Legal Governance in Facing the Challenges of a Sustainable Digital Economy in Indonesia: A Case Study of Personal Data Protection Based on Law Number 27 of 2022 concerning Personal Data Protection

Novi Eklesiya Tresnavionita[1], Ully Tangziyah Fatmala[2]
[1] *Graduate School, Law Study Program, Universitas Swadaya Gunung Jati, Indonesia.*
[2] *Graduate School, Law Study Program, Universitas Swadaya Gunung Jati, Indonesia.*

Corresponding Author: Novi Eklesiya Tresnavionita, **E-mail**: novieklesiya@gmail.com

| ABSTRACT

The development of the digital economy in Indonesia faces major challenges in maintaining sustainability through effective legal governance, particularly personal data protection as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This study aims to analyze legal governance in addressing the challenges of a sustainable digital economy in Indonesia, with a focus on personal data protection under Law Number 27 of 2022 concerning Personal Data Protection. This study analyzes the legal framework through a normative juridical approach using case studies of digital practices vulnerable to data leaks, such as e-commerce platforms, to identify regulatory gaps and their implementation in support of a sustainable digital economy. The analysis shows that the PDP Law provides a strong foundation for strengthening business accountability and public digital literacy, but challenges such as limited institutional capacity and consumer awareness continue to hamper its effectiveness. The case study reveals weaknesses in the data security system that require the adoption of international practices such as the GDPR to create a safe and trusted digital ecosystem. The study recommends strengthening regulations, increasing institutional oversight, and integrating educational programs as strategic steps to improve the effectiveness of personal data protection in supporting the development of an inclusive and sustainable digital economy in Indonesia.

| KEYWORDS

Digital economy, personal data protection, Law Number 27 of 2022, e-commerce, GDPR.

I. INTRODUCTION

The development of the digital economy in Indonesia faces major challenges in ensuring sustainability through effective legal governance, particularly with regard to personal data protection as regulated under Law Number 27 of 2022 on Personal Data Protection (PDP Law). [1] Indonesia's digital economy has been growing rapidly and has become one of the largest in the ASEAN region, while simultaneously serving as a key driver in accelerating national economic growth. In 2024, the value of Indonesia's digital economy reached USD 90 billion and is projected to surge to USD 360 billion by 2030. [2] This growth has been driven by e-commerce platforms such as Shopee and Tokopedia, which involve the management of personal data belonging to millions of users. However, the sustainability of the digital economy is threatened by data breaches, as exemplified by the 2020 Tokopedia incident that affected 91 million user accounts. [3]

Law Number 27 of 2022 on Personal Data Protection (PDP Law) represents a legal milestone in addressing these challenges by comprehensively regulating the collection, processing, and protection of personal data. [1] Nevertheless, its implementation continues to face obstacles, including a lack of harmonization with other regulations, such as the Electronic Information and Transactions Law (ITE Law), as well as limitations in supervisory infrastructure.

Previous research conducted by Burhanuddin in 2025 highlights fragmented regulatory frameworks and a lack of consumer awareness, while the theory of legal certainty remains highly relevant in this context. [4] This study aims to analyze the regulatory gaps within Law Number 27 of 2022 on Personal Data Protection. The research questions address: (1) how the PDP Law framework responds to data protection challenges in e-commerce; (2) existing

regulatory and implementation gaps; and (3) strategic recommendations. The findings are expected to contribute to policymakers and business actors in fostering an inclusive and sustainable digital ecosystem.

II. METHODOLOGY

The study employs a normative juridical research design with a statutory, conceptual, and case study approach. The sample includes the Personal Data Protection Law (UU PDP) as the primary legal source, a comparative analysis of the GDPR, and e-commerce data breach cases, such as those involving Tokopedia and other platforms during the 2020–2025 period. The operational variables encompass the accountability of data controllers (Articles 16–26 of the UU PDP), implementation effectiveness, and regulatory gaps, which are analyzed through qualitative legal interpretation, normative comparison, and case description to assess their contribution to the digital economy.

III. RESULTS AND DISCUSSION

Legal Framework of the Personal Data Protection Law in the Digital Economy

"The Personal Data Protection Law (Undang-Undang Perlindungan Data Pribadi/UU PDP) defines personal data as information relating to an identified or identifiable individual (Article 4). Article 4 provides that:

(1) Personal Data Processing includes:

a. acquisition and collection;

b. processing and analysis;

c. storage;

d. correction and updating;

e. display, announcement, transfer, dissemination, or disclosure; and/or

f. deletion or destruction.

(2) Personal Data Processing as referred to in paragraph (1) shall be conducted in accordance with Personal Data Protection principles, which include:

a. Personal Data shall be processed in a limited and specific manner, lawfully, and transparently;

b. Personal Data processing shall be carried out in accordance with its stated purposes;

c. Personal Data processing shall ensure the rights of the Personal Data Subject;

d. Personal Data processing shall be accurate, complete, not misleading, up to date, and accountable;

e. Personal Data processing shall protect the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, and loss of Personal Data;

f. Personal Data processing shall be conducted by notifying the purposes and activities of processing, as well as any failure of Personal Data Protection;

g. Personal Data shall be destroyed and/or deleted after the retention period expires or upon the request of the Personal Data Subject, unless otherwise stipulated by laws and regulations; and

h. Personal Data processing shall be carried out responsibly and demonstrably.

(3) Further provisions regarding the implementation of Personal Data Processing as referred to in paragraph (1) shall be regulated by Government Regulation.

The obligations of data controllers include obtaining explicit consent (Article 18), which provides that:

(1) Personal Data Processing may be conducted by two (2) or more Personal Data Controllers.

(2) In the event that Personal Data Processing is carried out by two (2) or more Personal Data Controllers, the following minimum requirements must be fulfilled:

a. the existence of an agreement among the Personal Data Controllers specifying their respective roles, responsibilities, and inter-controller relationships;

b. the existence of interrelated purposes and jointly determined methods of Personal Data Processing; and

c. the designation of a jointly appointed contact person.

With regard to data security, Article 36 stipulates that, in conducting Personal Data Processing, Personal Data Controllers are obliged to maintain the confidentiality of Personal Data.

Furthermore, the UU PDP provides for administrative and criminal sanctions (Articles 67–72). Article 67 states that:

(1) Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to them for the purpose of benefiting themselves or another person, resulting in harm to the Personal Data Subject as referred to in Article 65 paragraph (1), shall be punished with imprisonment for a maximum of five (5) years and/or a fine of up to IDR 5,000,000,000 (five billion rupiah).

(2) Any person who intentionally and unlawfully discloses Personal Data that does not belong to them as referred to in Article 65 paragraph (2) shall be punished with imprisonment for a maximum of four (4) years and/or a fine of up to IDR 4,000,000,000 (four billion rupiah).

(3) Any person who intentionally and unlawfully uses Personal Data that does not belong to them as referred to in Article 65 paragraph (3) shall be punished with imprisonment for a maximum of five (5) years and/or a fine of up to IDR 5,000,000,000 (five billion rupiah).

Article 68 provides that any person who intentionally creates false Personal Data or falsifies Personal Data for the purpose of benefiting themselves or another person, resulting in harm to others as referred to in Article 66, shall be punished with imprisonment for a maximum of six (6) years and/or a fine of up to IDR 6,000,000,000 (six billion rupiah).

Article 69 stipulates that, in addition to the principal penalties as referred to in Articles 67 and 68, additional penalties may be imposed in the form of confiscation of profits and/or assets obtained from criminal acts and the payment of compensation.

Article 70 regulates corporate liability, providing that:

(1) Where the criminal acts referred to in Articles 67 and 68 are committed by a corporation, criminal liability may be imposed on management, controlling shareholders, order-givers, beneficial owners, and/or the corporation.

(2) The criminal penalty that may be imposed on a corporation shall be limited to a fine.

(3) The fine imposed on a corporation may be up to ten (10) times the maximum fine prescribed.

(4) In addition to fines, corporations may be subject to additional penalties, including: confiscation of profits and/or assets obtained from criminal acts; suspension of all or part of corporate activities; permanent prohibition from engaging in certain activities; closure of all or part of business premises; fulfillment of neglected obligations; payment of compensation; revocation of licenses; and/or dissolution of the corporation.

Articles 71 and 72 further regulate the execution of fines and substitute penalties, including the seizure and auction of assets and, in the case of corporate offenders, the suspension of part or all business activities for a maximum period of five (5) years."

These provisions strengthen the accountability of digital business actors, as the digital economy relies heavily on data for service personalization. However, their effectiveness is constrained by limited institutional capacity. Public digital literacy also remains low; the 2024 APJII survey indicates that only 40% of users understand personal data risks. [5]

Case Study: Data Breach on an E-Commerce Platform

The Tokopedia data breach in 2020 exposed approximately 91 million user records, including email addresses and hashed passwords, as a result of a server vulnerability [6]. A juridical analysis indicates violations of Article 36 of the Personal Data Protection Law (UU PDP) concerning data security, which stipulates that, in processing Personal Data, the Personal Data Controller is obligated to ensure the confidentiality of such data. Furthermore, the case reflects inadequate notification to affected data subjects, in contravention of Article 25, which provides that: (1) the processing of children's Personal Data is subject to special protection; and (2) the processing of children's Personal Data as referred to in paragraph (1) must obtain consent from the child's parents and/or legal guardians in accordance with the applicable laws and regulations.

Gap Analysis in Indonesia's Data Protection Framework

This case study identifies three major gaps in the implementation of Indonesia's Personal Data Protection Law (Law No. 27 of 2022, hereinafter the PDP Law) that may undermine e-commerce security: (1) the absence of mandatory encryption standards, such as AES-256 [7], which are required under the General Data Protection Regulation (GDPR) [8]; (2) weak law enforcement resulting from overlapping institutional authority between the

National Cyber and Crypto Agency (BSSN) and the Personal Data Protection Supervisory Authority (DPDP); and (3) the lack of regular independent audit mechanisms.

First, the absence of mandatory encryption standards creates significant vulnerabilities to cyberattacks. Unlike the GDPR, which requires high-level encryption (e.g., AES-256 for sensitive data based on the 2023 ENISA Recommendations) [9], the PDP Law merely refers to encryption in general terms under Article 48, without providing technical specifications. Case studies of e-commerce platforms indicate that 65% of data breach incidents (based on the 2024 BSSN report) [10] were caused by weak encryption practices, such as the use of AES-128 or even outdated protocols, enabling brute-force exploitation within a matter of hours.

Second, weak enforcement is exacerbated by overlapping institutional mandates. BSSN focuses on national cybersecurity (Presidential Regulation No. 49 of 2017), while the DPDP is responsible for supervising personal data protection under Article 19 of the PDP Law, which stipulates that Personal Data Controllers and Personal Data Processors include: (a) individuals; (b) public bodies; and (c) international organizations. In practice, coordination between these institutions is frequently ineffective, as evidenced by a 2024 data breach case in which the response was delayed by 72 hours, exceeding the GDPR's 72-hour notification threshold under Article 33. The GDPR further stipulates that Personal Data Controllers are obliged to refuse access to or modification of Personal Data where such actions: (a) endanger the security, physical health, or mental health of the Data Subject and/or others; (b) result in the disclosure of another person's Personal Data; and/or (c) conflict with national defense and security interests. Data from the Ministry of Communication and Information Technology indicate that only 15% of violations were effectively enforced in 2024, compared to 85% in the European Union.

Third, the lack of regular independent audits creates a significant oversight gap. The PDP Law does not mandate annual third-party audits, unlike the GDPR, which requires periodic Data Protection Impact Assessments (DPIAs) [11]. In the examined case studies, e-commerce platforms failed to identify security vulnerabilities for up to 18 months due to biased internal audit processes.

Challenges and Recommendations

The primary challenges include low consumer awareness and weak institutional capacity. Accordingly, the following strategic recommendations are proposed:

1. Regulatory strengthening through the issuance of implementing Presidential Regulations to establish clear technical standards.
2. Enhanced supervision via collaboration between the Personal Data Protection Authority (DPDP) and the National Cyber and Crypto Agency (BSSN), supported by mandatory annual audits.
3. Integrated education programs coordinated by the Ministry of Education, Culture, Research, and Technology and the Ministry of Communication and Informatics, targeting 70% digital literacy by 2030.
4. Adoption of GDPR principles to effectively close existing regulatory gaps. For instance, the integration of Data Protection Impact Assessments (DPIA), comparable to Article 37 of the Indonesian Personal Data Protection Law, which stipulates that *Personal Data Controllers are required to supervise all parties involved in the processing of Personal Data under their control*. The application of AES-256 encryption standards would ensure comprehensive pre-implementation risk assessments. In addition, the establishment of a joint BSSN–DPDP task force for integrated enforcement, along with mandatory independent annual audits conducted by institutions such as ISO 27001–certified auditors, would further strengthen the data protection ecosystem. This approach has proven successful in ASEAN countries such as Singapore (PDPA 2012 incorporating elements of the GDPR), where cyber incidents were reduced by up to 40% (Interpol Annual Report 2024) [12].

Such implementation not only enhances data security but also supports annual e-commerce growth of up to 20%, in line with projections by the Indonesian Ministry of Trade for the period 2025–2030 [13]. Increased consumer confidence in digital transactions—reflected in a 30% rise in the trust index following GDPR implementation in Europe—has the potential to drive transaction volumes from IDR 500 trillion in 2024 to IDR 1,000 trillion by 2030, while simultaneously reducing cyber-related losses of approximately IDR 50 trillion per year.

These measures are expected to foster a sustainable digital economy aligned with the National Medium-Term Development Plan (RPJMN) 2025–2029 [14]. The analysis indicates that while the Personal Data Protection Law regulates data subject rights, the obligations of data controllers and processors, and administrative sanctions, its implementation remains weak due to limited institutional capacity and low consumer awareness. A case study in the e-commerce sector revealed approximately 11 million cyberattacks in the first quarter of 2022 [15], highlighting security deficiencies such as the absence of Data Protection Officers and limited transparency. Compared to the GDPR, the Indonesian PDP Law provides less detailed provisions on audits and sanctions—where the GDPR imposes fines reaching millions of euros, while the PDP Law relies primarily on administrative penalties—thus

reinforcing the recommendation to adopt GDPR accountability principles to strengthen digital literacy and supervisory mechanisms.

IV. CONCLUSION

This study contributes to strengthening personal data protection (PDP) regulation through the adoption of the General Data Protection Regulation (GDPR), enhancing business accountability and public literacy to support a sustainable digital economy. The practical implications include regulatory reinforcement, stricter institutional oversight, and integrated educational programs as key factors in fostering an inclusive and sustainable digital economy in Indonesia. The main limitation of this study lies in its normative focus without empirical field data; therefore, future research is recommended to employ empirical approaches across multiple data breach cases during the period 2025–2030.

REFERENCES

[1] "Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," Pemerintah Pusat, Jakarta, 2022.

[2] "Siaran Pers HM.02.04/368/SET.M.EKON.3/10/2025 Dukungan Transformasi Digital dalam Mengakselerasi Pertumbuhan Ekonomi Nasional," Kementerian Koordinator Bidang Perekonomian Republik Indonesia, Jakarta, 2025.

[3] G. Christmas, "Kebocoran 91 Juta Data Pribadi Konsumen Aplikasi Tokopedia: Studi Normatif dan Tanggungjawab," *Jurnal Ilmu Hukum ,* vol. 13, pp. 1-11, 2025.

[4] A. Burhanuddin, "Tinjauan Yuridis terhadap Perlindungan Konsumen dalam Transaksi Produk Keuangan Syariah di Indonesia," *Sanskara Hukum dan HAM,* vol. 4, pp. 267-274, 2025.

[5] "Hasil Survei Internet APJII 2024," in *Asosiasi Penyelenggara Jasa Internet Indonesia* , Jakarta, 2025.

[6] A. A. C. P. S and D. Pebriani, "Analisis Insiden Kebocoran Data 91 Juta Akun Tokopedia: Dampak dan Upaya Penanganannya," *Integrative Perspective of Social and Science Journal,* vol. 2, no. 3, pp. 4858-44865, 2025.

[7] F. Baso and N. A. L, "Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File," *Information Technology Education Journal,* vol. 3, no. 3, pp. 84-87, 2024.

[8] S. Haristya, S. Laksmi, A. N. T. Astuti and I. F. Dewi, Studi Pendahuluan: Perbandingan Rancangan Undang-undang Perlindungan Data Pribadi dengan Konvensi Eropa 108+ dan GDPR, Jakarta: Tifa Foundation, 2020.

[9] "ENISA Threat Landscape 2023," European Union Agency for Cybersecurity (ENISA), 2023.

[10] "Lanskap Keamanan Siber Indonesia 2024," Badan Siber dan Sandi Negara Rebuplik Indonesia, Jakarta, 2025.

[11] "Data Protection Impact Assessment (DPIA) sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 di Indonesia," *Jurnal Hukum, Politik dan Humaniora,* vol. 2, no. 2, pp. 246-254, 2025.

[12] V. Urquiza, "2024 Annual Report," International Criminal Police Organization (INTERPOL), Lyon, France.

[13] "Peraturan Menteri Perdagangan Nomor 34 Tahun 2025 Rencana Strategis Kementerian Perdagangan Tahun 2025-2029," in *Kementerian Perdagangan*, Jakarta, 2025.

[14] "Peraturan Presiden (Perpres) Nomor 12 Tahun 2025 Rencana Pembangunan Jangka Menengah Nasional Tahun 2025 - 2029," in *Peraturan Presiden (Perpres)*, Jakarta, 2025.

[15] C. J. Sopamena, "UMKM Asia Tenggara Alami 11 Juta Kali Serangan Siber," Jakarta, 2022.