity, honor, and dignity, while Article 28I paragraph (4) ensures that the protection and promotion of human rights are the responsibility of the state. These constitutional provisions affirm that privacy is part of the broader framework of human rights protection. Furthermore, Law No. 39 of 1999 on Human Rights reinforces this recognition, particularly through Article 29, which provides for the protection of personal life, family, and communication.

From a normative standpoint, the right to privacy is closely linked to human dignity (*martabat manusia*). As such, data privacy extends the traditional concept of privacy into the digital sphere, ensuring that individuals have control over their personal information in an increasingly connected society. Indonesia's commitment to international human rights instruments—specifically the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR)—further solidifies privacy as a fundamental right that must be upheld by both the government and private entities. Despite this recognition, practical enforcement remains a challenge. Prior to 2022, Indonesia lacked a comprehensive legal framework specifically addressing personal data protection. Privacy rights were dispersed across sectoral regulations, resulting in legal uncertainty. Therefore, the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a major step forward, providing clarity and coherence in protecting citizens' data privacy.

4.2 *The Personal Data Protection Law: Structure and Principles*

The Personal Data Protection Law (PDP Law) serves as Indonesia's first unified regulation governing the collection, storage, processing, and dissemination of personal data, drawing heavily from international best practices such as the European Union's General Data Protection Regulation (GDPR). It establishes fundamental principles including lawful and fair processing based on consent, purpose limitation, data minimization, accuracy, accountability, and transparency. The law also grants rights to data subjects—such as access, correction, deletion, and restriction of data processing—while imposing obligations on data controllers to report breaches, conduct impact assessments, and appoint data protection officers (DPOs). These provisions demonstrate Indonesia's effort to

harmonize its privacy protection framework with global standards and uphold data privacy as a component of human rights.

However, despite its alignment with the GDPR, the PDP Law faces notable implementation challenges. It lacks comprehensive mechanisms for data portability, privacy by design, and cross-border data flow regulation [7], and the absence of an independent supervisory authority weakens enforcement and accountability [7], [17]. Institutional and technical readiness remain limited [17], [18], as seen in recurring data breaches such as those involving Facebook and E-KTP [19]. To enhance its effectiveness, scholars recommend establishing an independent data protection authority, strengthening institutional capacity, incorporating modern data protection principles, and fostering public awareness through a co-regulatory approach involving both government and private sectors [7], [17], [20].

4.3 Institutional and Enforcement Challenges

Although the PDP Law has created a comprehensive structure for data privacy protection, several institutional and enforcement challenges persist:

- a. **Fragmented Legal Enforcement** – Various institutions, including the Ministry of Communication and Informatics (Kominfo), the National Cyber and Encryption Agency (BSSN), and the Indonesian National Police, share overlapping responsibilities in data protection. This fragmentation often leads to confusion over jurisdiction and weak enforcement.
- b. **Limited Public Awareness** – Many citizens remain unaware of their rights under the PDP Law. This lack of understanding reduces public participation in monitoring and reporting data violations.

- c. **Weak Sanctions and Oversight Mechanisms** – Although the PDP Law stipulates administrative and criminal sanctions, the procedures for imposing penalties and resolving disputes are not yet fully operational. The absence of an independent supervisory body has delayed consistent enforcement.
- d. **Technological and Resource Constraints** – Many organizations, particularly small and medium enterprises (SMEs), lack the technological capacity to implement robust data protection measures. Additionally, there is a shortage of skilled professionals trained in cybersecurity and legal compliance.

These challenges indicate that while Indonesia has made significant legislative progress, institutional readiness and enforcement capacity must be strengthened to ensure that privacy rights are effectively protected.

4.4 Comparative Insights: Indonesia and Global Standards

Comparative analysis reveals that Indonesia's PDP Law shares many similarities with the GDPR, particularly in defining data subject rights, consent requirements, and data controller obligations. However, the enforcement mechanisms differ significantly. The GDPR operates under the supervision of independent data protection authorities across EU member states, ensuring a strong institutional framework. Indonesia, in contrast, still lacks a fully operational supervisory body, limiting its ability to impose sanctions and monitor compliance effectively.

ASEAN countries such as Singapore and Malaysia offer useful lessons for Indonesia. Singapore's Personal Data Protection Act (PDPA) of 2012 has established the Personal Data Protection Commission (PDPC), which functions as an independent regulatory authority. Malaysia's PDPA 2010 also provides clear administrative enforcement procedures. These examples

demonstrate that independent oversight is essential for ensuring public trust and compliance with privacy laws.

By adopting similar mechanisms, Indonesia can enhance its data governance system and strengthen the protection of citizens' privacy as a human right. Furthermore, harmonizing national standards with ASEAN's digital data protection frameworks could facilitate cross-border data exchange while maintaining high levels of privacy protection.

4.5 Data Privacy and Human Dignity in the Digital Age

The recognition of data privacy as a human right reflects a broader philosophical understanding of human dignity in the digital era. In modern society, personal data has become an extension of individual identity, and its misuse or unauthorized exploitation constitutes a direct violation of human dignity. Legal scholars argue that privacy enables individuals to maintain autonomy and freedom from arbitrary interference, making data privacy an essential component of human rights protection. In Indonesia, safeguarding data privacy is not merely a matter of legal compliance but also of preserving public trust and ethical governance. As highlighted by various scholars, integrating human rights principles into data protection laws ensures that individuals' rights to freedom, dignity, and security remain protected amid rapid technological advancement.

The integration of personal data protection with human rights concepts in Indonesia has been significant, though challenges persist. These challenges include a lack of awareness among data subjects and controllers, complex data processing systems, and weak data security measures [14]. Indonesia's current legal framework remains sectoral and lacks harmonization, reducing the effectiveness of data protection efforts [20]. Internal obstacles include the absence of a comprehensive legal

structure and a dedicated independent data protection authority, while external challenges involve unauthorized data interception, particularly in government and financial sectors [14]. Scholars recommend adopting a co-regulatory approach that involves both government and businesses to enhance data protection and to develop a comprehensive legal framework that reflects international best practices [20].

Effective data protection is thus crucial for upholding human rights in the digital age, particularly regarding privacy, transparency, and accountability [21]. Despite notable progress, Indonesia's legal framework still requires further development to align with global standards such as the GDPR to ensure robust human rights protection in the digital landscape [22]. Strengthening data privacy not only safeguards individual autonomy but also promotes accountability in both public administration and private enterprise. Transparent data governance enhances citizens' confidence in digital systems, thereby supporting broader participation in e-government initiatives and the digital economy. Consequently, effective data privacy protection contributes not only to the realization of fundamental human rights but also to the advancement of democratic governance and sustainable development.

4.6 Discussion and Policy Implications

The findings reveal that although Indonesia has made notable progress in codifying data privacy protection, several crucial areas still require enhancement to fully align with human rights standards. Institutional strengthening through the establishment of an independent data protection authority is essential for impartial oversight and effective enforcement, while collaborative efforts between government and civil society are needed to improve digital literacy and public awareness of privacy rights. Clear cross-sectoral coordination is required to prevent regulatory overlap, and

harmonization with global and ASEAN data protection standards will foster international cooperation and trade. Furthermore, embedding ethical governance principles ensures that data protection remains rooted in human dignity and justice. In conclusion, data privacy in Indonesia has evolved into a core pillar of human rights protection in the digital era, and its legal recognition through the Personal Data Protection Law must be supported by strong institutions, active public participation, and ethical governance to guarantee that every citizen's right to privacy is upheld and effectively enforced.

5. CONCLUSION

The recognition and protection of data privacy as a human right in Indonesia mark a crucial milestone in the nation's legal evolution. The 1945 Constitution and Law No. 39 of 1999 on Human Rights provide the normative basis for the right to privacy, which has been further institutionalized through the Personal Data Protection Law (Law No. 27 of 2022). This law establishes comprehensive principles such as lawful data processing, consent, transparency, and accountability, positioning Indonesia's regulatory framework closer to international standards

like the General Data Protection Regulation (GDPR). Nonetheless, despite this legal progress, several challenges remain, including weak institutional enforcement, fragmented regulations, and low public awareness. The absence of an independent supervisory authority and overlapping institutional mandates continue to hinder effective implementation, while limited understanding among citizens and organizations regarding their rights and obligations further constrains compliance.

To reinforce data privacy protection as a fundamental human right, Indonesia must prioritize key measures such as establishing an independent data protection authority with sufficient authority and resources, enhancing digital literacy and public education, promoting cross-sectoral coordination among government institutions, and aligning domestic frameworks with global and ASEAN data protection standards. Ultimately, safeguarding data privacy is not merely a technical or administrative issue but a manifestation of the state's dedication to human dignity, freedom, and justice. Upholding privacy as a human right ensures that Indonesia's digital transformation advances in a way that respects individual autonomy, strengthens public trust in digital governance, and upholds the rule of law in an increasingly interconnected society.

REFERENCES

- [1] I. Lutrianto and R. Riswaldi, "Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia," *Greenation Int. J. Law Soc. Sci.*, vol. 3, no. 2, pp. 345–350, 2025.
- [2] D. D. Wijayanto and K. W. Indrayanti, "Personal Data Protection in Digital Business Based on the Law on Personal Data Protection," *Int. J. Res. Soc. Sci. Humanit.*, vol. 6, no. 8, pp. 6–12, 2025.
- [3] R. S. Ahmad, D. A. Puspaningtyas, and M. N. K. Al Ismariy, "Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital," *The Juris*, vol. 9, no. 1, pp. 15–23, 2025.
- [4] J. E. Widodo, A. Suganda, and T. A. Darodjat, "Data Privacy And Constitutional Rights In Indonesia: Data Privacy And Constitutional Rights In Indonesia," *PENA LAW Int. J. Law*, vol. 2, no. 2, 2024.
- [5] L. Judijanto, N. Solapari, and I. Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *East J. Law Hum. Rights*, vol. 3, no. 01, pp. 20–29, 2024.
- [6] M. A. Nirwana, "Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual," *AL WASATH J. Ilmu Huk.*, vol. 3, no. 2, pp. 93–104, 2022.
- [7] G. Karnedi and R. G. Alam, "Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa," *El-Mujtama J. Pengabd. Masy.*, vol. 5, no. 3, pp. 610–622, 2025, doi: <https://doi.org/10.47467/elmujtama.v5i3.8549>.
- [8] A. S. Kriswandaru, B. Pratiwi, and S. Suwardi, "Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus," *Hakim J. Ilmu Huk. Dan Sos.*, vol. 2, no. 4, pp. 740–756, 2024.
- [9] J. Holvast, "History of privacy," in *In The history of information security*, Elsevier Science BV, 2007, pp. 737–769.
- [10] J. E. Mai, *Situating personal information: Privacy in the algorithmic age*. 2019.
- [11] B. Singh, "Cherish data privacy and human rights in the Digital Age: Harmonizing innovation and individual

- autonomy," in *In Balancing human rights, social responsibility, and digital ethics*, IGI Global, 2024, pp. 199–226.
- [12] A. Beresford and D. Scott, "Data Privacy," *Wiley Encycl. Comput. Sci. Eng.*, 2007.
- [13] K. Kurdi and J. Cahyono, "Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *JUNCTO J. Ilm. Huk.*, vol. 6, no. 2, pp. 330–339, 2024.
- [14] N. Angraini K, Z. . Makkawaru, and A. Almusawir, "Perlindungan Hukum Data Pribadi Dalam Perspektif Hak Asasi Manusia," *Indones. J. Leg. Law*, vol. 7, no. 1, pp. 46–51, 2024, doi: <https://doi.org/10.35965/ijlf.v7i1.5267>.
- [15] D. N. F. Ahmad, P. A. Zubaedah, R. Hafizi, F. C. Umam, and L. Judijanto, "The Evolution of Data Privacy Laws: Balancing Technological Innovation and Human Rights in the Age of Big Data," *Pakistan J. Life Soc. Sci.*, vol. 22, no. 2, 2024.
- [16] A. Duha, "Law for Ensuring Data Security in the Digital Age: Challenges for Government and Warnings for Us," *Verdict J. Law Sci.*, vol. 3, no. 2, pp. 111–119, 2024.
- [17] M. Taufiq and A. S. Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR," *Int. J. Business, Law, Educ.*, vol. 6, no. 2, pp. 1260–1268, 2025.
- [18] F. Razi and D. P. Markus, "Implementation and Challenges of the Personal Data Protection Law in Indonesia," *J. Indones. Sos. Teknol.*, vol. 5, no. 12, 2024.
- [19] M. Yusup and N. Ruhaeni, "Peraturan Perlindungan Data Pribadi Berdasarkan Instrumen Hukum Internasional Dan Implementasinya Di Indonesia," *Pros. Ilmu Huk.*, vol. 5, no. 1, pp. 109–116, 2019.
- [20] S. Dewi, "Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia," *J. Jure*, vol. 15, no. 2, p. 165, 2015.
- [21] V. P. Shehu and V. Shehu, "Human rights in the technology era–Protection of data rights," *Eur. J. Econ.*, vol. 7, no. 2, 2023.
- [22] L. Judijanto, A. F. Lubis, D. E. S. Karauwan, S. S. Bungin, and H. A. Mau, "Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia," *Sanskara Huk. dan HAM*, vol. 3, no. 01, pp. 34–42, 2024.