Journal of Private and Commercial Law

A peer-reviewed journal published by Faculty of Law Universitas Negeri Semarang, Indonesia. The title has been indexed by DOAJ, SINTA, GARUDA. ISSN 2599-0314 (Print) 2599-0306 (Online). Available online at https://journal.unnes.ac.id/journals/index.php/jpcl/index

Legal Gaps and Risks in Consumer Data Processing: An Analysis of Indonesian E-Commerce under the Personal Data Protection Law

Tegar Islami Putra [1]✉, **Adinda Zeranica Putri Fakhis** [2], **Anisa Tussaleha** [1], **Mahima Umaela Firdhausya** [1], **Muhammad Hilmi Naufal Aflah** [1], **Souad Ahmed Ezzerouali** [3], **Mohamed Cheick Banane** [4]

[1] Faculty of Law, Universitas Negeri Semarang, Indonesia
[2] Ahmad Ibrahim Kuliyyah of Law, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[3] College of Law, Dhofar University, Salalah, Oman
[4] Faculty of Legal Sciences Ait Melloul, Ibn Zohr University, Agadir, Morocco

✉ Corresponding email: tegarislami44@mail.unnes.ac.id

Abstract

The advancement of information and communication technology has significantly eroded traditional privacy boundaries, particularly within Indonesia's rapidly growing e-commerce sector. The increasing volume and value of online transactions have intensified the collection and processing of consumer personal data, thereby amplifying legal and commercial risks at every stage of data processing. This study aims to analyze the forms of risks arising at each stage of personal data processing on e-commerce websites, as stipulated in Article 16 of Law No. 27 of 2022 on Personal Data Protection, while also identifying existing legal gaps in its implementation. This research adopts a normative juridical approach, employing library-based legal research focused on statutory and conceptual analysis. The findings demonstrate that distinct risks emerge across different stages of personal data processing, both prior to and following data storage by data

controllers. Key risks include non-compliant data collection practices, lack of transparency, excessive and unlawful data collection, as well as unauthorized access, disclosure, modification, misuse, destruction, and loss of personal data. These risks are further exacerbated by ambiguities in regulatory provisions, particularly regarding consent standards, accountability mechanisms, and enforcement. This study contributes to the discourse in private and commercial law by offering a stage-based risk mapping of personal data processing within Indonesian e-commerce, highlighting specific regulatory shortcomings under the Personal Data Protection Law. It provides a nuanced understanding of how legal gaps translate into practical vulnerabilities for consumers. The research also proposes practical mitigation measures, including regular system updates and strengthening the capacity of human resources responsible for data processing, to enhance compliance and consumer data protection in Indonesia's digital economy.

KEYWORDS *Personal Data Protection; E-Commerce; Data Processing Risks; Indonesian Law; Consumer Privacy*

Introduction

The rapid advancement of information and communication technology has fundamentally transformed commercial transactions, particularly through the proliferation of e-commerce platforms.[1] In Indonesia, the exponential growth of digital markets has not only increased transaction volumes but also intensified the large-scale collection, processing, and commercialization of consumer personal data.[2] While these developments generate significant economic benefits, they simultaneously erode traditional privacy boundaries and expose consumers to heightened risks of data misuse. Personal data—once confined to limited transactional

[1] Xing, Zhongwei. "The impacts of Information and Communications Technology (ICT) and E-commerce on bilateral trade flows." *International Economics and Economic Policy* 15, no. 3 (2018): 565-586; Gupta, Anjali. "E-Commerce: Role of E-Commerce in today's business." *International Journal of Computing and Corporate Research* 4, no. 1 (2014): 1-8.

[2] Sarangi, Unmana. "Information economy and data protection laws: a global perspective." *International Journal of Business and Management Research* 6, no. 2 (2018): 15-35; Salam, U., et al. "Indonesia case study: Rapid technological change–challenges and opportunities." *Pathways for Prosperity Commission Background Paper Series* 1, no. 1 (2018): 2009-2019.

contexts—is now continuously processed across complex digital ecosystems, making it increasingly vulnerable at every stage of its lifecycle.[3]

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a critical milestone in Indonesia's effort to establish a comprehensive legal framework governing personal data. The law introduces key principles such as lawful processing, consent, purpose limitation, and accountability of data controllers and processors.[4] However, despite its normative significance, the practical implementation of these principles in e-commerce environments remains contested. Ambiguities persist regarding the validity of consumer consent in digital contracts, the scope of data controller liability, and the effectiveness of enforcement mechanisms.[5] These challenges are particularly evident when examining the stages of personal data processing as outlined in Article 16 of the PDP Law, which encompass data collection, processing, storage, dissemination, and deletion.[6]

From a private and commercial law perspective, the relationship between consumers and e-commerce platforms is often characterized by an imbalance of bargaining power, where standard form contracts and opaque privacy policies limit meaningful consent and control.[7] This imbalance

---

3 Hicks, Jacqueline. "A 'data realm' for the Global South? Evidence from Indonesia." *Third World Quarterly* 42, no. 7 (2021): 1417-1435; Santoso, Edy. "Opportunities and challenges: e-commerce in Indonesia from a legal perspective." *Jurnal Penelitian Hukum De Jure* 22, no. 3 (2022): 395-410. *See also* Haganta, Raphael. "Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic." *Lex Scientia Law Review* 4, no. 2 (2020): 77-90.

4 Diniyanto, Ayon, and Heris Suhendar. "How Law Responds to Technological Development?." *Unnes Law Journal* 6, no. 2 (2020): 405-426; Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (2022): 1443-1457; Marune, Abraham Ethan Martupa Sahat, and Brandon Hartanto. "Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective." *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143-152.

5 Pohan, Tia Deja, and Muhammad Irwan Padli Nasution. "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce." *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen* 1, no. 3 (2023): 42-48; Hidayah, Ardhiana, and Marsitiningsih Marsitiningsih. "Aspek Hukum Perlindungan Data Konsumen E-Commerce." *Kosmik Hukum* 20, no. 1 (2020): 56-63. *See also* Aminah, Sitti, and Herie Saksono. "Digital transformation of the government: A case study in Indonesia." *Jurnal Komunikasi: Malaysian Journal of Communication* 37, no. 2 (2021): 272-288.

6 *See* Republic of Indonesia. *Undang-Undang Nomor Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. (Jakarta: sekretariat Negara, 2022). Available online at https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/undangundang+nomor+27+tahun+2022

7 Mantzari, Despoina. "Power imbalances in online marketplaces: at the crossroads of competition law and regulation." *Research Handbook on the Law and Economics of Competition Enforcement*. (London: Edward Elgar Publishing, 2022), pp. 170-192.

raises critical questions regarding the adequacy of existing legal safeguards in protecting consumer rights. Moreover, the integration of automated systems and cross-border data flows further complicates regulatory oversight, increasing the likelihood of unauthorized access, data breaches, and commercial exploitation.

On the other hand, e-commerce refers to the conduct of commercial transactions—whether involving goods, services, or information—through internet-based platforms. Within this digital environment, e-commerce operators are required to ensure that consumers' personal data is securely processed and adequately protected, as data security constitutes a fundamental element in maintaining consumer trust and fostering long-term commercial relationships.[8] According to the *e-Conomy SEA 2023* report, Indonesia's e-commerce sector recorded a gross transaction value (GTV) of approximately US$62 billion in 2023, reflecting a year-on-year growth of 7%. Moreover, Indonesia is projected to remain a key driver of e-commerce expansion in the Asia-Pacific region, with estimates by RedSeer indicating that the market will reach US$137.5 billion by 2025.[9]

This rapid growth is closely linked to technological advancements, particularly the expansion of internet infrastructure and the widespread penetration of mobile devices, which have significantly accelerated digital trade activities. However, the increasing reliance on e-commerce platforms is accompanied by a corresponding rise in associated risks and unlawful activities.[10] Consumers are increasingly exposed to various challenges, including personal data breaches, deceptive or misleading advertising practices, the circulation of counterfeit goods, and the limited effectiveness of dispute resolution mechanisms.[11] These developments underscore the

---

8 Cheung, Christy MK, and Matthew KO Lee. "Understanding consumer trust in Internet shopping: A multidisciplinary approach." *Journal of the American society for Information Science and Technology* 57, no. 4 (2006): 479-492.

9 *See* Business Indonesia. "Report: e-commerce to fuel Indonesia's digital economy growth to $110 Bn by 2025", *Business Indonesia Report,* November 9, 2023. Retrieved from https://business-indonesia.org/news/report-e-commerce-to-fuel-indonesia-s-digital-economy-growth-to-110-bn-by-2025

10 Purba, Bonaraja, et al. "Transformasi Hukum E-Commerce di Indonesia: Analisis dan Solusi Permasalahan." *Jurnal Sosial Humaniora Sigli* 6, no. 2 (2023): 373-383; Sirait, Ningrum Natasya. "E-commerce growth and development, impact, and challenges in Indonesia." *Neoclassical Legal Review: Journal of Law and Contemporary Issues* 1.2 (2022): 54-72; Ariansyah, Kasmad, et al. "Drivers of and barriers to e-commerce adoption in Indonesia: Individuals' perspectives and the implications." *Telecommunications Policy* 45, no. 8 (2021): 102219.

11 Prastyanti, Rina Arum, et al. "Law and personal data: Offering strategies for consumer protection in new normal situation in Indonesia." *Jurnal Jurisprudence* 11, no. 1 (2022): 82-99; Poernomo, Sri Lestari. "Transformative Justice, Protection of Consumer Personal Data in Online Loan Business in Indonesia." *Russian Law Journal* 11, no. 3 (2023): 559-570; Saimima, Ika Dewi Sartika, and Valentino Gola Patria. "The Fintech

urgent need for robust legal and regulatory frameworks to address the multifaceted risks inherent in the digital marketplace.

In this context, personal data protection emerges as a critical legal issue in e-commerce, particularly with regard to the confidentiality, security, and lawful processing of consumer information.[12] Participation in online transactions inherently requires consumers to disclose personal data, thereby placing them in a position of structural vulnerability within digital commercial ecosystems.[13] To address these concerns, this study adopts the framework set out in Article 16 paragraph (1) of Law No. 27 of 2022 on Personal Data Protection as the analytical basis for examining the stages of personal data processing. Within this framework, e-commerce platforms act as personal data controllers responsible for managing consumer data across a sequence of processing activities, including the collection and acquisition of data, processing and analysis, storage, updating and correction, display and publication, transfer and dissemination, as well as erasure or destruction.[14]

Each stage of this processing cycle entails distinct legal and technical risks. For example, the initial stages of data collection may involve excessive, non-specific, or non-compliant practices, while subsequent

Phenomenon: Protection of Consumer Privacy Data in Online Lending." *Jurnal Kajian Ilmiah* 21, no. 2 (2021): 185-194. For further cases, *see also* Tjipto, Felix Pratama, et al. "Consumer Protection Law: The Case Study of Grabtoko Company in Indonesian E-Commerce Transactions." *Journal of Private and Commercial Law* 5, no. 2 (2021): 120-140; Dinanti, Dinda, et al. "Politics of Law for the Protection of Debtors as Consumers in Fintech based Loaning Services." *Unnes Law Journal* 6, no. 2 (2020): 427-444; Jusmadi, Rhido. "The Existence of Digital Platforms and the Challenges in Enforcement of Indonesian Competition Law." *Unnes Law Journal* 9, no. 1 (2023): 183-204; Fiorentina, Prita, et al. "Legal Protection of Consumer Personal Data in Indonesia Fintech Peer-To-Peer Lending Pioneers." *Pandecta Research Law Journal* 17, no. 2 (2022): 307-312; Sari, Chatrin Intan. "Consumer protection on illegal drugs cases in Indonesia." *Indonesia Media Law Review* 1, no. 1 (2022): 63-80.

12 Sikder, Abu Sayed, and Joe Allen. "An In-depth Exploration of Emerging Technologies and Ethical Considerations in Cross-border E-commerce: A Comprehensive Analysis of Privacy, Data Protection, Intellectual Property Rights, and Consumer Protection in the context of Bangladesh*See*." *International Journal of Imminent Science & Technology*. 1, no. 1 (2023): 116-137.

13 Smith, Rhys, and Jianhua Shao. "Privacy and e-commerce: a consumer-centric perspective." *Electronic Commerce Research* 7, no. 2 (2007): 89-116.

14 Article 16(1) of Indonesia's Personal Data Protection Law (Law No. 27 of 2022) outlines the stages of personal data processing, including collection, processing, storage, updating, disclosure, and deletion. However, the provision is largely descriptive and lacks detailed operational standards for implementation. It does not specify technical requirements, risk-based differentiation, or clear compliance benchmarks for each stage. This creates legal ambiguity in practice, particularly in complex digital ecosystems such as e-commerce, where data flows are continuous and automated. As a result, enforcement becomes inconsistent, and data controllers may interpret obligations differently, weakening overall accountability and reducing the effectiveness of personal data protection.

stages such as storage and processing may expose data to unauthorized access, breaches, or misuse. The risks become even more pronounced during the transfer, dissemination, or disclosure of data, particularly in cross-border digital environments where regulatory oversight may be limited. As an illustration, log data—commonly used in cybersecurity systems for insider-threat detection—contain detailed records of system activities and user interactions, highlighting the sensitivity and strategic importance of personal data within digital infrastructures. These vulnerabilities persist throughout the entire data lifecycle, both before and after storage by the data controller.

Furthermore, the speed, scale, and transnational nature of information flows in the digital era intensify the challenges of protecting privacy rights. The ease with which personal data can be accessed, replicated, and disseminated has significantly weakened traditional privacy boundaries, increasing the likelihood of unauthorized use and exploitation. Against this backdrop, this research aims to analyze the legal risks to consumer personal data protection at each stage of data processing on e-commerce websites in Indonesia. The urgency of this study lies in its effort to provide a systematic, stage-based understanding of data protection risks, enabling regulators, business actors, and other stakeholders to better identify vulnerabilities and strengthen compliance mechanisms. In doing so, this research contributes to bridging the gap between normative legal provisions and the practical realities of data processing in Indonesia's rapidly evolving digital economy.

Several prior studies have examined the issue of personal data protection in the context of e-commerce and information systems, although with different scopes and emphases. Putri and Fahrozi identify three primary threats to combined personal data in e-commerce transactions, particularly in relation to IP address usage: geographic location tracking, unauthorized access and disclosure of personal data, and Distributed Denial of Service (DDoS) attacks. However, the study is limited in scope as it focuses exclusively on combined personal data and does not comprehensively examine risks across the broader stages of personal data processing.[15]

Similarly, Dokuachev, in *"Classification of Personal Data Security Threats in Information Systems"*, analyzes various threats arising in the processing of personal data within information systems. The study

[15] Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com)." *Borneo Law Review* 5, no. 1 (2021): 46-68.

highlights the vulnerability of different categories of data, including passport information, employment records, corporate data, contact details, and email addresses, all of which may become targets of cyberattacks. While the proposed classification provides a useful foundation for developing threat models, the research is primarily technical in nature and does not address the legal dimensions of data protection in e-commerce contexts.[16]

Furthermore, Spalevic, in *"GDPR and Challenges of Personal Data Protection"*, emphasizes that the rapid development of the digital economy—driven by advancements in information and communication technology—has introduced new challenges to privacy and personal data protection. The study identifies key risks such as unauthorized disclosure, identity theft, and cyberbullying. Nevertheless, its focus is largely on the European regulatory framework and does not specifically engage with the Indonesian legal context or the operational realities of e-commerce platforms.[17]

By adopting a stage-based analytical approach grounded in Article 16 of Indonesia's Personal Data Protection Law, this study offers a more comprehensive understanding of how risks manifest throughout the data lifecycle. This research contributes to the literature in several ways. First, it provides a systematic and in-depth analysis of stage-specific risks in personal data processing, thereby enhancing both academic and practical understanding of consumer vulnerabilities in e-commerce. Second, it offers a foundation for the development of more robust legal policies and regulatory frameworks aimed at strengthening personal data protection in Indonesia, with potential relevance at the international level. Third, it proposes practical recommendations for e-commerce operators, particularly in adopting technical and organizational measures to mitigate data security risks. Accordingly, this study not only advances scholarly discourse but also has tangible implications for promoting more secure and sustainable e-commerce practices, especially in light of the increasing incidence of personal data-related crimes in Indonesia.

Against this backdrop, this study seeks to analyze the forms of legal risks that arise at each stage of personal data processing on e-commerce websites in Indonesia. By adopting a normative juridical approach, this research examines how the regulatory framework under the PDP Law addresses (or fails to address) these risks in practice. The novelty of this

[16] Dokuchaev, Vladimir A., Victoria V. Maklachkova, and V. Yu Statev. "Classification of personal data security threats in information systems." *Т-Comm-Телекоммуникации и Транспорт (T-Comm-Telecommunications and Transport)* 14, no. 1 (2020): 56-60.

[17] Spalević, Žaklina, and Kosana Vićentijević. "GDPR and challenges of personal data protection." *The European Journal of Applied Economics* 19, no. 1 (2022): 55-65.

study lies in its stage-based analysis of data processing risks, offering a more granular understanding of how vulnerabilities emerge throughout the data lifecycle rather than treating data protection as a singular legal issue.

This research contributes to the development of private and commercial law scholarship by identifying specific legal gaps within Indonesia's data protection regime and linking them to operational practices in e-commerce. It also provides practical insights for policymakers and industry actors to strengthen regulatory compliance, enhance accountability mechanisms, and improve consumer data protection. In doing so, the study aims to bridge the divide between normative legal provisions and the realities of digital commerce in Indonesia's evolving data-driven economy.

Legal Framework and Pre-Storage Risks in Personal Data Processing on E-Commerce Websites

The legal framework governing personal data processing in Indonesia is primarily regulated under Law No. 27 of 2022 on Personal Data Protection (PDP Law). A central provision relevant to the data processing lifecycle is Article 16, which stipulates: *"The processing of Personal Data consists of: a. acquisition and collection; b. processing and analysis; c. storage; d. repair and updating; e. display, announcement, transfer, dissemination or disclosure; and f. deletion or destruction."* This provision establishes a structured lifecycle approach to data governance, aligning Indonesia with modern data protection systems such as the GDPR. From a doctrinal perspective, Article 16 reflects a functional segmentation of data processing activities, ensuring that each stage is subject to specific legal obligations and risk controls, particularly in high-risk sectors such as e-commerce.[18]

In addition, the classification of personal data is regulated under Article 4 of the PDP Law, which states: *"Personal Data consists of: (1) Specific Personal Data, which includes health data and information, biometric data, genetic data, criminal records, child data, personal*

[18] Rahman, Yogi Muhammad, Aflah Haora, and Elsa Nurfitriani Sutansi. "Personal Data Protection In The Era Of Globalization (Indonesia Perspective)." *Tirtayasa Journal of International Law* 2, no. 1 (2023): 15-30. *See also* Arifin, Ridwan, et al. "Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia." *Jambura Law Review* 3, no. 1 (2021): 135-160; Ningsih, Ayup Suran. "Indonesia Data Protection in the Use of M-Banking, Is It Save?." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 10, no. 3 (2021): 434-445.

financial data, and/or other data in accordance with the provisions of laws and regulations; and (2) General Personal Data, which includes full name, gender, citizenship, religion, marital status, and/or Personal Data combined to identify a person." This classification is normatively significant because it introduces a differentiated protection regime based on sensitivity. In e-commerce systems, however, both categories are often collected simultaneously, which raises compliance concerns regarding proportionality and necessity of data collection.[19]

At the acquisition and collection stage under Article 16(a), the PDP Law imposes strict requirements of transparency and lawful processing. The obligation of transparency is derived from the principle that data subjects must be fully informed regarding the purpose, scope, and consequences of data processing. However, in practice, e-commerce platforms frequently reduce transparency to formal privacy notices that are difficult to interpret. Solove[20] conceptualizes this as "informational asymmetry," where data controllers possess significantly greater informational power than users. This asymmetry weakens the normative effectiveness of consent and challenges the substantive realization of Article 16 obligations.

The legal requirement of transparency must also be understood in relation to consent validity. Although the PDP Law requires consent to be specific, informed, and explicit, in digital practice consent is often obtained through click-wrap mechanisms. Kuner argues that such consent models are structurally problematic because users rarely engage with the full content of privacy policies.[21] Consequently, consent becomes formalistic rather than substantive, raising questions about whether it satisfies the legal threshold of "*informed consent*" as required under data protection principles.

Another significant legal issue is the violation of purpose limitation and data minimization principles, which are implicitly embedded in the structure of the PDP Law. While not explicitly stated in Article 16, these principles are derived from the requirement that data processing must be specific and lawful. Cavoukian's Privacy by Design framework emphasizes

[19] *See* Mutiara, Upik, and Romi Maulana. "Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi." *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020): 42-54; Saly, Jeane Neltje, et al. "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022." *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145-153.

[20] *See* Solove, Daniel J. *Understanding Privacy*. (Harvard, MA: Harvard University Press, 2010).

[21] *See* Kuner, Christopher. *European Data Privacy Law and Online Business*. (Oxford: Clarendon Press, 2003).

that only necessary data should be collected at the source.[22] However, e-commerce platforms often engage in extensive data harvesting, including behavioral tracking and device identification, which exceeds what is necessary for transactional purposes. This practice creates legal tension between operational efficiency and compliance obligations.

The absence of strict purpose limitation creates significant risks of secondary data use. In many e-commerce systems, personal data collected for transaction purposes is later used for profiling, marketing, or algorithmic personalization. Wagner and Janssen argue that vague purpose statements such as "service improvement" fail to meet the legal requirement of specificity, thereby enabling uncontrolled data reuse. This undermines the legal certainty required under Article 16 and increases the likelihood of regulatory non-compliance.[23]

Privacy policies, although widely used as contractual instruments, raise doctrinal concerns regarding their legal enforceability. In principle, privacy policies function as binding agreements between data controllers and users. However, their acceptance through click-wrap mechanisms often lacks meaningful consent. Cate describes this phenomenon as "consent fatigue," where users habitually accept terms without reading or understanding them.[24] This weakens the protective function of privacy policies and raises concerns about their compatibility with the transparency requirement under Article 16(a) PDP Law.

From a systemic perspective, excessive data collection at the acquisition stage increases vulnerability to cyber threats. Ohm argues that large-scale data aggregation inherently increases the risk of re-identification and data breaches, even when anonymization techniques are applied.[25] In e-commerce ecosystems that process millions of transactions daily, centralized databases become attractive targets for cyberattacks. This creates a structural paradox: while data collection enhances business intelligence, it simultaneously increases systemic exposure to security risks.

---

[22] Cavoukian, Ann. "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*. (Dordrecht: Springer Netherlands, 2012), pp. 175-202.

[23] *See* Wagner, Julian. "The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?." *International Data Privacy Law* 8, no. 4 (2018): 318-337; Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." *2011 44th Hawaii International Conference on System Sciences*. IEEE, 2011.

[24] Cate, Fred H. "The limits of notice and choice." *IEEE Security & Privacy* 8, no. 2 (2010): 59-62.

[25] Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57, no. 6 (2010).

In addition to external threats, internal risks significantly contribute to data vulnerability. According to the Ponemon Institute on 2022 as cited by Mostafa[26], a substantial proportion of data breaches result from human error or negligence. In the context of e-commerce platforms, employees with access to personal data may inadvertently expose sensitive information due to inadequate training or weak internal controls. This highlights the importance of organizational compliance mechanisms such as access restrictions, audit trails, and continuous employee training as part of PDP Law implementation.

The risks identified at the acquisition and collection stage can be theoretically analyzed through contextual integrity theory[27] and risk society theory.[28] Contextual integrity emphasizes that privacy is violated when data flows deviate from socially accepted norms, even if consent is formally obtained. Meanwhile, Beck's theory suggests that modern technological systems inherently produce systemic risks that cannot be fully eliminated but must be managed institutionally.[29] In the Indonesian e-commerce context, these theories highlight the gap between the normative structure of Article 16 PDP Law and the practical realities of digital data processing, particularly in pre-storage stages.

Processing, Storage, and Post-Collection Operational Risks in E-Commerce Personal Data Processing

1. Processing and Analytical Phase: Expansion of Surveillance and Erosion of Contextual Privacy

The processing and analytical phase of personal data in e-commerce ecosystems represents a decisive transformation stage in which raw personal data is converted into structured, predictive, and behavioral insights. Under Article 16(b) of Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law), this stage forms an integral part of lawful data lifecycle governance. However, in practice, the processing stage is increasingly characterized by algorithmic intensification, where data is subjected to profiling, segmentation, and predictive analytics.

[26] Mostafa, A. A. "Cyber Crime in Business." *International Journal of Academic Research in Business and Social Sciences*. 12, no. 6 (2022): 962-972.
[27] Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 79.1 (2004): 119.
[28] Beck, Ulrich. *Risk Society: Towards a New Modernity*. Vol. 17. (London: SAGE, 1992).
[29] Beck.

From a theoretical perspective, this phenomenon aligns with Zuboff's concept of surveillance capitalism, which argues that digital platforms extract behavioral data to predict and modify user behavior for commercial gain.[30] Similarly, Floridi emphasizes that digital environments generate "informational overexposure," where individuals lose control over contextual boundaries of their personal data.[31] In the e-commerce context, this is manifested through recommendation engines, behavioral tracking systems, and real-time analytics that continuously process consumer data beyond its original transactional purpose.

This stage also raises concerns under Nissenbaum's theory of contextual integrity, which asserts that privacy violations occur when information flows deviate from socially expected norms. In e-commerce systems, data originally collected for transactional purposes is often repurposed for behavioral profiling without explicit contextual justification. This creates what Tufekci describes as "algorithmic opacity," where users are unable to understand how their data is processed or how decisions are made based on it.[32]

In addition, system-level vulnerabilities become more pronounced at this stage due to increased interconnectivity between databases, third-party APIs, and cloud infrastructures. According to Ohm[33], the aggregation of large datasets significantly increases the probability of re-identification and unintended disclosure, even in systems that employ anonymization techniques. Consequently, the processing phase represents not only a technical transformation of data but also a legal transformation of risk exposure under PDP Law obligations.

A significant legal weakness at this stage is the absence of explicit regulatory provisions governing algorithmic decision-making and automated profiling under the PDP Law. While Article 16 provides structural stages of processing, it does not adequately regulate how data analytics, artificial intelligence, and machine learning systems should be constrained in practice. This creates a normative gap where advanced processing technologies operate beyond the effective reach of legal control.

---

30 Zuboff, Shoshana. "The Age of Surveillance Capitalism." In *Social Theory Re-wired*. (London: Routledge, 2023), pp. 203-213.

31 Floridi, Luciano. *The Ethics of Information*. (Oxford: Oxford University Press, 2013).

32 Tufekci, Zeynep. "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency." *Colorado Technology Law Journal* 13, no. 2 (2015): 203.

33 *See* Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization."

According to Mittelstadt et.al[34], such gaps in algorithmic governance result in "accountability deficits," where individuals cannot meaningfully challenge automated decisions affecting their data

Although the PDP Law requires transparency, there is no detailed enforcement mechanism ensuring meaningful disclosure of algorithmic logic or profiling criteria. As Kuner[35] argues in comparative data protection law, transparency obligations often fail in digital contexts because controllers provide generalized explanations rather than actionable information. This weakens the legal effectiveness of informed consent and limits the ability of data subjects to exercise their rights under Article 16 processing safeguards.

Another legal gap lies in the absence of specific remedies for harms caused by algorithmic profiling or automated decision-making in e-commerce systems. While PDP Law provides general rights to access and correction, it does not explicitly recognize algorithmic harm as a distinct legal category. Floridi emphasizes that informational harms in digital environments require "proactive rights-based governance,"[36] yet Indonesia's framework remains reactive, relying on post-violation remedies rather than preventive algorithmic oversight.

2. *Storage (Retention) Phase: Centralization Risk, Cyber Threats, and Legal Fragility of Data Security*

The storage or retention phase constitutes a high-risk stage in personal data lifecycle management, as it involves the long-term centralization of vast quantities of sensitive and non-sensitive data. Under Article 16(c) of the PDP Law, data controllers are obligated to ensure security and integrity of stored personal data. However, the concentration of data in centralized systems creates what Shoshana Zuboff refers to as "behavioral surplus accumulation," where stored data becomes a high-value target for exploitation.[37]

From a cybersecurity perspective, storage systems are vulnerable to multiple categories of attacks. Logical attacks, such as SQL injection and credential exploitation, represent targeted efforts to breach system architecture by exploiting software vulnerabilities. Malware and

[34] Mittelstadt, Brent Daniel, et al. "The ethics of algorithms: Mapping the debate." *Big Data & Society* 3, no. 2 (2016): 1-21.
[35] *See* Kuner, *European Data Privacy Law and Online Business*.
[36] *See* Floridi, *The Ethics of Information*
[37] *See* Zuboff, "The Age of Surveillance Capitalism." In *Social Theory Re-wired*.

ransomware attacks, as discussed by Dwyer, et.al in cybersecurity literature, involve the infiltration of systems through malicious code capable of encrypting or exfiltrating data.[38] Meanwhile, Denial of Service (DoS) attacks disrupt system availability by overwhelming servers with excessive traffic, a phenomenon widely documented in distributed network security studies.

These threats are compounded by the heterogeneous nature of stored data in e-commerce systems, which includes textual identifiers, biometric data, financial records, images, and behavioral logs. According to Cavoukian, the failure to implement "Privacy by Design" principles at the storage level significantly increases systemic exposure to breach incidents.[39] Multi-format data storage requires differentiated security protocols, yet many e-commerce platforms rely on uniform security architectures that fail to address data-specific vulnerabilities.

Legally, the PDP Law adopts a principle-based approach requiring data controllers to ensure confidentiality, integrity, and availability. However, as Kuner observes in comparative data protection law, principle-based frameworks often face enforcement challenges in rapidly evolving technological environments.[40] This gap between normative obligation and technical implementation creates what Bennett and Raab describe as "compliance without control," where formal adherence to law does not necessarily translate into effective risk mitigation.[41]

In further, a key legal limitation is the absence of binding minimum technical security standards within the PDP Law. Unlike the GDPR, which incorporates risk-based obligations such as "appropriate technical and organizational measures," Indonesia's PDP Law does not specify encryption standards, authentication protocols, or breach resilience requirements. This creates interpretive flexibility that may lead to inconsistent implementation across e-commerce platforms.

Although data breach risks are significant at the storage stage, the PDP Law provides limited clarity on mandatory breach notification timelines and enforcement mechanisms. Kuner highlights that effective breach governance requires strict temporal obligations,[42] however, in Indonesia, enforcement mechanisms remain underdeveloped. This reduces regulatory deterrence and delays consumer awareness of potential harm.

---

[38] Dwyer, Andrew C., et al. "What can a critical cybersecurity do?." *International Political Sociology* 16, no. 3 (2022): olac013.

[39] *See* Cavoukian, "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*.

[40] *See* Kuner, *European Data Privacy Law and Online Business*.

[41] *See* Bennett, and Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*.

[42] *See* Kuner, *European Data Privacy Law and Online Business*.

Another structural weakness is the lack of a comprehensive liability regime for data controllers in cases of storage failures. While civil liability may be implied under general tort principles, the PDP Law does not establish strict liability or presumption of negligence in cases of large-scale data breaches. Bennett and Raab argue that without clear liability allocation, data protection regimes risk becoming "symbolic rather than effective."[43]

3. *Human Error, Internal Threats, and Organizational Vulnerability*

Beyond external cyber threats, internal risks remain one of the most persistent vulnerabilities across both processing and storage phases. Empirical findings from the Ponemon Institute consistently indicate that human error accounts for a significant proportion of data breaches globally. In e-commerce systems, such errors may include misconfiguration of databases, improper access rights allocation, or accidental disclosure of sensitive datasets.

From an organizational theory perspective, Siponen and Vance argue that information security failures are often rooted in behavioral and compliance deficiencies rather than purely technological weaknesses.[44] This suggests that legal compliance under PDP Law must be complemented by organizational discipline and security culture. In many cases, insider threats are not malicious but arise from inadequate training and weak procedural enforcement.

Moreover, Floridi (2016) emphasizes that the increasing automation of data processing systems paradoxically increases reliance on human oversight at critical decision points. A single human error in system configuration can lead to cascading failures across interconnected databases. This is particularly relevant in e-commerce environments where real-time processing and high transaction volumes amplify the impact of operational mistakes.

In the further context, the PDP Law does not explicitly require mandatory certification or standardized training for employees handling personal data. This creates variability in compliance capacity across organizations. Siponen and Vance emphasize that security behavior is

[43] Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. (London: Routledge, 2017).

[44] Vance, Anthony, and Mikko T. Siponen. "IS security policy violations: A rational choice perspective." *Journal of Organizational and End User Computing (JOEUC)* 24, no. 1 (2012): 21-41.

strongly influenced by institutional enforcement structures[45], yet Indonesia's legal framework lacks enforceable HR compliance obligations.

While external cyber threats are widely acknowledged, insider threats are not explicitly regulated under PDP Law. This creates a blind spot in legal accountability for internal actors who misuse or negligently handle personal data. From a governance perspective, this omission weakens the completeness of the risk management framework. There is also limited obligation for continuous internal auditing of data access and usage logs. In comparative frameworks such as GDPR, auditability is a key compliance requirement. However, Indonesia's PDP Law does not fully institutionalize continuous monitoring mechanisms, resulting in reactive rather than preventive enforcement structures.

4. *Data Security Architecture and Regulatory Governance as Risk Mitigation Mechanisms*

Given the complexity of risks in processing and storage phases, effective mitigation requires a multi-layered data security architecture that integrates technical, organizational, and legal safeguards. Under PDP Law obligations, data controllers are required to implement measures ensuring protection against unauthorized access, disclosure, alteration, and destruction.

From a technical perspective, this includes encryption protocols, zero-trust architecture, intrusion detection systems, and continuous vulnerability assessments. From an organizational perspective, ISO/IEC 27001 standards emphasize the importance of access control systems, audit logging, and incident response frameworks. These technical measures are supported by governance mechanisms that ensure accountability and traceability of data processing activities.

Theoretically, this aligns with Beck's (1992) risk society theory, which posits that modern technological systems generate systemic risks that cannot be eliminated but must be managed through institutional reflexivity. In this context, data protection is not merely a compliance requirement but a governance function embedded in digital infrastructure. Furthermore, Nissenbaum's (2010) contextual integrity framework reinforces the need for context-sensitive data governance, ensuring that data flows remain consistent with user expectations and legal norms. This requires e-commerce platforms to move beyond formal compliance toward adaptive

[45] *See* Vance, and Siponen. "IS security policy violations: A rational choice perspective."

governance models that integrate legal, technical, and ethical considerations.

The PDP Law does not explicitly integrate international technical standards such as ISO/IEC 27001 into its compliance framework. This creates a disconnect between legal obligations and operational cybersecurity practices, reducing enforceability in technical environments. Unlike GDPR Article 25, Indonesia's PDP Law does not explicitly mandate "privacy by design and by default." Cavoukian emphasizes that preventive design is essential for systemic risk reduction, but the absence of such obligation limits proactive compliance enforcement.[46]

Finally, institutional fragmentation in enforcement creates uncertainty regarding supervisory authority and coordination mechanisms. Without a centralized and empowered data protection authority, enforcement may remain inconsistent, reducing the overall effectiveness of governance frameworks.

Post-Storage Risks in Personal Data Processing: Correction, Disclosure, and Deletion Vulnerabilities in E-Commerce Systems

1. Risks in Data Correction and Updating Phase: Data Integrity, Human Error, and Legal Fragility

The correction and updating phase of personal data processing represents a crucial governance mechanism for ensuring data accuracy and reliability in e-commerce ecosystems. Under the Indonesian Personal Data Protection Law (Law No. 27 of 2022), data controllers are legally required to maintain accurate and up-to-date personal data in accordance with processing purposes. However, despite this normative requirement, the implementation of data rectification mechanisms remains highly vulnerable to operational inefficiencies. From a legal perspective, this stage is essential because inaccurate personal data may lead to unlawful decisions affecting consumer rights, including credit scoring, transaction rejection, or profiling errors. Scholars such as Bygrave (2014) emphasize that data accuracy is not merely a technical requirement but a substantive element of informational justice, ensuring fairness in automated decision-making systems.

A primary risk at this stage is data input errors, lack of validation mechanisms, and systemic inconsistencies within integrated e-commerce

[46] *See* Cavoukian, "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*.

databases. These problems are exacerbated by the increasing complexity of digital platforms, where data flows across multiple systems and third-party services. Floridi (2014) argues that digital ecosystems inherently generate "informational entropy," where data degradation occurs due to continuous modification without robust verification structures. In practice, weak validation systems allow incorrect data to persist and propagate across interconnected platforms, creating cumulative distortions in consumer profiles.

Furthermore, human error remains the dominant structural vulnerability in data correction processes. According to the Ponemon Institute (2022), human negligence accounts for a significant proportion of data breaches globally, particularly in systems requiring continuous data updates. Siponen and Vance further argue that organizational compliance behavior is often weaker than technological safeguards, meaning that even well-designed systems may fail due to improper human interaction.[47] In e-commerce contexts, employees responsible for updating databases may unintentionally introduce inconsistencies due to lack of training or procedural oversight. This demonstrates that legal compliance under PDP Law cannot be achieved without parallel investment in human capital and institutional discipline.

2. *Risks in Disclosure, Transfer, and Dissemination Phase: Structural Exposure and Jurisdictional Fragmentation*

The disclosure, transfer, and dissemination phase of personal data processing represents one of the most legally sensitive stages in the data lifecycle. Under Article 16 of the PDP Law, data processing activities involving disclosure must adhere to principles of lawfulness, purpose limitation, and security safeguards. However, in e-commerce ecosystems, data dissemination often extends beyond intended boundaries due to system interconnectivity and platform integration. This creates a structural tension between operational efficiency and legal compliance, particularly in cross-platform data environments.

One of the most critical risks is unauthorized internal access or improper display of personal data within organizational systems. This occurs when access control mechanisms are insufficient or improperly configured, allowing employees or system users to view data beyond their

47 *See* Vance, and Siponen. "IS security policy violations: A rational choice perspective."

authorization level. Nissenbaum's (2010) theory of contextual integrity is highly relevant here, as it argues that privacy violations occur when information flows deviate from expected contextual norms, even in the absence of malicious intent. In e-commerce systems, internal exposure of consumer data undermines both legal compliance and consumer trust.

Another significant issue is improper data announcement exceeding lawful disclosure limits, where personal data controllers disclose more information than necessary for operational purposes. This violates the principle of data minimization, which is central to modern data protection regimes such as the GDPR. Wagner and Janssen (2019) argue that vague disclosure practices create regulatory ambiguity, allowing excessive data exposure under broad justifications such as "service improvement" or "user personalization." This lack of specificity weakens legal enforceability under PDP Law principles.

Furthermore, cross-border data transfers and inter-platform dissemination introduce significant jurisdictional fragmentation risks. Data transferred between countries or platforms may fall outside effective regulatory oversight, creating enforcement gaps. Kuner highlights that cross-border data flows are one of the most challenging aspects of global data governance due to inconsistent legal standards.[48] In Indonesia's context, such transfers may expose data to foreign jurisdictions with weaker or incompatible privacy protections, increasing systemic vulnerability.

Lastly, software malfunction and system errors can lead to unintended disclosure or incorrect dissemination of personal data. Ohm notes that digital systems are inherently prone to failure, and even minor software errors can result in large-scale privacy violations.[49] In high-volume e-commerce environments, such technical failures can rapidly escalate into systemic breaches affecting millions of users.

3. *Risks in Deletion and Destruction Phase: Data Persistence, Institutional Weakness, and Enforcement Gaps*

The deletion and destruction phase represents the final safeguard in the personal data lifecycle, governed by Articles 42, 43, and 44 of the PDP Law, which mandate termination of processing when data is no longer necessary, consent is withdrawn, or data is unlawfully obtained. However,

[48] *See* Kuner, *European Data Privacy Law and Online Business*.
[49] *See* Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization."

despite its normative clarity, this stage is characterized by significant implementation failures and institutional weaknesses.

A major risk is the ineffectiveness of data deletion processes, particularly due to persistence in digital environments such as search engines and cached systems. This phenomenon is closely linked to the "right to delisting" under Government Regulation No. 71 of 2019. However, as Solove (2013) argues, digital deletion is inherently incomplete because data replication across networks creates "informational permanence." Even after deletion requests are executed, copies of personal data may remain accessible through third-party indexing systems or archived databases.

Another significant issue is the lack of effective institutional mechanisms for enforcing deletion obligations. Unlike the GDPR system, which is supported by strong supervisory authorities, Indonesia's enforcement framework remains fragmented and institutionally limited. Bennett and Raab emphasize that effective data protection requires strong regulatory institutions capable of monitoring compliance, imposing sanctions, and ensuring corrective action.[50] Without such institutional strength, deletion obligations risk becoming symbolic rather than enforceable.

Additionally, incomplete implementation of Articles 42–44 PDP Law creates legal uncertainty regarding retention and destruction obligations. While the law provides conditions for lawful deletion, it does not fully operationalize technical or procedural standards for execution. This creates variability in compliance practices across e-commerce platforms, leading to inconsistent enforcement outcomes. Cavoukian's Privacy by Design framework stresses that deletion mechanisms must be embedded into system architecture rather than applied as afterthoughts.[51]

4. *Structural Governance Gap and the Need for Integrated Risk Architecture*

A broader structural issue underlying these risks is the absence of centralized enforcement authority and weak coordination mechanisms in Indonesia's data protection governance system. This institutional gap reduces the effectiveness of PDP Law implementation and creates uncertainty in compliance enforcement. Beck's (1992) risk society theory is

[50] *See See* Bennett, and Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*.

[51] *See* Cavoukian, "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*.

relevant here, as it suggests that modern technological risks require reflexive institutional governance rather than fragmented regulatory responses.

To address these challenges, scholars increasingly advocate for integrated governance frameworks combining legal, technical, and organizational safeguards. From a technical perspective, secure deletion protocols, encryption lifecycle management, and automated compliance systems are necessary. From an organizational standpoint, continuous auditing, accountability frameworks, and employee training are essential. From a reputational perspective, e-commerce platforms must develop trust-based governance models, as consumer trust is increasingly shaped by perceived data protection reliability.

Ultimately, effective post-storage governance requires a shift from formal legal compliance toward adaptive risk-based regulation, where legal norms, technological design, and organizational behavior operate in an integrated system. Without such alignment, the risks embedded in correction, disclosure, and deletion phases will continue to undermine the effectiveness of personal data protection in Indonesia's e-commerce ecosystem.

Beyond Compliance: Closing the Enforcement Gap in Indonesia's Personal Data Protection Regime

The enactment of Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a significant milestone in the formal recognition of personal data as a legal object requiring structured protection. However, the increasing incidence of personal data-related crimes in Indonesia indicates that legal formalization alone is insufficient to ensure effective protection. Cybercrime reports and digital fraud cases show a growing trend of data breaches involving e-commerce platforms, financial services, and digital applications. This suggests a widening gap between normative legal frameworks and practical enforcement realities. As Floridi (2014) argues, the governance of digital information requires not only legal articulation but also systemic integration between law, technology, and institutional capacity. In the Indonesian context, this gap reflects a transition from a formal compliance model toward a more complex risk governance environment.

The rise of personal data crime in Indonesia is closely linked to the rapid expansion of digital economy ecosystems, particularly e-commerce

platforms that rely heavily on data-driven business models. According to Zuboff (2019), digital platforms operate through "surveillance capitalism," where personal data becomes a primary economic resource. In such systems, data is continuously extracted, processed, and monetized, increasing exposure to misuse and unauthorized access. In Indonesia, the increasing frequency of data leaks, phishing attacks, and identity theft cases reflects the structural vulnerabilities embedded in digital infrastructure. These risks are not merely incidental but systemic, arising from the scale and complexity of data processing activities. Consequently, legal protection mechanisms must evolve to address not only isolated breaches but also systemic patterns of exploitation.

One of the central challenges in Indonesia's PDP regime is the weak integration between legal norms and technical enforcement mechanisms. While the PDP Law establishes principles such as lawfulness, transparency, and accountability, it does not sufficiently operationalize these principles into enforceable technical standards. This creates what Kuner describes as a "normative-technical divide," where legal requirements exist at a doctrinal level but lack practical implementation tools.[52] For example, obligations related to data security and breach prevention are not accompanied by mandatory technical benchmarks such as encryption standards or system audit requirements. As a result, compliance becomes fragmented and inconsistent across different sectors and organizations.

This disconnect between law and technology is particularly evident in the absence of standardized cybersecurity obligations within the PDP Law. Unlike the European Union's GDPR, which integrates risk-based technical requirements such as "appropriate technical and organizational measures," Indonesia's framework remains principle-based without detailed operational guidance. According to Bennett and Raab, such principle-based systems often risk becoming "symbolic compliance regimes," where organizations formally comply with legal requirements without achieving substantive data protection outcomes.[53] This situation highlights the need for stronger integration between legal drafting and cybersecurity engineering standards.

Increasing personal data crime also reflects structural weaknesses in enforcement capacity. Even though regulatory provisions exist, enforcement mechanisms remain limited in terms of institutional coordination, technical expertise, and monitoring capability. Beck's (1992) risk society theory is relevant in explaining this phenomenon, as modern

[52] *See* Kuner, *European Data Privacy Law and Online Business*.
[53] *See* Bennett, and Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*.

technological risks often exceed the regulatory capacity of traditional institutions. In Indonesia, the enforcement of data protection law requires coordination across multiple agencies, yet institutional fragmentation reduces effectiveness. Without a centralized and empowered supervisory authority, enforcement becomes reactive rather than preventive.

Another critical dimension is the importance of combining regulatory compliance with system security upgrades. Legal compliance alone is insufficient if not supported by robust technical infrastructure. Cavoukian's "Privacy by Design" framework emphasizes that privacy protection must be embedded into system architecture rather than applied as an external layer.[54] In e-commerce environments, this includes encryption protocols, secure authentication systems, intrusion detection mechanisms, and continuous vulnerability assessments. Without these technical safeguards, even legally compliant organizations remain exposed to high levels of cyber risk.

System security upgrades also play a crucial role in reducing operational vulnerabilities in data processing environments. Ohm highlights that large-scale data aggregation inherently increases the risk of re-identification and unauthorized access, even in systems that employ anonymization techniques.[55] In Indonesia's digital economy, where data is processed across multiple platforms and cloud infrastructures, system security becomes a foundational requirement for legal compliance. Therefore, technical resilience must be understood as a legal necessity rather than a purely IT-related concern.

In addition to technical infrastructure, human resource capacity building is a critical component of effective data protection governance. Empirical studies, including those by the Ponemon Institute show that a significant proportion of data breaches are caused by human error rather than external attacks. Siponen and Vance argue that information security behavior is strongly influenced by organizational culture and employee awareness.[56] In the Indonesian context, many data protection failures occur due to inadequate training, weak internal controls, and lack of awareness regarding legal obligations under the PDP Law.

Human resource development must therefore be integrated into compliance strategies through continuous training, certification programs, and internal audit mechanisms. Floridi (2016) emphasizes that digital

---

54 *See See* Cavoukian, "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*.

55 *See* Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization."

56 *See* Vance, and Siponen. "IS security policy violations: A rational choice perspective."

governance requires “responsible informational agents” who understand both legal and technical dimensions of data processing. Without such capacity building, legal compliance remains superficial and reactive. This is particularly relevant in e-commerce companies where data processing is highly automated but still dependent on human oversight in critical operational stages.

Corporate governance also plays a central role in bridging the enforcement gap. Effective data protection requires internal accountability structures, including data protection officers, compliance committees, and risk management frameworks. Nissenbaum’s (2010) theory of contextual integrity suggests that privacy protection must be embedded within organizational practices and decision-making structures. In the absence of strong governance mechanisms, data protection obligations under the PDP Law risk being treated as external legal formalities rather than internal organizational responsibilities.

Furthermore, corporate governance must extend beyond compliance to include trust-building mechanisms with consumers. Trust is a critical asset in digital economies, as users increasingly evaluate platforms based on perceived data security and transparency. According to Mayer, Davis, and Schoorman[57], trust is built through perceived competence, integrity, and benevolence. In e-commerce ecosystems, strong data protection practices contribute directly to consumer trust, which in turn influences platform sustainability and market competitiveness.

Ultimately, closing the enforcement gap in Indonesia’s personal data protection regime requires a multi-dimensional approach that integrates legal, technical, and organizational elements. Beck’s (1992) risk society framework suggests that modern risks cannot be managed through law alone but require reflexive governance structures that adapt to technological complexity. In this sense, the effectiveness of the PDP Law depends not only on its normative strength but also on its ability to be operationalized through institutional coordination and technological integration.

The Indonesian experience demonstrates that personal data protection is no longer solely a legal issue but a systemic governance challenge. As digital transformation accelerates, the boundary between legal compliance and technical security becomes increasingly blurred. Therefore, addressing personal data crime requires a holistic strategy that integrates regulatory enforcement, cybersecurity infrastructure, human resource development, and corporate governance. Without such integration, the

[57] Schoorman, F. David, Roger C. Mayer, and James H. Davis. "Organizational trust: Philosophical perspectives and conceptual definitions." *Academy of Management Review* 21, no. 2 (1996): 337-340.

enforcement gap will persist, undermining the effectiveness of Indonesia's data protection regime in the long term.

Conclusion

This study concludes that Indonesia's Personal Data Protection Law (Law No. 27 of 2022) provides a comprehensive normative framework for regulating personal data processing in e-commerce, particularly through the structured lifecycle approach under Article 16. However, the main research question—how risks emerge at each stage of personal data processing in e-commerce websites—reveals a persistent gap between legal design and practical enforcement. The findings confirm that risks occur systematically across all stages, including non-transparent and excessive data collection, algorithmic and processing vulnerabilities, cybersecurity threats in storage systems, human error in data correction, uncontrolled disclosure and cross-border transfers, and ineffective deletion mechanisms. These risks are not isolated technical issues but interconnected governance failures reflecting weak integration between legal norms, technological safeguards, and organizational practices. The study therefore concludes that the effectiveness of personal data protection in Indonesian e-commerce is currently constrained by an enforcement gap that limits the operational impact of otherwise robust legal provisions.

To address these challenges, this study recommends a multi-layered reform strategy combining (i) stronger regulatory enforcement through the establishment of a centralized and independent data protection authority, (ii) mandatory adoption of technical standards such as encryption, privacy-by-design, and cybersecurity certification for e-commerce platforms, (iii) structured human resource capacity building through compulsory data protection training and certification programs, and (iv) enhanced corporate governance frameworks that institutionalize accountability, auditability, and consumer trust mechanisms. For future research, further empirical studies are needed to examine how Indonesian e-commerce companies actually implement PDP Law compliance at the operational level, particularly in relation to algorithmic decision-making, cross-border data transfers, and deletion practices. Comparative studies with GDPR-based jurisdictions are also recommended to identify best practices for closing the gap between legal norms and technical enforcement in developing digital economies.

References

Aminah, Sitti, and Herie Saksono. "Digital transformation of the government: A case study in Indonesia." *Jurnal Komunikasi: Malaysian Journal of Communication* 37, no. 2 (2021): 272-288. https://doi.org/10.17576/jkmjc-2021-3702-17

Ariansyah, Kasmad, et al. "Drivers of and barriers to e-commerce adoption in Indonesia: Individuals' perspectives and the implications." *Telecommunications Policy* 45, no. 8 (2021): 102219. https://doi.org/10.1016/j.telpol.2021.102219

Arifin, Ridwan, et al. "Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia." *Jambura Law Review* 3, no. 1 (2021): 135-160. https://doi.org/10.33756/jlr.v3i0.9635

Beck, Ulrich. *Risk Society: Towards a New Modernity*. Vol. 17. (London: SAGE, 1992).

Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. (London: Routledge, 2017). https://doi.org/10.4324/9781315199269

Business Indonesia. "Report: e-commerce to fuel Indonesia's digital economy growth to $110 Bn by 2025", *Business Indonesia Report*, November 9, 2023. Retrieved from https://business-indonesia.org/news/report-e-commerce-to-fuel-indonesia-s-digital-economy-growth-to-110-bn-by-2025

Cate, Fred H. "The limits of notice and choice." *IEEE Security & Privacy* 8, no. 2 (2010): 59-62. https://doi.org/10.1109/msp.2010.84

Cavoukian, Ann. "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*. (Dordrecht: Springer Netherlands, 2012), pp. 175-202. https://doi.org/10.1007/978-94-007-5170-5_8

Cheung, Christy MK, and Matthew KO Lee. "Understanding consumer trust in Internet shopping: A multidisciplinary approach." *Journal of the American society for Information Science and Technology* 57, no. 4 (2006): 479-492. https://doi.org/10.1002/asi.20312

Dinanti, Dinda, et al. "Politics of Law for the Protection of Debtors as Consumers in Fintech based Loaning Services." *Unnes Law Journal* 6, no. 2 (2020): 427-444. https://doi.org/10.15294/ulj.v6i2.48219

Diniyanto, Ayon, and Heris Suhendar. "How Law Responds to Technological Development?." *Unnes Law Journal* 6, no. 2 (2020): 405-426. https://doi.org/10.15294/ulj.v6i2.48218

Dokuchaev, Vladimir A., Victoria V. Maklachkova, and V. Yu Statev. "Classification of personal data security threats in information systems." *T-Comm-Телекоммуникации и Транспорт (T-Comm-Telecommunications and Transport)* 14, no. 1 (2020): 56-60. https://doi.org/10.36724/2072-8735-2020-14-1-56-60

Dwyer, Andrew C., et al. "What can a critical cybersecurity do?." *International Political Sociology* 16, no. 3 (2022): olac013.
Fiorentina, Prita, et al. "Legal Protection of Consumer Personal Data in Indonesia Fintech Peer-To-Peer Lending Pioneers." *Pandecta Research Law Journal* 17, no. 2 (2022): 307-312. https://doi.org/10.15294/pandecta.v17i2.40235
Floridi, Luciano. *The Ethics of Information*. (Oxford: Oxford University Press, 2013).
Gupta, Anjali. "E-Commerce: Role of E-Commerce in today's business." *International Journal of Computing and Corporate Research* 4, no. 1 (2014): 1-8.
Haganta, Raphael. "Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic." *Lex Scientia Law Review* 4, no. 2 (2020): 77-90.
Hicks, Jacqueline. "A 'data realm' for the Global South? Evidence from Indonesia." *Third World Quarterly* 42, no. 7 (2021): 1417-1435. https://doi.org/10.1080/01436597.2021.1901570
Hidayah, Ardhiana, and Marsitiningsih Marsitiningsih. "Aspek Hukum Perlindungan Data Konsumen E-Commerce." *Kosmik Hukum* 20, no. 1 (2020): 56-63. https://doi.org/10.30595/kosmikhukum.v20i1.8251
Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." *2011 44th Hawaii International Conference on System Sciences*. IEEE, 2011. https://doi.org/10.1109/hicss.2011.103
Jusmadi, Rhido. "The Existence of Digital Platforms and the Challenges in Enforcement of Indonesian Competition Law." *Unnes Law Journal* 9, no. 1 (2023): 183-204. https://doi.org/10.15294/ulj.v9i1.37279
Kuner, Christopher. *European Data Privacy Law and Online Business*. (Oxford: Clarendon Press, 2003).
Mantzari, Despoina. "Power imbalances in online marketplaces: at the crossroads of competition law and regulation." *Research Handbook on the Law and Economics of Competition Enforcement*. (London: Edward Elgar Publishing, 2022), pp. 170-192. https://doi.org/10.2139/ssrn.4873444
Marune, Abraham Ethan Martupa Sahat, and Brandon Hartanto. "Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective." *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143-152. https://doi.org/10.46336/ijbesd.v2i4.170
Mittelstadt, Brent Daniel, et al. "The ethics of algorithms: Mapping the debate." *Big Data & Society* 3, no. 2 (2016): 1-21. https://doi.org/10.1177/2053951716679679
Mostafa, A. A. "Cyber Crime in Business." *International Journal of Academic Research in Business and Social Sciences*. 12, no. 6 (2022): 962-972.
Mutiara, Upik, and Romi Maulana. "Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri

Pribadi." *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020): 42-54. https://doi.org/10.31000/ijlp.v1i1.2648

Ningsih, Ayup Suran. "Indonesia Data Protection in the Use of M-Banking, Is It Save?." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 10, no. 3 (2021): 434-445. https://doi.org/10.24843/jmhu.2021.v10.i03.p01

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 79.1 (2004): 119.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57, no. 6 (2010).

Poernomo, Sri Lestari. "Transformative Justice, Protection of Consumer Personal Data in Online Loan Business in Indonesia." *Russian Law Journal* 11, no. 3 (2023): 559-570. https://doi.org/10.52783/rlj.v11i3.1196

Pohan, Tia Deja, and Muhammad Irwan Padli Nasution. "Perlindungan Hukum Data Pribadi Konsumen dalam Platform E-Commerce." *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen* 1, no. 3 (2023): 42-48. https://doi.org/10.47861/sammajiva.v1i3.336

Prastyanti, Rina Arum, et al. "Law and personal data: Offering strategies for consumer protection in new normal situation in Indonesia." *Jurnal Jurisprudence* 11, no. 1 (2022): 82-99. https://doi.org/10.23917/jurisprudence.v11i1.14756

Purba, Bonaraja, et al. "Transformasi Hukum E-Commerce di Indonesia: Analisis dan Solusi Permasalahan." *Jurnal Sosial Humaniora Sigli* 6, no. 2 (2023): 373-383. https://doi.org/10.47647/jsh.v6i2.1570

Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com)." *Borneo Law Review* 5, no. 1 (2021): 46-68. https://doi.org/10.35334/bolrev.v5i1.2014

Rahman, Yogi Muhammad, Aflah Haora, and Elsa Nurfitriani Sutansi. "Personal Data Protection In The Era Of Globalization (Indonesia Perspective)." *Tirtayasa Journal of International Law* 2, no. 1 (2023): 15-30. https://doi.org/10.51825/tjil.v2i1.19603

Republic of Indonesia. *Undang-Undang Nomor Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. (Jakarta: sekretariat Negara, 2022). Available online at https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/undangundang+nomor+27+tahun+2022

Saimima, Ika Dewi Sartika, and Valentino Gola Patria. "The Fintech Phenomenon: Protection of Consumer Privacy Data in Online Lending." *Jurnal Kajian Ilmiah* 21, no. 2 (2021): 185-194. https://doi.org/10.31599/jki.v21i2.564

Salam, U., et al. "Indonesia case study: Rapid technological change–challenges and opportunities." *Pathways for Prosperity Commission Background Paper Series* 1, no. 1 (2018): 2009-2019.

Saly, Jeane Neltje, et al. "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022." *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145-153.

Santoso, Edy. "Opportunities and challenges: e-commerce in Indonesia from a legal perspective." *Jurnal Penelitian Hukum De Jure* 22, no. 3 (2022): 395-410. https://doi.org/10.30641/dejure.2022.v22.395-410

Sarangi, Unmana. "Information economy and data protection laws: a global perspective." *International Journal of Business and Management Research* 6, no. 2 (2018): 15-35. https://doi.org/10.37391/ijbmr.060203

Sari, Chatrin Intan. "Consumer protection on illegal drugs cases in Indonesia." *Indonesia Media Law Review* 1, no. 1 (2022): 63-80. https://doi.org/10.15294/imrev.v1i1.56678

Schoorman, F. David, Roger C. Mayer, and James H. Davis. "Organizational trust: Philosophical perspectives and conceptual definitions." *Academy of Management Review* 21, no. 2 (1996): 337-340. https://doi.org/10.5465/amr.1996.27003218

Sikder, Abu Sayed, and Joe Allen. "An In-depth Exploration of Emerging Technologies and Ethical Considerations in Cross-border E-commerce: A Comprehensive Analysis of Privacy, Data Protection, Intellectual Property Rights, and Consumer Protection in the context of Bangladesh." *International Journal of Imminent Science & Technology*. 1, no. 1 (2023): 116-137. https://doi.org/10.70774/ijist.v1i1.15

Sirait, Ningrum Natasya. "E-commerce growth and development, impact, and challenges in Indonesia." *Neoclassical Legal Review: Journal of Law and Contemporary Issues* 1.2 (2022): 54-72. https://doi.org/10.32734/nlr.v1i1.9603

Smith, Rhys, and Jianhua Shao. "Privacy and e-commerce: a consumer-centric perspective." *Electronic Commerce Research* 7, no. 2 (2007): 89-116. https://doi.org/10.1007/s10660-007-9002-9

Solove, Daniel J. *Understanding Privacy*. (Harvard, MA: Harvard University Press, 2010).

Spalević, Žaklina, and Kosana Vićentijević. "GDPR and challenges of personal data protection." *The European Journal of Applied Economics* 19, no. 1 (2022): 55-65. https://doi.org/10.5937/ejae19-36596

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (2022): 1443-1457. https://doi.org/10.1108/jfc-09-2021-0193

Tjipto, Felix Pratama, et al. "Consumer Protection Law: The Case Study of Grabtoko Company in Indonesian E-Commerce Transactions." *Journal of Private and Commercial Law* 5, no. 2 (2021): 120-140. https://doi.org/10.15294/jpcl.v5i2.32161

Tufekci, Zeynep. "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency." *Colorado Technology Law Journal* 13, no. 2 (2015): 203.

Vance, Anthony, and Mikko T. Siponen. "IS security policy violations: A rational choice perspective." *Journal of Organizational and End User Computing (JOEUC)* 24, no. 1 (2012): 21-41. https://doi.org/10.4018/joeuc.2012010102

Wagner, Julian. "The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?." *International Data Privacy Law* 8, no. 4 (2018): 318-337. https://doi.org/10.1093/idpl/ipy008

Xing, Zhongwei. "The impacts of Information and Communications Technology (ICT) and E-commerce on bilateral trade flows." *International Economics and Economic Policy* 15, no. 3 (2018): 565-586. https://doi.org/10.1007/s10368-017-0375-5

Zuboff, Shoshana. "The Age of Surveillance Capitalism." In *Social Theory Re-wired*. (London: Routledge, 2023), pp. 203-213. https://doi.org/10.4324/9781003320609-27

***

"In a digital world, privacy must be a priority, not an option."

Margrethe Vestager (EU Competition & Digital Policy Leader)

DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

This research funded by Universitas Negeri Semarang (UNNES), Indonesia.

ACKNOWLEDGMENT

The authors gratefully acknowledge the collaborative research support provided by the Faculty of Law, Universitas Negeri Semarang, Indonesia; the Ahmad Ibrahim Kulliyyah of Law, International Islamic University Malaysia, Kuala Lumpur, Malaysia; the College of Law, Dhofar University, Salalah, Oman; and the Faculty of Legal Sciences Ait Melloul, Ibn Zohr University, Agadir, Morocco. This research is the result of an international academic collaboration aimed at advancing comparative legal scholarship in the field of personal data protection and e-commerce law. The authors extend their sincere appreciation to all institutional partners for their valuable academic contributions, insightful discussions, and continuous support throughout the research process.

GENERATIVE AI STATEMENT

None

HISTORY OF ARTICLE

Submitted : February 11, 2024
Revised : May 21, 2024; September 11, 2024; October 30, 2024
Accepted : November 5, 2024
Published : November 30, 2024