Journal of Cyber Law
and Information Security
Volume 3, Number 2, 2024

Effectiveness of Personal Data Protection Regulations in Electronic Commerce Transactions in Indonesia: Challenges and the Urgency of Legal Reform

Setya Eko Wasito[1]

[1] Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Abstract

Article history:
Received: September 9, 2024
Revised: October 17, 2024
Accepted: November 4, 2024
Published: December 30, 2024

Keywords:
Personal Data Protection, Electronic Commerce, Data Breach, Cyber Regulation, Digital Law, Indonesia, GDPR
.

Identifier:
Zera Open
Page: 108-130
https://zeraopen.com/journal/jclis

The rapid expansion of digital technology has accelerated the growth of electronic commerce (e-commerce) in Indonesia, simultaneously generating significant risks of personal data breaches and misuse. According to the Indonesian Internet Service Providers Association (*Asosiasi Penyelenggara Jasa Internet Indonesia*/APJII), internet users in Indonesia reached 215.63 million in the 2022–2023 period, yet this growth has been accompanied by a surge in data breach incidents, including the leakage of 91 million Tokopedia user accounts (2020), 279 million BPJS Kesehatan participant records (2021), and data from Bukalapak and Bhinneka.com. This study aims to analyze the effectiveness of personal data protection regulations within the context of e-commerce transactions in Indonesia and to identify the urgency of comprehensive legal reform. Employing a normative-comparative method reinforced by a sociological approach, this research examines the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*/UU ITE) as amended, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions (*Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*/PP PSTE), and compares them with the European Union's General Data Protection Regulation (GDPR). The findings reveal that existing

*Corresponding author:
(Setya Eko Wasito)

regulations contain fundamental weaknesses: the absence of explicit data subject rights, disproportionate sanctions, and fragmented supervisory mechanisms. The urgency of enacting a standalone Personal Data Protection Law (*Undang-Undang Perlindungan Data Pribadi*/UU PDP) is paramount to ensuring legal certainty and providing genuine protection for millions of Indonesian digital consumers.

1. Introduction

Indonesia stands as one of the fastest-growing internet and e-commerce markets in Southeast Asia. According to the Indonesian Internet Service Providers Association (*Asosiasi Penyelenggara Jasa Internet Indonesia*/APJII), internet users in Indonesia reached 210.03 million in the 2021–2022 period, equivalent to 77.02 percent of the total national population, and further increased to 215.63 million or 78.19 percent of the population in the 2022–2023 period (APJII, 2022; APJII, 2023). This figure reflects a decade-long upward trend, from a penetration rate of 64.8 percent in 2018 to over 78 percent by 2023. This surge in connectivity corresponds directly with the dramatic growth of e-commerce transaction volumes, which Bank Indonesia reported at IDR 476.3 trillion in 2022, positioning Indonesia as the largest digital market in the region.

Behind this impressive growth lies a serious threat that often escapes public attention: the protection of consumers' personal data. Every e-commerce transaction requires users to surrender various sensitive data, including full names, addresses, phone numbers, and financial information. This data becomes a valuable commodity vulnerable to exploitation by irresponsible parties, whether through system breaches,

illegal data trading, or unauthorized consumer profiling. The rapid monetization of digital personal data has transformed data breaches from isolated technical incidents into a systematic threat to individual rights and national digital security.

A series of large-scale data breach incidents in Indonesia powerfully illustrates this threat. In March 2019, a hacker known as Gnosticplayers claimed to have stolen 13 million user accounts from the e-commerce platform Bukalapak and sold them for US$5,000 on the dark web (Databoks Katadata, 2020). In May 2020, the hacker group ShinyHunters exposed 91 million Tokopedia user records including names, email addresses, phone numbers, and dates of birth and offered them for sale at US$5,000 on the Raid Forums dark web marketplace; the same group subsequently claimed 1.2 million records from Bhinneka.com (CNN Indonesia, 2020; Kompas.com, 2020). The most alarming incident occurred in May 2021, when data purportedly belonging to 279 million Social Security Administration for Health (*Badan Penyelenggara Jaminan Sosial Kesehatan*/BPJS Kesehatan) participants including 20 million records containing personal photographs were found being sold on Raid Forums by an account named "Kotz," prompting investigations by the Ministry of Communication and Information Technology (*Kementerian Komunikasi dan Informatika*/Kominfo), the National Cyber and Encryption Agency (*Badan Siber dan Sandi Negara*/BSSN), and the National Police (Tempo.co, 2021; Kompas.com, 2021; CNN Indonesia, 2021). Ironically, not one of these cases resulted in criminal prosecution of the responsible parties, exposing the fundamental inadequacy of existing legal instruments.

This pattern of impunity reflects a fundamental gap between the reality of cyber threats and the availability of effective legal instruments for data protection. Indonesia has long lacked a comprehensive standalone law governing personal data protection. Existing provisions remain scattered across various sectoral regulations, including the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*/UU ITE) as amended by Law Number 19 of 2016, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions (*Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*/PP PSTE), and the Ministerial Regulation of the Ministry of Communication and Information Technology (*Peraturan Menteri Komunikasi dan Informatika*/Permenkominfo) Number 20 of 2016 on Personal Data Protection in Electronic Systems. As The Conversation Indonesia (2020) observed, the absence of comprehensive regulation means that data breach cases frequently end without resolution, and responsible parties face minimal legal consequences.

This regulatory fragmentation creates compounding practical problems: overlapping authority between supervisory institutions, ambiguous definitions of personal data, insufficient explicitly recognized data subject rights, and imbalance between business obligations and available sanctions are recurring grievances among stakeholders. The Draft Personal Data Protection Law (*Rancangan Undang-Undang Perlindungan Data Pribadi*/RUU PDP), submitted since 2016, was only enacted in September 2022 as the Personal Data Protection Law (*Undang-Undang Perlindungan Data Pribadi*/UU PDP), and remains in a two-year transitional implementation period. The six-year delay in enacting this legislation left Indonesian digital

consumers without adequate legal protection during one of the most consequential periods of data breach activity in the country's history.

This study advances two primary research questions. First (RQ1), how effective are the existing personal data protection regulations in providing protection for consumer data in e-commerce transactions in Indonesia? Second (RQ2), why is comprehensive legal reform and implementation of personal data protection regulations an urgent necessity within the Indonesian e-commerce ecosystem? These two questions serve as the analytical framework examining regulations from both normative and empirical perspectives. Theoretically, this study contributes to Indonesian cyber law literature by mapping structural weaknesses in the existing regulatory framework. Practically, the findings are intended to inform policymakers in accelerating the implementation of UU PDP, as well as to guide e-commerce industry players in building responsible data governance.

2. Methods

This study employs a multi-method approach integrating four principal methods in legal research, namely the normative, comparative, systematic, and sociological approaches, to produce a comprehensive analysis of the effectiveness of personal data protection regulations in the Indonesian e-commerce context.

First, the normative legal research approach serves as the primary foundation, examining legal norms embodied in various legislative instruments. Primary legal sources examined include: UU ITE as amended; Government Regulation Number 71 of 2019 (PP PSTE); Permenkominfo Number 20 of 2016 on Personal Data

Protection in Electronic Systems; Law Number 8 of 1999 on Consumer Protection (*Undang-Undang Perlindungan Konsumen*/UU PK); and UU PDP (Law Number 27 of 2022).

Second, the comparative approach is employed to compare Indonesia's personal data protection regulatory framework with the European Union's General Data Protection Regulation (GDPR), widely regarded as the most advanced and comprehensive data protection instrument in the world. The comparison encompasses the definition of personal data, data subject rights, data controller obligations, supervisory mechanisms, and the sanctions regime. This method assists in identifying systemic gaps and weaknesses in the domestic regulatory framework.

Third, the systematic approach is used to map the interconnectedness and coherence among existing regulations, identifying whether the applicable regulations form a harmonious unified legal system or instead produce overlaps and inconsistencies that generate legal uncertainty.

Fourth, the sociological jurisprudence approach is used to understand the practical effectiveness of law by analyzing secondary data comprising news reports, supervisory agency reports, documented data breach cases, and published empirical studies on the legal awareness and compliance of e-commerce businesses. Secondary sources include news media reports from CNN Indonesia, Tempo.co, Kompas.com, CNBC Indonesia, Katadata, and official publications from APJII and BSSN. Data analysis is conducted qualitatively using the descriptive-analytical technique.

3. Results

3.1. The Regulatory Framework for Personal Data Protection in Indonesian E-Commerce

Personal data protection in Indonesia has long rested upon a sectoral and fragmented regulatory framework. UU ITE, as the first cyber law instrument in Indonesia, contains provisions related to privacy and information confidentiality, particularly in Article 26, which regulates the distribution of electronic information concerning a person's personal data without that person's consent. However, the practical application of this provision has been demonstrably inadequate: despite high-profile breaches affecting hundreds of millions of Indonesians between 2019 and 2022, no e-commerce company has been criminally prosecuted under UU ITE for negligently failing to protect user data (The Conversation Indonesia, 2020).

Government Regulation Number 71 of 2019 (PP PSTE) attempted to fill this gap by imposing obligations on Electronic System Providers (*Penyelenggara Sistem Elektronik*/PSE) to protect users' personal data. Article 14 of PP PSTE requires PSE to maintain the confidentiality, integrity, and availability of personal data they manage. Article 15 requires PSE to ensure that collection, processing, and use of personal data is conducted on the basis of explicit consent. However, this regulation suffers from a critical structural weakness: it is self-regulatory in nature, relying entirely on the good faith of PSE without systematic state audit and verification mechanisms (Sinta Dewi, 2016). The Tokopedia, Bukalapak, and Bhinneka cases all of which involved PSE that had ostensibly adopted security standards demonstrate

that self-regulatory compliance is insufficient to prevent large-scale data breaches (Cyberthreat.id, 2020).

Permenkominfo Number 20 of 2016 is the most specific regulation governing personal data protection in electronic systems. This regulation defines personal data as "any data concerning a person who is individually identified and/or identifiable, either independently or in combination with other information, directly or indirectly through electronic and/or non-electronic systems." Although this definition is relatively broad, the regulation only binds electronic system providers and does not cover the full e-commerce ecosystem, which also involves logistics service providers, payment gateways, and digital marketing agents (Djafar, 2019). Moreover, the notification obligation under this regulation requiring data controllers to inform affected users of a breach within 14 days was conspicuously ignored in the Tokopedia and BPJS Kesehatan cases, with neither entity issuing a comprehensive breach notification to all affected users within the required timeframe (The Conversation Indonesia, 2020).

Comparative analysis with the GDPR reveals a significant structural gap. The GDPR, which entered into force in May 2018, establishes eight fundamental rights for data subjects: the right to be informed, the right of access, the right to rectification, the right to erasure or "right to be forgotten," the right to restriction of processing, the right to data portability, the right to object, and rights related to automated decision-making (Voigt & Von dem Bussche, 2017). Indonesian regulations prior to UU PDP only explicitly recognized the right of access and the right to correct data under Article 26(1) of Permenkominfo 20/2016. Furthermore,

while GDPR mandates data breach notification to supervisory authorities within 72 hours of awareness, no equivalent binding obligation existed in Indonesian law prior to UU PDP. This gap contributed directly to the delayed public disclosure of the Tokopedia breach which occurred on 20 March 2020 but only became public in early May 2020 and to the BPJS Kesehatan case, where the extent of the breach remained disputed for weeks (Dewi Rosadi & Gumelar Pratama, 2018; CNN Indonesia, 2020).

The sanctions regime further illustrates the regulatory deficit. Article 83 of UU ITE provides a maximum criminal sentence of eight years imprisonment and/or a fine of up to IDR 2 billion for data violations, yet this provision has never been enforced against a corporation for negligent data protection. By contrast, under the GDPR, breaches of the regulation's core provisions can attract fines of up to €20 million or 4 percent of global annual turnover. As Cyberthreat.id (2020) noted, if Tokopedia, Bukalapak, and Bhinneka had operated in Europe and suffered comparable breaches, they could have faced fines exceeding Rp 300 billion. The disparity between the potential harm to hundreds of millions of affected Indonesians and the absence of any meaningful corporate accountability underscores the inadequacy of the existing sanctions framework.

Law Number 27 of 2022, UU PDP, which was finally enacted after years of deliberation in the House of Representatives (*Dewan Perwakilan Rakyat*/DPR), represents a significant legislative breakthrough. UU PDP adopts various GDPR principles, recognizes nine data subject rights, establishes stricter obligations for data controllers and processors, and creates a supervisory mechanism under the coordination of Kominfo. However, UU PDP remains in a two-year transitional

period, and its effectiveness cannot yet be fully evaluated. The Indonesian government's delayed response to data breach incidents the Ministry PANRB publicly called for accelerated enactment of the personal data protection law only after the BPJS Kesehatan breach in 2021 (Kementerian PANRB, 2021) reflects the extent to which regulatory reform has historically lagged behind the pace of digital threats.

3.2. Regulatory Effectiveness in Practice: A Critical Analysis (RQ1)

In answering RQ1, this study finds that Indonesia's personal data protection legal framework has not been substantively effective. This ineffectiveness can be examined through three interconnected dimensions: the substance of law, the structure of law, and the culture of law, following Lawrence Friedman's framework of legal effectiveness.

From the dimension of legal substance, four fundamental weaknesses are identified. First, the absence of a single and consistent definition of "personal data" across legislative instruments leads to varied interpretations among businesses and law enforcement officers. Second, provisions on "valid consent" remain vague and susceptible to exploitation through lengthy standard clauses in e-commerce terms and conditions, which do not provide consumers with a genuinely free and informed choice. Third, available sanctions are disproportionate to potential harm: as noted above, Article 83 of UU ITE has never been enforced against a corporation for data negligence despite repeated large-scale breaches. Fourth, there is no obligation for businesses to appoint an independent Data Protection Officer (DPO) (Lesmana et al., 2021). Together, these weaknesses meant that when 91 million Tokopedia

accounts were exposed in 2020, affected users had no effective legal mechanism to compel the company to act or to claim compensation (CNN Indonesia, 2020; CNBC Indonesia, 2020).

From the dimension of legal structure, the central problem lies in institutional fragmentation. Oversight of data protection is dispersed across Kominfo, the Financial Services Authority (*Otoritas Jasa Keuangan*/OJK) for fintech and digital banking, the Food and Drug Supervisory Agency (*Badan Pengawas Obat dan Makanan*/BPOM) for health platforms, and the National Consumer Protection Agency (*Badan Perlindungan Konsumen Nasional*/BPKN). The BPJS Kesehatan breach in 2021 starkly exposed the consequences of this fragmentation: Kominfo, BSSN, and the National Police all conducted separate investigations, yet no coordinated accountability mechanism existed to determine which institution bore ultimate responsibility and impose sanctions. Civil society group Periksa Data subsequently announced a lawsuit against all three institutions for failing to protect citizens' data (Suara.com, 2021). This fragmentation differs fundamentally from the GDPR model, which requires each member state to establish an independent Supervisory Authority (Albrecht, 2016).

From the dimension of legal culture, BSSN reported over 1.65 billion cyber traffic anomalies in 2021 and approximately 976 million in 2022, with data leakage (*information leak*) ranking as the second most prevalent category of cyber attack at 14.75 percent in 2022, after malware (BSSN, 2022; BSSN, 2023; Antara News, 2023). Despite the scale of these threats, a low level of voluntary legal compliance persists among businesses. Based on published empirical studies, the majority of micro,

small, and medium enterprises (*Usaha Mikro, Kecil, dan Menengah*/UMKM) selling through marketplaces do not have adequate privacy policies and are unaware of their obligations as data controllers (Yuniarti, 2019). Even among large-scale e-commerce platforms — Tokopedia, Bukalapak, and Bhinneka had all adopted internationally recognized security standards such as SHA-384 hashing and ISO 27001 — these technical measures proved insufficient to prevent breaches, and corporate communication following the incidents was criticized for being evasive and delayed (Cyberthreat.id, 2020).

A comparative study of ASEAN member states' regulations further contextualizes Indonesia's position. Singapore has had a Personal Data Protection Act (PDPA) since 2012, subject to several substantive revisions; Thailand enacted its Personal Data Protection Act in 2019 and began enforcing sanctions fully in 2022; and Malaysia has operated under the Personal Data Protection Act 2010 for over a decade (Greenleaf, 2019). Indonesia's delayed enactment of a standalone data protection law — and the six-year gap between the tabling of RUU PDP in 2016 and its enactment as UU PDP in 2022 — created a prolonged period of legal uncertainty that left digital consumers exposed to some of the largest data breach incidents in the region's history.

Analysis using Friedman's three indicators of legal effectiveness reveals that Indonesian personal data protection regulations are weak across all three dimensions simultaneously: the substance is incomplete and inconsistent; the structure is fragmented and lacks a unified enforcement authority; and the culture is characterized by low compliance, delayed notification, and absence of meaningful

corporate accountability. These weaknesses are mutually reinforcing. The failure to impose sanctions following the Tokopedia breach in 2020 signaled to other businesses that the cost of non-compliance was negligible, further entrenching a culture of inadequate data governance.

3.3 The Urgency of Legal Reform and Implementation of Personal Data Protection Regulations (RQ2)

In answering RQ2, this study identifies five fundamental and interrelated arguments establishing why comprehensive personal data protection legal reform is a non-deferrable imperative.

First, the urgency of protecting citizens' constitutional rights. The Constitutional Court (*Mahkamah Konstitusi*/MK), in Decision Number 5/PUU-VIII/2010, affirmed that the right to privacy is part of the fundamental human rights guaranteed under Article 28G(1) of the 1945 Constitution (*Undang-Undang Dasar 1945*/UUD 1945). The serial data breach incidents of 2019–2022 represent concrete violations of this constitutional guarantee. The inability of Tokopedia, BPJS Kesehatan, and other data-holding institutions to protect the personal information entrusted to them and the state's failure to hold them accountable constitutes a failure by the Indonesian state to fulfill its constitutional obligation to protect the fundamental rights of its citizens in the digital sphere (MK, 2010; Kementerian PANRB, 2021).

Second, the urgency of economic stability and digital trust. The sustainable growth of the e-commerce ecosystem is fundamentally dependent on consumer trust. Surveys conducted by various research institutions indicate that concerns

about data security constitute one of the greatest barriers to consumer adoption of new digital services (Lim et al., 2022). The recurring data breach incidents have measurably damaged this trust: research shows that e-commerce platforms experiencing major data breaches face significant short-term declines in consumer confidence and transaction intent (Harahap et al., 2023). Legal uncertainty also acts as a barrier to foreign investment, as many institutional investors from EU member states require adequate data protection standards in partner countries known as adequacy decisions as a prerequisite for cross-border data transfers under the GDPR framework.

Third, the urgency of preventing data-driven cybercrime. The data leaked through e-commerce and public sector breaches does not simply disappear from circulation. BSSN data shows that between 2021 and 2022, Indonesia faced over 2.6 billion cumulative cyber threat anomalies (BSSN, 2022; BSSN, 2023). Leaked personal data fuels downstream cybercrimes including identity fraud, targeted phishing, social engineering, and financial scams. The 279 million BPJS Kesehatan records exposed in 2021 contained not only names and identification numbers but also health history data a particularly sensitive category that can be exploited for insurance fraud and other targeted crimes (Tempo.co, 2021). Effective regulation functions as a preventive mechanism by creating incentives for businesses and public institutions to invest in cybersecurity and sound data governance (Djafar, 2019).

Fourth, the urgency of alignment with international standards. In an era of cross-border digital commerce, Indonesia cannot operate in a regulatory vacuum. Various new-generation free trade agreements, including the Comprehensive and

Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP), contain provisions on cross-border data flows and personal data protection. Countries lacking adequate data protection standards risk facing barriers in digital trade and exclusion from the global data ecosystem (Dewi Rosadi & Gumelar Pratama, 2018). The reputational damage from large-scale breaches including international media coverage of the Tokopedia and BPJS cases further signals to foreign partners and investors that Indonesia's digital governance framework requires urgent strengthening.

Fifth, the momentum of UU PDP implementation. The enactment of Law Number 27 of 2022 represents a historic legislative milestone, achieved after six years of parliamentary deliberation that spanned multiple data breach crises. UU PDP adopts GDPR-aligned principles including nine enumerated data subject rights, mandatory breach notification, and the prospect of independent supervisory oversight. However, UU PDP requires implementing regulations and adequate institutional infrastructure to function effectively. The supervisory body mandated by UU PDP must be established promptly with clear authority, adequate resources, and independence from industry interference. Failure to build a solid implementation ecosystem will render UU PDP merely a "paper tiger" textually impressive yet practically ineffective as has been the fate of previous regulations. The calls for accelerated enactment of UU PDP from multiple government ministries following the BPJS breach (Kementerian PANRB, 2021) illustrate that policymakers themselves recognized the urgency of the reform; the challenge now lies in translating legislative intent into institutional reality.

The findings of this study are consistent with Solove's (2022) argument that the effectiveness of privacy regulation is determined not solely by the sophistication of its normative text but by the institutional design of its enforcement, the capacity of supervisory human resources, and the quality of the compliance culture among regulated entities. Indonesia must learn from the experience of GDPR implementation in Europe and the PDPA in Singapore, which demonstrate that a transitional period optimally utilized through education programs, technical guidance, and multi-stakeholder dialogue is highly determinative of the long-term effectiveness of a data protection regulation.

4. Conclusion

This study produces two principal conclusions that directly address the research questions advanced, drawing on both normative legal analysis and empirical evidence from documented data breach incidents.

With respect to RQ1, the personal data protection regulatory framework in force in Indonesia both prior to and during the transitional period of UU PDP has not been substantively effective. The recurrence of major data breaches, including the 13 million Bukalapak account breach (2019), the 91 million Tokopedia account breach (2020), the 1.2 million Bhinneka.com user record breach (2020), and the 279 million BPJS Kesehatan participant data breach (2021), none of which resulted in criminal prosecution or proportionate corporate accountability, constitutes the most compelling empirical evidence of this ineffectiveness. This ineffectiveness stems from three interrelated weaknesses: (1) substantive weaknesses comprising the

incompleteness and inconsistency of legal norms, the absence of a comprehensive catalog of data subject rights, and the disproportionality of the sanctions regime; (2) structural weaknesses comprising fragmentation among supervisory institutions as exposed by the uncoordinated response to the BPJS Kesehatan breach involving Kominfo, BSSN, and the National Police without a single fully empowered independent authority; and (3) cultural weaknesses comprising low legal awareness and compliance among businesses, particularly UMKM that dominate the national e-commerce ecosystem.

With respect to RQ2, the urgency of comprehensive reform and implementation of personal data protection regulations rests upon five mutually reinforcing pillars demonstrated by this study: the state's constitutional obligation to protect the right to privacy as a fundamental human right, as affirmed by the Constitutional Court; the economic necessity of rebuilding consumer digital trust that has been eroded by repeated high-profile breach incidents; the imperative of preventing increasingly sophisticated data-driven cybercrime, against the backdrop of over 2.6 billion cyber threat anomalies recorded by BSSN in 2021–2022; the obligation to align with international regulatory standards for Indonesia's full participation in the global digital trading ecosystem; and the need to seize the momentum of UU PDP's enactment after a six-year legislative journey to build a solid and effective implementation infrastructure before the transitional period expires.

Based on these conclusions, this study formulates four policy recommendations. First, the government and DPR must immediately accelerate the

establishment of an independent data protection supervisory body as mandated by UU PDP, with clear investigative authority, sanctions-imposition power, and adequate budgetary resources. Second, a nationwide education and socialization program specifically targeting UMKM e-commerce players is required, accompanied by practical and easily implementable technical guidance. Third, the complaint and dispute resolution mechanism for personal data protection must be designed to be easily accessible to consumers, including through digital channels and simplified out-of-court settlement procedures. Fourth, a regular and transparent evaluation of UU PDP implementation effectiveness should be conducted, involving civil society and academics as part of an external accountability mechanism, drawing lessons from the institutional failures documented in the pre-UU PDP era.

This study acknowledges limitations in its reliance on secondary data analysis. Future research employing surveys and in-depth interviews with e-commerce businesses, consumers, and law enforcement officers would provide a more complete picture of UU PDP implementation dynamics. Comparative studies with data protection regulations in similarly situated emerging digital economies, such as India and Brazil, could further enrich the policy recommendations.

References

Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review*, 2(3), 287–289. https://doi.org/10.21552/EDPL/2016/3/4

Antara News. (2023). BSSN ungkap serangan keamanan siber di 2022 turun dibanding 2021. *Antara News*. https://www.antaranews.com/berita/3356178/bssn-ungkap-serangan-keamanan-siber-di-2022-turun-dibanding-2021

Asosiasi Penyelenggara Jasa Internet Indonesia. (2022). *Laporan survei penetrasi internet Indonesia 2021–2022*. APJII. https://apjii.or.id/berita/d/apjii-di-indonesia-digital-outloook-2022_857

Asosiasi Penyelenggara Jasa Internet Indonesia. (2023). *Laporan survei penetrasi internet Indonesia 2022–2023*. APJII. https://survei.apjii.or.id/

Badan Siber dan Sandi Negara. (2022). *Laporan tahunan monitoring keamanan siber Indonesia 2021*. BSSN. https://www.bssn.go.id/monitoring-keamanan-siber-2022/

Badan Siber dan Sandi Negara. (2023). *Lanskap keamanan siber Indonesia tahun 2022*. BSSN. https://www.bssn.go.id/publikasi/

CNBC Indonesia. (2020). Cerita lengkap bocornya 91 juta data akun Tokopedia. *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia

CNN Indonesia. (2020). Kronologi lengkap 91 juta akun Tokopedia bocor dan dijual. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

CNN Indonesia. (2021). Kominfo telusuri 279 juta data bocor: Diduga kuat dari BPJS. *CNN Indonesia*.

https://www.cnnindonesia.com/teknologi/20210521115652-185-645201/kominfo-telusuri-279-juta-data-bocor-diduga-kuat-dari-bpjs

Cyberthreat.id. (2020). Kebocoran data pengguna Tokopedia, Bukalapak, dan Bhinneka: Siapa peduli? *Cyberthreat.id*. https://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli

Databoks Katadata. (2020). Bocornya puluhan juta data pengguna e-commerce Indonesia. *Katadata*. https://databoks.katadata.co.id/datapublish/2020/05/12/bocornya-puluhan-juta-data-pengguna-e-commerce-indonesia

Dewi, S. (2015). *Cyber law: Aspek data privasi menurut hukum internasional, regional, dan nasional*. Refika Aditama.

Dewi Rosadi, S., & Gumelar Pratama, G. (2018). Urgensi perlindungan data privasi dalam era ekonomi digital di Indonesia. *Veritas et Justitia*, 4(1), 88–110. https://journal.unpar.ac.id/index.php/veritas/article/view/2916

Djafar, W. (2019). *Hukum perlindungan data pribadi di Indonesia: Lanskap, urgensi dan kebutuhan pembaruan*. Makalah disampaikan dalam kuliah umum Program Pascasarjana Fakultas Hukum Universitas Gadjah Mada, Yogyakarta.

Djafar, W., Sumigar, B. R. F., & Setianti, B. L. (2016). *Perlindungan data pribadi: Usulan pelembagaan kebijakan dari perspektif hak asasi manusia*. Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Greenleaf, G. (2019). Global data privacy laws 2019: 132 national laws and many bills. *Privacy Laws & Business International Report*, 157, 14–18.

Harahap, W. F., Daulay, A. R. R., Alfisyahri, P. N., & Silalahi, P. R. (2023). Analisis citra marketplace PT Tokopedia dalam meningkatkan kepercayaan konsumen pasca kebocoran data pengguna. *CEMERLANG: Jurnal Manajemen dan Ekonomi Bisnis*, 3(1), 29–41.

Indonesian Constitutional Court. (2010). *Decision Number 5/PUU-VIII/2010 regarding judicial review of Law Number 11 of 2008 on Electronic Information and Transactions*. Constitutional Court of the Republic of Indonesia.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. (2021). Data BPJS Kesehatan diduga bocor, Menteri Tjahjo dukung Kemkominfo usut tuntas. *Kementerian PANRB*. https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas

Kompas.com. (2020). Hacker klaim punya data 1,2 juta pengguna Bhinneka.com. *Kompas.com*. https://tekno.kompas.com/read/2020/05/10/21120067/hacker-klaim-punya-data-12-juta-pengguna-bhinnekacom

Kompas.com. (2021). Dugaan kebocoran data 279 juta WNI, BPJS Kesehatan tempuh langkah hukum. *Kompas.com*. https://nasional.kompas.com/read/2021/05/25/11140881/dugaan-kebocoran-data-279-juta-wni-bpjs-kesehatan-tempuh-langkah-hukum

Lesmana, C. S. A. T., Elis, E., & Hamimah, S. (2021). Urgensi undang-undang perlindungan data pribadi dalam menjamin keamanan data pribadi sebagai

pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, 3(2), 1–7. https://doi.org/10.52005/rechten.v3i2.78

Lim, W. M., Kumar, S., & Ali, F. (2022). Advancing knowledge through literature reviews: What, why, and how to contribute. *The Service Industries Journal*, 42(7–8), 481–513. https://doi.org/10.1080/02642069.2022.2047941

Rosadi, S. D., Noviandika, A., Walters, R., & Rahadatul Aisy, F. (2022). Indonesia's Personal Data Protection Bill 2020: Does it meet the needs of the new digital economy? *International Review of Law, Computers & Technology*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198615

Sinta Dewi, R. (2016). Konsep perlindungan hukum atas privasi dan data pribadi dikaitkan dengan penggunaan cloud computing di Indonesia. *Yustisia*, 5(1), 22–30. https://doi.org/10.20961/yustisia.v5i1.8712

Solove, D. J. (2023). The limitations of privacy rights. *Notre Dame Law Review*, 98(3), 975–1042.

Suara.com. (2021). Kominfo dan BSSN akan turut digugat dalam kasus kebocoran data BPJS Kesehatan. *Suara.com*. https://www.suara.com/tekno/2021/06/17/191004/kominfo-dan-bssn-akan-turut-digugat-dalam-kasus-kebocoran-data-bpjs-kesehatan

Tempo.co. (2021). Data penduduk di BPJS Kesehatan bocor, bukti lemahnya perlindungan data pribadi. *Tempo.co*. https://www.tempo.co/arsip/data-penduduk-di-bpjs-kesehatan-bocor-bukti-lemahnya-perlindungan-data-pribadi-510693

The Conversation Indonesia. (2020). Tokopedia dan Bukalapak memang bisa digugat, tapi tidak lantas masalah kebocoran data tuntas. *The Conversation*. https://theconversation.com/tokopedia-dan-bukalapak-memang-bisa-digugat-tapi-tidak-lantas-masalah-kebocoran-data-tuntas-140193

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, 1(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030