EISSN: 2622-9668|PISSN: 2622-982X
Volume 9 Nomor 2 Agustus 2026: 469-499
DOI: 10.30996/jhbbc.v9i2.133568
Jurnal Hukum Bisnis Bonum Commune

Toothless Tiger? Evaluating the Effectiveness of Indonesia's Personal Data Protection Law in Ensuring Consumer Justice

Kusnan[1*], Bintoro Wardiyanto[2], Erna Setijaningrum[3], Ika Lestari[4]
[1,2,3]Universitas Airlangga, Indonesia
[4]Community of Research Laboratory, Indonesia
*Corresponding Author: kusnan-2022@fisip.unair.ac.id

Article History:
Submitted:
22-05-2026
Received:
12-06-2026
Accepted:
18-07-2026

Keywords:
cyberattacks; data breaches; consumer protection; strict liability

Abstract

The rising number of personal data breaches in Indonesia involves not only the public sector but also state-owned enterprises, financial institutions, and digital platforms. This condition reveals a systemic weakness in the architecture of national cyber law. Although Law No. 27/2022 has been enacted, its normative framework remains dominated by administrative compliance and has not yet adequately provided a civil liability regime, evidentiary rules, collective redress, or victim-oriented compensation. Meanwhile, Law No. 8/1999 has not been reconstructed to address data-driven markets, namely a condition in which personal data functions simultaneously as an economic asset and as a source of consumer vulnerability. This study analyzes the relationship between the two statutes through a normative matrix, compares them with remedial standards under the GDPR, and presents illustrative cases of data breaches in Indonesia, including those involving Tokopedia, Bukalapak, BPJS Kesehatan, KPU voter data, Bank Syariah Indonesia, and PDNS 2. The research method used is normative-doctrinal legal research employing statutory, conceptual, comparative, and illustrative case-analysis approaches to connect doctrinal examination with concrete enforcement patterns in Indonesia. The findings show that Indonesia requires an integrated model of digital consumer data protection: Law No. 27/2022 must operate as a lex specialis for data-processing obligations, while Law No. 8/1999 remains applicable to consumer safety, information duties, and damages. This article proposes the establishment of an Integrated Consumer Data Protection Code, a rebuttable presumption of liability for data controllers, clearer regulation of material and immaterial harm, mechanisms for class actions and small claims, mandatory security audits, and an independent personal data protection authority vested with investigative, corrective, and accountable enforcement powers.

1. Introduction

Indonesia is one of the countries targeted by cyberattacks. The 2022 Check Point Threat Intelligence Report, for example, ranked Indonesia first among Southeast Asian countries for the highest risk and vulnerability to cyberattacks, and fifth globally.[1] Furthermore, a report by the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) in August 2023 recorded Indonesia as ranking first globally in the number of cyberattacks, with 43.9 million attacks, followed by the United States with 4.23 million, Singapore with 1.79 million, Russia with 1.52 million, and the Netherlands with 1.43 million.[2]

[1]Dythia Novianty, "Peneliti: Indonesia Peringkat 5 Global Paling Berisiko Kena Serangan Siber," www.suara.com, 2022, https://www.suara.com/tekno/2022/12/01/143251/peneliti-indonesia-peringkat-5-global-paling-berisiko-kena-serangan-siber#.
[2]Susi Setiawati, "Tak Cuma Kemhan Pak Anies, Ini Daftar Instansi Yang Diserang Hacker," www.cnbcindonesia.com, 2024, https://www.cnbcindonesia.com/research/20240108091525-128-503641/tak-cuma-kemhan-pak-anies-ini-daftar-instansi-yang-diserang-hacker.

In more recent developments, Indonesia has also experienced a massive cyberattack regarded as an entry point into a national "cyber disaster," namely the 2024 ransomware attack.[3] That attack paralyzed the Temporary National Data Center (Pusat Data Nasional Sementara, PDNS) 2 in Surabaya, affected more than 200 government agencies,[4] and disrupted public services across multiple sectors of government.[5]

These cyberattacks correlate with the increasing number of personal data breaches. In Indonesia, personal data breach incidents show a significantly rising trend. In 2026, for example, reports emerged concerning an alleged breach of 58 million student records[6] and university student data from 13 higher education institutions.[7] In previous years, several other data breach cases also appeared, including the alleged leakage of 252 million permanent voter list records for the 2024 General Election,[8] the sale of 1.3 billion Telkomsel customer records in 2022,[9] the leakage of 13 million Bukalapak user records, and 90 million Tokopedia user records.[10]

This series of data breach incidents demonstrates the weakness of data protection governance in Indonesia. This condition is dangerous for data subjects because, amid the increasing frequency and scale of data breaches, there has been no visible pattern of effective legal consequences - administrative, civil, or criminal - capable of creating a deterrent effect against digital criminals or data controllers.[11] The absence of consistent legal consequences reinforces the assumption that Indonesia's data protection legal system remains symbolic and

---

[3]Yakub Pryatama Wijayaatmaja, "Kebocoran Data PDN Dianggap Pintu Bencana Nasional Keamanan Siber," mediaindonesia.com, 2024, https://mediaindonesia.com/politik-dan-hukum/681701/kebocoran-data-pdn-dianggap-pintu-bencana-nasional-keamanan-siber.

[4]Aisyah Amira Wakang, "Daftar Status Layanan Instansi Yang Terdampak Serangan Siber PDNS per 26 Juni," www.tempo.co, 2024, https://www.tempo.co/hukum/daftar-status-layanan-instansi-yang-terdampak-serangan-siber-pdns-per-26-juni-45170.

[5]Agus Bhakti et al., "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions : A Case Study in Indonesia," *Journal of Human Security* 20, no. 1 (2024): 109–17.

[6]Nicholas Ryan Aditya, "Pratikno: Tak Ada Indikasi Kebocoran 58 Juta Data Siswa, Tapi...," nasional.kompas.com, 2026, https://nasional.kompas.com/read/2026/02/10/12312261/pratikno-tak-ada-indikasi-kebocoran-58-juta-data-siswa-tapi.

[7]Intan Rakhmayanti Dewi, "Komdigi Jawab Isu Data 13 Universitas Di Indonesia Bocor," www.cnbcindonesia.com, 2026, https://www.cnbcindonesia.com/tech/20260123101312-37-704671/komdigi-jawab-isu-data-13-universitas-di-indonesia-bocor.

[8]Iqbal Basyari and Nikolaus Harbowo, "Nvestigasi Dugaan Kebocoran Data Pemilih Dituntut Transparan," www.kompas.id, 2023, https://www.kompas.id/artikel/investigasi-dugaan-kebocoran-data-pemilih-dituntut-transparan.

[9]Rully R. Ramli, "Soal Dugaan Kebocoran Data SIM Card, Telkomsel: Data Yang Tersimpan Dalam Sistem Internal Tetap Aman," money.kompas.com, 2022, https://money.kompas.com/read/2022/09/02/134500926/soal-dugaan-kebocoran-data-sim-card-telkomsel--data-yang-tersimpan-dalam.

[10]Achmad Firdaus, "Kasus Kebocoran Data Pribadi Di Indonesia: 10 Kejadian Terbesar Yang Perlu Diketahui," www.medcom.id, 2024, https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus-kebocoran-data-pribadi-di-indonesia-10-kejadian-terbesar-yang-perlu-diketahui.

[11]Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, and Muhammad Fadly Nasution, "Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana Di Indonesia," *Jurnal Minfo Polgan* 14, no. 2 (2025): 604–13.

rhetorical, rather than transformative and substantive. This condition is also affirmed by research findings showing that the Indonesian government has not yet been able to provide an optimal level of data protection to citizens because the legal and regulatory instruments required to establish an effectively binding legal framework and data protection standards are not yet available.[12]

Normatively, the state bears a constitutional obligation to protect the right to security and self-protection as guaranteed under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Personal data, as an extension of the identity and personal integrity of modern human beings, should be situated within the scope of that constitutional right. However, the implementation of that constitutional obligation has not been adequately reflected in the performance of positive law, particularly after the enactment of Law Number 27 of 2022 concerning Personal Data Protection (Law No. 27/2022). This statute regulates data-processing principles, obligations of data controllers, and the rights of data subjects. Article 20 of Law No. 27/2022, for example, requires data controllers to ensure the accuracy of personal data; Article 35 requires the implementation of data security measures; and Article 46 requires notification to data subjects in the event of a failure to protect personal data. Yet the structure of these obligations remains predominantly administrative and declaratory; it does not yet provide an adequate liability mechanism to address actual harm suffered by data subjects.[13]

The more fundamental problem in Law No. 27/2022 lies in the unclear legal liability regime. Article 64 indeed opens room for compensation claims, but it does not regulate the standard of proof, allocation of the burden of proof, compensation procedures, or punitive damages. The administrative sanctions under Article 57, which include written warnings, temporary suspension of data processing, and administrative fines, have not, in practice, formed an effective enforcement pattern. Without a strong civil-sanctions mechanism, data protection norms lose operational force and risk becoming an ethical framework without sufficient coercive power.[14] As a result, business actors and government agencies lack sufficient structural incentives to strengthen cybersecurity, because the cost of non-compliance may become cheaper than the cost of compliance.[15]

Further, Indonesian law remains trapped in a textual and institutional approach that overemphasizes fulfillment of formal obligations rather than a substantive protection regime placing victims at the center of legal protection. In the global context, however, data protection is an integral component of digital consumer rights.[16] Through the General Data Protection

[12]Muhamad Adri Rinjani and Ricky Firmansyah, "Hambatan Implementasi UU 27 / 2022 Dan Strategi Penguatan Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 8, no. 1 (2025): 70–83.
[13]Musrika Yanti, "Analisis Tanggung Jawab Perdata Dalam Kebocoran Data: Sinkronisasi UU Perlindungan Data Pribadi Dan KUH Perdata," *Jurnal Ilmu Sosial Dan Humaniora* 1, no. 4 (2025): 1539–1549.
[14]Giulia Gentile and Orla Lynskey, "Deficient by Design? The Transnational Enforcement of the GDPR," *International & Comparative Law Quarterly* 71, no. October (2022): 799–830, https://doi.org/10.1017/S0020589322000355.
[15]Mona Naomi Lintvedt, "Putting a Price on Data Protection Infringement," *International Data Privacy Law* 12, no. 1 (2022): 1–15.
[16]Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015).

Regulation (GDPR), the European Union treats personal data simultaneously as an economic asset and a fundamental right protected through stringent obligations, such as breach notification within 72 hours, the obligation to conduct data protection impact assessments, and administrative fines that may reach 4% of a company's global turnover. This shows that the GDPR was designed to impose strong legal compliance through a combination of preventive duties, institutional accountability, and economically deterrent sanctions.[17] By contrast, Law No. 27/2022 demonstrates that personal data protection in Indonesia remains far below these international standards.

The normative gap becomes even more evident when Law No. 27/2022 is read together with Law Number 8 of 1999 concerning Consumer Protection (Law No. 8/1999). Law No. 8/1999 guarantees consumers the right to comfort, security, and safety in consuming goods and/or services, as affirmed in Article 4, letter a. However, Law No. 8/1999 has not anticipated the phenomenon of data-driven markets, namely, circumstances in which personal data becomes a primary commodity in digital economic activity. There is no explicit provision that places personal data as an object of consumer protection. Yet Article 7 requires business actors to provide accurate, clear, and honest information and to be responsible for consumer losses. In the digital economy, that obligation logically includes the security of information systems used by business actors.[18] Nevertheless, because no norm directly connects personal data with the elements of "goods" or "services" that must be protected, a legal vacuum arises concerning the liability of business actors when a data breach occurs.[19]

The two statutes, in fact, regulate overlapping fields, but they do not refer to one another, thereby producing fragmentation within the legal system. Law No. 27/2022 does not expressly position itself as a *lex specialis* to Law No. 8/1999, while Law No. 8/1999 has not been amended to include digital consumer rights. Consequently, victims of data breaches face legal uncertainty: whether they must file claims under Law No. 8/1999, pursue tort claims under the Indonesian Civil Code, or use the administrative mechanisms under Law No. 27/2022. This fragmentation creates jurisdictional confusion and obscures the function of law as an instrument of social engineering. In the context of massive data breaches, the available mechanisms have not been able to provide swift and proportionate justice. The state appears to have failed in its role as both regulator and protector, leaving legal protection at the level of formal narrative with minimal effectiveness.[20]

This condition reveals disharmony between Law No. 27/2022 and Law No. 8/1999, which ultimately weakens the ability of Indonesia's legal system to ensure accountability among business actors and public bodies. Law No. 27/2022 emphasizes the obligations of data controllers but does not comprehensively elaborate on compensation mechanisms.

---

[17]Paul de Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation : Still a Sound System for the Protection of Individuals ?," *Computer Law & Security Review: The International Journal of Technology Law and Practice* 32, no. 2 (2016): 179–94, https://doi.org/10.1016/j.clsr.2016.02.006.
[18]Daniel J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126, no. 7 (2013): 1880–1903.
[19]Sinta Dewi Rosadi and Pratama Garry Gumelar, "Urgensi Perlindungan Data Privasidalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (2018): 88–110, https://doi.org/10.25123/vej.2916.
[20]Lynskey, *The Foundations of EU Data Protection Law*.

Meanwhile, Law No. 8/1999 provides the basis for consumer protection but does not define data as an object of protection. Accordingly, the absence of a concept of data as a consumer asset prevents data protection law from being strongly rooted in the principle of concrete consumer redress. A remedial legal *vacuum* emerges and, in turn, weakens the legal position of consumers as injured parties.

The disharmony between Law No. 27/2022 and Law No. 8/1999 also demonstrates the absence of a comprehensive legal protection framework in an era of predictive and data-driven economies. The ideal legal protection model should integrate data protection, consumer protection, and cybersecurity principles in a unified manner. Data protection is insufficient if it merely regulates formal rights and obligations; it must guarantee effective redress, establish measurable security standards, impose deterrent sanctions, and provide collective litigation mechanisms for victims. Without a paradigm shift toward consumer-centered data protection, the objective of Law No. 27/2022 to protect personal data will not be substantively achieved.

Therefore, this research remains important despite the existence of many related studies. Oktaria Wim Kusuma and Abraham Ferry Rosando's study, titled "*Urgensi Perlindungan Hukum Terhadap Data Pribadi Peminjam dalam Layanan Aplikasi Pinjaman Online*," discusses the protection of consumer personal data in online lending services and the liability of business actors for misuse of personal data; the findings show that the protection of personal data of online lending users is regulated under POJK No. 77/POJK.01/2016, and victims may file tort claims under Article 1365 of the Indonesian Civil Code to obtain damages.[21] Wilma Laura Sahetapy's study, titled "*Perlindungan Data Pribadi Anak dalam E-Commerce di Masa Pandemi Covid-19*," highlights the protection of children's personal data in the use of digital technology during the Covid-19 pandemic. Its findings show that the increasing use of social media, online games, and e-commerce makes children's personal data vulnerable to misuse, thereby requiring stronger legal protection and supervision.[22] Muhammad Yustino Aribawa's study, titled "Legal Certainty of Home Industry Food Through the National Agency of Drug and Food Control's Post-Market Oversight in Light of Law Number 8 of 1999 on Consumer Protection," discusses the legal certainty of consumer protection for home-industry food products through post-market oversight by the National Agency of Drug and Food Control (BPOM). The findings show that BPOM's administrative supervision through BPOM Regulation Number 22 of 2018 and BPOM Regulation Number 9 of 2020 provides legal protection and legal certainty for consumers against hazardous food products.[23]

Prior studies share similarities with this research, particularly because they examine consumer legal protection, business actors' liability, and the role of the state in guaranteeing public safety in modern economic activity. They also show that technological development and the digital economy create new challenges for the effectiveness of legal protection in

[21]Oktaria Wim Kusuma and Abraham Ferry Rosando, "Urgensi Perlindungan Hukum Terhadap Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online," *Jurnal Hukum Bisnis Bonum Commune* 5, no. 1 (2022): 123–41.
[22]Wilma Laura Sahetapy, "Perlindungan Data Pribadi Anak Dalam E-Commerce Di Masa Pandemi Covid-19," *Jurnal Hukum Bisnis Bonum Commune* 4, no. 2 (2021): 214–25.
[23]Muhammad Yustino Aribawa, "Legal Certainty of Home Industry Food Through National Agency of Drug And Food Control's Post Market In View From Law No. 8 of 1999 Concerning Consumer Protection," *Jurnal Hukum Bisnis Bonum Commune* 6, no. 1 (2023): 21–29.

Indonesia. Nevertheless, this research differs because it starts from the need to critically and comprehensively examine the inconsistency between Law No. 27/2022 and Law No. 8/1999 and its implications for legal gaps in the enforcement of personal data protection, particularly for consumers in the digital ecosystem. This research aims to formulate an ideal model of legal protection to address these challenges by relying on constitutional principles, global developments, and domestic needs to establish modern, effective, and victim-redress-oriented data protection law.

2. Methods

A normative-doctrinal legal approach is the research method used to examine legal norms, principles, and doctrines relevant to personal data protection law and consumer protection law. The normative approach is used to identify legal rules, legal principles, and legal doctrines in order to answer the legal issues under review.[24] In addition, the statutory approach is necessary to analyze all regulations related to the research issue.[25] Therefore, this study uses legislation to systematically interpret the provisions of Law No. 27/2022 and Law No. 8/1999, including the hierarchical relationship and normative disharmony between the two.

Next, the conceptual approach is used to examine theoretical constructions concerning the right to personal data, liability regimes, and the concept of data-driven consumer protection within a legal framework. The conceptual approach is necessary to understand the concepts, principles, and legal doctrines developed in legal scholarship as the basis for forming legal arguments.[26] The comparative approach is also used to compare Indonesia's data protection model with international legal frameworks, especially the European Union's GDPR. This comparison is important to identify substantive parameters for effective protection standards. Identifying similarities and differences between legal systems is intended to encourage legal reform and improvement in Indonesia.[27] The entire analysis is conducted qualitatively through doctrinal interpretation and systematic legal argumentation.

To ensure that the analysis in this study does not stop at the abstract level, several empirical-illustrative cases are used. The selected cases are Tokopedia, Bukalapak, *Badan Penyelenggara Jaminan Sosial* (BPJS) Kesehatan, voter data of the General Elections Commission (*Komisi Pemilihan Umum*, KPU), Bank Syariah Indonesia (BSI), and PDNS 2. These cases are not treated as statistical samples, but as doctrinal stress tests to assess whether Indonesia's existing regulatory architecture is able to identify the principal authority, establish liability, guarantee notification, and provide compensation or collective redress. This method is relevant for normative legal research because the quality of a legal regime is measured not only by its textual formulation, but also by its institutional capacity to operate coherently when applied to concrete disputes.[28]

---

[24]Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Prenada Media, 2017).
[25]Johnny Ibrahim, *Teori Dan Metodologi Penelitian Hukum Normatif* (Bayumedia Publishing, 2006).
[26]Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Raja Grafindo Persada, 2010).
[27]Zainuddin Ali, *Metode Penelitian Hukum* (Sinar Grafika, 2021).
[28]Neil MacCormick, *Rhetoric and the Rule of Law: A Theory of Legal Reasoning* (Oxford University Press, 2005).

3. Results and Discussion

3.1. Legal Framework: The Structure of Law No. 27/2022 and Law No. 8/1999

The legal framework governing personal data protection and the legal relationship between business actors and consumers in Indonesia's digital economy is fundamentally anchored in two principal statutes: Law No. 27/2022 and Law No. 8/1999. Although these two laws were born in different regulatory eras and paradigms, functionally they have a significant jurisdictional overlap, particularly in protecting citizens' constitutional rights to privacy under Article 28G of the 1945 Constitution, the right to security, and the right to legal certainty. Law No. 27/2022 regulates the legal relationship among data controllers, data processors, and data subjects, whereas Law No. 8/1999 regulates the legal relationship between business actors and consumers as defined in Article 1 number 2 of Law No. 8/1999, namely every person who uses goods and/or services available in society, whether for the benefit of themselves, their family, other persons, or other living creatures, and not for trade.

Doctrinally, the relationship between Law No. 27/2022 and Law No. 8/1999 cannot be explained simply as the absolute application of the *principle lex specialis derogat legi generali*. The *lex specialis* principle may displace a general norm only when at least three cumulative conditions are satisfied,[29] first, both norms regulate the same legal subject matter and legal relationship; second, there is an actual incompatibility that makes both norms incapable of being applied simultaneously;[30] and third, the special norm regulates the matter with sufficient completeness so that the general norm is no longer needed for that particular issue.[31] In this context, those three conditions are only partially met. Law No. 27/2022 is indeed special with respect to data-processing principles, lawful bases for processing, controllers' obligations, notification of protection failures, and supervisory compliance. However, Law No. 27/2022 is not yet complete in relation to consumer safety, digital services based on standard-form clauses, compensation procedures, evidentiary presumptions, or collective redress for consumers harmed by data breaches.

Accordingly, the problem identified in this article is not always a pure conflict of norms in the strict sense, but rather a combination of overlapping regulation, incomplete remedies, and institutional uncertainty. Law No. 27/2022 and Law No. 8/1999 can still be applied simultaneously within a model of layered regulation: Law No. 27/2022 governs data-processing obligations and supervisory compliance, while the Consumer Protection Law remains relevant to consumers' rights to security, accurate information, and compensation for unsafe or defective digital services. Therefore, Law No. 27/2022 fails to function as a complete *lex specialis* because it does not expressly determine whether a personal data breach by a digital service provider automatically constitutes a violation of consumer rights, how the burden of proof must be allocated, and which procedural route should be prioritized when millions of consumers experience similar privacy and economic risks.

---

[29]Bryan A. Garner and Antonin Scalia, *Reading Law: The Interpretation of Legal Texts* (West Group, 2011).
[30]Joost Pauwelyn, *Conflict of Norms in Public International Law: How WTO Law Relates to Other Rules of International Law* (Cambridge University Press, 2009).
[31]Sir Ian McTaggart Sinclair, *The Vienna Convention on the Law of Treaties* (Manchester University Press, 1984).

Table 1. Matrix of Law No. 27/2022 and Law No. 8/1999 in Digital Consumer Data Protection

Issue	Law No. 27/2022	Law No. 8/1999	Implication
Protected subject	Personal data subjects whose personal data is processed by controllers/processors.	Consumers who use goods and/or services, including digital services.	These subjects often overlap in digital markets, but the two laws use different legal categories.
Protected object	Personal data and the legality, proportionality, accuracy, security, and accountability of processing.	Safety, security, comfort, information, and compensation in the consumption of goods/services.	Personal data has not been expressly qualified as a consumer asset, thereby creating a remedial gap.
Main obligations	Controllers' obligations: lawful basis for processing, data security, prevention of protection failures, notification, and compliance.	Business actors' obligations: accurate information, good faith, safety standards, and compensation for consumer losses.	Dual obligations may operate simultaneously; the Personal Data Protection Law does not fully override consumer protection obligations.
Logic of liability	Dominated by administrative mechanisms and a fault-oriented approach; no explicit strict liability or reversal of the burden of proof for data breach victims.	Regulates compensation for consumer losses and product/service liability, but was not designed for data-based harm.	The emerging gap is remedial, not merely a conflict of norms: victims lack a clear route for proof and compensation.
Institutional route	PDP supervisory authority and courts; institutional independence and procedures remain insufficiently developed.	BPSK, courts, and consumer institutions; they lack specialized PDP expertise.	Jurisdictional overlap requires coordination or an integrated code, not the automatic exclusion of one regime by another.

Source: Primary data, 2026

Law No. 27/2022 normatively establishes a personal data protection structure oriented toward data-processing principles. Article 3 of Law No. 27/2022 sets out fundamental principles, including the lawfulness of processing purposes, processing limitation, data accuracy, security, and the accountability of data controllers. Article 20 of Law No. 27/2022 regulates the basic obligations of data controllers, including obtaining explicit consent from data subjects, conducting processing in a limited and proportionate manner, ensuring data security, and preventing failures of personal data protection. Article 20 letter c even requires

data controllers to protect and ensure the security of personal data being processed, a norm that substantively indicates the existence of a duty of care that should be strict.

However, the fundamental weakness of Law No. 27/2022 lies in the construction of its liability regime. Law No. 27/2022 does not explicitly establish strict liability for data breaches. Article 46 states that a data controller must provide written notification to data subjects in the event of a failure to protect personal data, but it does not provide that such failure automatically becomes a basis for absolute liability. In other words, the liability framework under Law No. 27/2022 still tends to be fault-based and requires proof of negligence or fault by the data controller; consequently, the burden of proof often falls on data subjects who do not have equal economic, technological, or informational capacity to prove a breach of data security obligations.[32] The absence of a strict liability norm impedes legal effectiveness because data breaches are inherent risks that may occur without any direct involvement by data subjects.[33] In consumer protection, strict liability has become a common standard for various high-risk products and services, whereas Law No. 27/2022 has not yet applied it in the digital context.

The proposition that Law No. 27/2022 has not adopted a modern data protection remedial model must be evaluated through concrete benchmarks, not by treating the GDPR merely as a symbol of modernity. The GDPR is relevant because it integrates preventive obligations, independent supervision, individual rights, administrative fines, and civil compensation into a single remedial architecture. The difference between the GDPR and Law No. 27/2022 directly affects access to justice. When victims lack forensic information concerning the cause of a breach, do not know the value of their immaterial harm, and have no representative mechanism to consolidate mass claims, the right to compensation becomes merely declaratory. The following comparison shows that the principal weakness of Law No. 27/2022 lies not only in the substance of its norms, but also in the absence of procedural bridges that enable victims to transform normative rights into effective remedies.

Table 2. Comparative Remedial Matrix: GDPR and Law No. 27/2022

Remedial mechanism	GDPR benchmark	Law No. 27/2022	Consequence for access to justice
Breach notification	Article 33 requires notification to the supervisory authority within 72 hours unless the breach is unlikely to result in risk; Article 34 requires notification to data subjects in high-risk cases.	Article 46 requires notification to data subjects and the authority, but the operational standards remain insufficiently detailed and depend on implementing regulations.	Late or vague notification impedes victims' ability to mitigate identity theft, fraud, or misuse.

[32]Brendan Van Alsenoy, "Liability under EU Data Protection Law From Directive 95/46 to the General Data Protection Regulation," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2, no. d (2016): 271–88.

[33]Radoslaw Strugala, "Art. 82 GDPR: Strict Liability or Liability Based on Fault?," *European Journal of Privacy Law & Technologies*, 2020, 71–79.

Remedial mechanism	GDPR benchmark	Law No. 27/2022	Consequence for access to justice
Compensation	Article 82 expressly covers material and non-material damage.	The right to compensation has been recognized, but statutory guidance on immaterial harm, causation, and valuation remains very thin.	Privacy harm may be viewed as speculative, making claims unattractive or difficult to win.
Representative/collective actions	Article 80 allows data subjects to mandate qualified nonprofit bodies to exercise rights and seek remedies.	No specific PDP representative action mechanism is available.	Victims of mass breaches must rely on general civil procedure or consumer mechanisms not designed for data harm.
Administrative fines	Article 83 requires fines that are effective, proportionate, and dissuasive, including turnover-based ceilings.	Administrative fines are recognized, but their calculation formula, publication practice, and relationship to victim compensation have not been clearly institutionalized.	Weak deterrence reduces incentives for prevention and audit readiness.
Independent supervision	Articles 51-52 require independent supervisory authorities.	The authority is placed under the President and its institutional design remains incomplete.	Enforcement against public bodies or politically sensitive entities may face actual or perceived conflicts of interest.

Source: Primary data, 2026

Conversely, Law No. 8/1999, as the older statute, provides a general framework for consumer protection that emphasizes the right to security, comfort, and safety under Article 4 letter a of Law No. 8/1999, namely the consumer's right to comfort, security, and safety in consuming goods and/or services. This provision materially also encompasses the right to personal data security, because data forms part of the services used by consumers in electronic transactions. Although Law No. 8/1999 does not use the term "personal data," Article 4 letter h grants consumers the right to obtain compensation and/or damages if the goods or services received do not conform to the agreement or cause loss. On the obligation side, Article 7 letter

b requires business actors to provide accurate, clear, and honest information concerning the condition and guarantee of goods and/or services, including instructions for use, repair, and maintenance, which teleologically should also include information regarding the management of personal data. Furthermore, Article 8 prohibits business actors from trading goods or services that fail to meet safety standards, which from a teleological perspective may be extended to include the obligation to maintain consumer data security.

Nevertheless, Law No. 8/1999 also contains a fundamental weakness because it does not regulate digital consumer rights that are highly important in modern electronic transactions.[34] Law No. 8/1999 was enacted in the pre-digital era and thus did not anticipate data-driven business models, including profiling, tracking, microtargeting, and algorithmic processing. Law No. 8/1999 also does not recognize the concept of a data fiduciary duty, namely the fiduciary obligation of business actors to process data with a higher standard of care akin to fiduciary relationships in civil law. The absence of such a norm places digital business actors in a dominant position without an adequate duty of care over consumer data, thereby creating a serious information asymmetry.[35]

Conceptually, the two statutes have an important point of convergence: personal data protection is an inherent part of digital consumer protection. This means that business actors processing consumer data in fact bear dual obligations: obligations as data controllers under Law No. 27/2022 and obligations as business actors under Law No. 8/1999. However, the two laws do not expressly refer to each other. Law No. 27/2022 does not mention Law No. 8/1999 as a normative reference, and conversely, Law No. 8/1999 has not been amended to include data protection as a special category of consumer rights. This condition creates interpretive ambiguity in practice, for example, whether a data protection violation automatically constitutes a consumer rights violation, or whether compensation mechanisms must follow general civil law, consumer dispute-resolution mechanisms, or administrative law under Law No. 27/2022.

This normative tension becomes more complex because there is no special procedural law for resolving data breach disputes. There are no provisions on the burden of proof, digital evidence, presumptions of violation, or digital forensic standards. Consequently, although Article 12 of Law No. 27/2022 grants data subjects the right to assert their rights, the remedial mechanisms available in practice remain inefficient, time-consuming, and place consumers in a weak position. In mass data breach cases, such as those in banking, health care, or e-commerce, there is no uniform dispute-resolution mechanism; some business actors choose private settlement, some use administrative channels, and others provide no adequate response.

Fragmentation also occurs at the institutional level. Law No. 27/2022 indeed regulates the establishment of a personal data protection authority as a supervisory body. Before Law No. 27/2022 entered into force, however, data protection jurisdiction was dispersed among several institutions, such as BSSN, which handles cybersecurity; the Ministry of

[34] Shoshana Zuboff, "The Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75–89, https://doi.org/10.1057/jit.2015.5.
[35]Jack M. Balkin, "Information Fiduciaries and the First Amendment," *U.C. Davis Law Review* 49, no. 4 (2016): 1183.

Communication and Informatics, now named the Ministry of Communication and Digital Affairs, which supervises electronic system operators; the Financial Services Authority, which supervises financial data; the National Agency of Drug and Food Control, which oversees health-related data concerning drugs and food; and the Indonesian Consumers Foundation, which operates in the field of consumer protection. Overlapping authority creates regulatory uncertainty, including in determining which institution is authorized to receive complaints, conduct investigations, or issue sanction recommendations. Jurisdictional fragmentation weakens the single-authority principle that constitutes the foundation of modern data protection supervision in many countries.

In the context of personal data protection, the urgency of harmonizing Law No. 27/2022 and Law No. 8/1999 is not merely a technical regulatory issue, but a constitutional necessity to guarantee equal protection of privacy rights and consumer rights. First, consumer personal data is, in principle, part of the right to data security,[36] and therefore must be protected not only as an object of information control, but also as part of consumer protection rights.[37] Second, the legal liability framework must be aligned with the development of the digital economy, which requires strict liability or at least a presumption of liability in data breach cases that cause consumer harm.[38] Third, harmonization must include the integration of procedural law systems that provide more effective access to justice for digital consumers.[39] Fourth, a single technical authority with exclusive jurisdiction over consumer personal data protection is needed so that fragmentation no longer potentially obstructs legal certainty.[40]

Accordingly, the legal analysis of Law No. 27/2022 and Law No. 8/1999 shows that although both share the same objective - protecting citizens' fundamental interests in the digital sphere - they have not yet formed a coherent regulatory framework. Law No. 27/2022 is overly technocratic and administrative, while Law No. 8/1999 is too general and insufficiently responsive to digital data issues. Ultimately, without a clear and directed normative reconstruction, Indonesian digital consumers remain vulnerable when confronting data-processing practices by business actors, and the state has not fully fulfilled its constitutional mandate to protect privacy and consumer rights effectively.

3.2. Data Breaches as Structural Negligence and Regulatory Ineffectiveness

The phenomenon of massive personal data breaches in Indonesia in recent years demonstrates the state's structural failure to guarantee citizens' constitutional rights to privacy

[36]Ratna Januarita, Indra Fajar Alamsyah, and Arif Perdana, "Guardians of Data: TruMe Life's Continuous Quest for Data Protection," *Journal of Information Technology Teaching Cases* 15, no. 2 (2025): 254–64, https://doi.org/10.1177/20438869241242141.

[37]Adis Nur Hayati, "The Issue of Dark Patterns in Digital Platforms: The Challenge for Indonesia's Consumer Protection Law," *Asian Journal of Law and Society* 11, no. 4 (2024): 453–465.

[38]Rafael de Freitas Valle Dresch and José Luiz de Moura Faleiro Júnior, "Special Strict Civil Liability in Brazil's General Data Protection Law," *Brazilian Journal of Law, Technology and Innovation* 2, no. 2 (2024): 98–128, https://doi.org/10.59224/bjlti.v2i2.98-128.

[39]Yosia Hetharie et al., "Hybrid Model of Personal Data Protection for Consumers in Digital MSMEs: A Comparative Study of Indonesian and Chinese Regulations," *Journal of Law and Legal Reform* 6, no. 4 (2025): 2015–2058.

[40]Inggret Adu, "Personal Data Protection in E-Commerce Platforms : Legal Challenges , Regulatory Frameworks , and the Path toward Digital Consumer Trust," *Priviet Social Sciences Journal* 6, no. 5 (2026): 118–128.

and security as affirmed in Article 28G paragraph (1) of the 1945 Constitution, namely the right of every person to protection of themselves, their family, honor, dignity, and property under their control, as well as the right to security and protection from threats of fear in exercising or refraining from exercising a human right. Thus, personal data, as an integral part of individual identity, dignity, and integrity, should be treated as a fundamental right, not merely as an administrative object.[41] Therefore, when a data breach occurs because of the negligence of a data controller, whether a private entity or public body, the state not only fails to protect the rights of data subjects, but also fails to fulfill its constitutional obligation as constructed under the principle of human rights due diligence in the digital sphere.[42] The state's obligation does not end with the enactment of regulations; it includes the duty to ensure that those regulations are effective, enforceable, and capable of providing substantive redress to victims.[43]

This weakness becomes clearer when major data breach incidents in Indonesia are read as institutional stress tests. The Tokopedia incident involved reports of approximately 91 million compromised user accounts and prompted Kominfo to request an internal investigation.[44] The Bukalapak incident involved approximately 13 million unique accounts exposed from backup data.[45] The BPJS Kesehatan case involved an alleged 279 million citizen records and triggered coordination among BPJS Kesehatan, Kominfo, BSSN, and law enforcement authorities.[46] The KPU case involved the alleged sale of voter data and generated public statements from KPU as well as BSSN involvement in digital forensic examination.[47] The 2023 Bank Syariah Indonesia incident showed a similar fragmentation in the financial sector: OJK emphasized restoration of banking operations and cyber-resilience governance, while public reporting on the alleged LockBit claim raised separate questions concerning

[41]Gianclaudio Malgieri and Jędrzej Niklas, "Vulnerable Data Subjects," *Computer Law and Security Review* 37, no. 788039 (2020): 1–16, https://doi.org/10.1016/j.clsr.2020.105415.
[42]Alessandro Mantelero, *Beyond Data. In Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (TMC Asser Press, 2020).
[43]Orla Lynskey, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy," *Theoretical Inquiries in Law* 20, no. 1 (2019): 189–220, https://doi.org/10.1515/til-2019-0007.
[44]Kementerian Komunikasi dan Informatika, "Siaran Pers No. 63/HM/KOMINFO/05/2020 tentang Demi Melindungi Data Pengguna, Kominfo Minta Tokopedia Lakukan Investigasi Internal," www.komdigi.go.id, 2020, https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-63-hm-kominfo-05-2020-tentang-demi-melindungi-data-pengguna-kominfo-minta-tokopedia-lakukan-investigasi-internal.
[45]Intan Rakhmayanti Dewi, "13 Juta Data Milik Bukalapak Diduga Dijual di Dark Web," www.tekno.sindonews.com, 2020, https://tekno.sindonews.com/read/19589/207/13-juta-data-milik-bukalapak-diduga-dijual-di-dark-web-1588770317.
[46]Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, "Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kemkominfo Usut Tuntas," www.menpan.go.id, 2021, https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas.
[47]Komisi Pemilihan Umum, "Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU," www.kpu.go.id, 2023, https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu.

customer notification, privacy harm, and compensation.[48] The PDNS 2 ransomware incident then shifted the issue from corporate data governance to national digital infrastructure because the attack disrupted digital public services and forced cross-agency recovery coordination.[49] These incidents arose from diverse sectors - private e-commerce, public health insurance, electoral administration, banking, and national digital infrastructure - yet all display the same enforcement pattern: public clarification and inter-agency coordination are visible, while deterrent sanctions, forensic transparency, compensation formulas, and collective redress channels remain unclear.

Table 3. Data Breach Cases in Indonesia and Their Remedial Gaps

Case	Reported scale/sector	Institutional response	Remedial gap
Tokopedia (2020)	E-commerce; approximately 91 million user accounts reportedly affected.	Kominfo requested Tokopedia to conduct an internal investigation and coordinate with relevant agencies.	The response focused on investigation and platform assurances; no predictable compensation or group redress route emerged.
Bukalapak (2020)	E-commerce; approximately 13 million unique accounts exposed from old backups according to Have I Been Pwned and media reports.	Company statements emphasized the absence of a new breach and the strengthening of security measures.	Consumer recovery depended on individual action and platform mitigation, not a statutory procedure for mass harm.
BPJS Kesehatan (2021)	Public health insurance; alleged 279 million citizen records.	Coordination was reported among BPJS, Kominfo, BSSN, and law enforcement authorities.	Health-data risk was primarily treated as an investigative/cybercrime issue; victim notification and compensation remained unclear.
KPU voter data (2023)	Electoral administration; alleged sale of voter data.	KPU issued a public statement; Kominfo and BSSN were involved in follow-up and forensic examination.	No independent PDP adjudication or uniform remedial route for voters was available.

[48]Otoritas Jasa Keuangan, "Press Release: Bank Syariah Indonesia Operates Back to Normal, Public Can Rest Assured," ojk.go.id, 2023, https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/Bank-Syariah-Indonesia-Operates-Back-To-Normal%2C-Public-Can-Rest-Assured.aspx?.

[49]Kementerian Komunikasi dan Informatika, "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware," www.komdigi.go.id, 2024, https://www.komdigi.go.id/berita/berita-pemerintahan/detail/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware.

Case	Reported scale/sector	Institutional response	Remedial gap
PDNS 2 (2024)	National public digital infrastructure; ransomware disrupted government services.	The government prioritized service restoration, migration, and technical containment.	The case demonstrated service-availability and accountability risks, but did not produce a clear compensation framework for data subjects.
Bank Syariah Indonesia (2023)	Ransomware disruption of banking services and public reports concerning an alleged LockBit claim involving customer and operational data at large scale.	OJK emphasized service restoration and cyber-resilience supervision; public debate also concerned banking security and customer protection.	The response showed separation between operational recovery in the banking sector and PDP-based redress, especially notification, valuation of privacy harm, and compensation for affected customers.

Source: Primary data, 2026

The issue of data breaches becomes more complex when analyzed from the perspective of legal liability. Law No. 27/2022 does not explicitly establish a strict liability regime for data breaches. Article 46 requires data controllers to notify data subjects when there is a failure to protect personal data; however, that provision does not state that notification automatically becomes a basis for liability without the need to prove fault. This model returns the liability framework to the principle of fault-based liability.[50] In the context of data breaches, proving fault is extremely difficult for data subjects because they lack access to the controller's internal systems, lack the technical capacity to conduct audits, and do not know how the security failure occurred. This information asymmetry reveals the imbalance of power between data controllers and data subjects in personal data protection disputes.[51] The uncertainty regarding the burden of proof creates legal uncertainty and limits victims' ability to obtain compensation.[52] Article 12 indeed states that data subjects have the right to file a civil claim; however, that provision is declaratory and contains no procedural mechanism, formula for calculating damages, or evidentiary rule more favorable to victims.

Ambiguity of causation in the digital context also weakens the effectiveness of Law No. 27/2022. The relevant causal framework should not be limited to the classical doctrine of conditio sine qua non or the but-for test, because victims often cannot prove that subsequent

[50]Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *Columbia Business Law Review* 2 (2019): 1–129, https://doi.org/10.22161/ijels.105.78.
[51]Julie E. Cohen, *Between Truth and Power* (Oxford University Press, 2019).
[52]Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet(Part 1)," *International Journal of Law and Information Technology* 18, no. 2 (2010): 176–93, https://doi.org/10.1093/ijlit/eaq002.

fraud, profiling practices, or risks of identity misuse,[53] would not have occurred without a particular breach. A more appropriate framework is risk-based causation supplemented by adequate causation: plaintiffs should show that the controller's security failure materially increased the legally relevant risk, and that the type of harm suffered - such as exposure to identity theft, risk of account takeover, reputational harm, loss of control, or mitigation costs - was a foreseeable consequence of the failure that created the risk. This approach is consistent with the distinction in tort law between factual causation and normative attribution,[54] and is more suitable for the technical opacity of data breach disputes.

Under that model, at the initial stage it should be sufficient for data subjects to prove that personal data under the controller's control was exposed, that the type of data exposed was capable of causing the alleged risk, and that the controller failed to demonstrate compliance with reasonable security measures. Thereafter, the burden of proof should shift to the controller to prove that the breach was not attributable to its system or that the harm was caused by an independent intervening event. Without such a presumption, Law No. 27/2022 leaves victims trapped between two evidentiary burdens: proving technical negligence in a system they cannot access and proving downstream harm that may develop gradually over time.

When analyzed from the perspective of Law No. 8/1999, a data breach committed by a business actor can in fact be constructed as a failure to fulfill consumers' rights to security, comfort, and safety under Article 4 letter a of Law No. 8/1999. Digital or electronic services that process consumer data should be subject to the principle of consumer safety.[55] In addition, Article 7 letter c requires business actors to provide accurate, clear, and honest information regarding the condition and guarantee of goods and/or services. From a teleological perspective, this obligation also includes the duty to explain to consumers how personal data is processed, stored, and protected. If a digital service fails to provide adequate security, the business actor may be deemed to have violated Article 8, which prohibits the trading of goods or services that do not meet safety standards.

However, Law No. 8/1999 does not classify personal data as a consumer asset. There is no category of "data" as an object of consumer protection. This creates a vacuum of remedy when consumers suffer harm, because Law No. 8/1999 only regulates protection for physical or conventional goods and/or services, not data-driven digital systems. The absence of recognition of data as an object of consumer protection prevents the product liability principle in Law No. 8/1999 from being optimally applied to digital services. Substantively, digital services are products equivalent to physical goods and services, and indeed carry greater risks because they may generate harm related to privacy, reputation, and identity security.[56] This

[53]Daniel J. Solove, "The Myth of the Privacy Paradox," George Washington Law Review 89, no. 1 (2021): 1–51, https://doi.org/10.2139/ssrn.3536265.
[54]H. L. A. Hart and Tony Honoré, Causation in the Law, 2nd ed. (Oxford: Clarendon Press, 1985).
[55]F. de Elizalde, *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*, *Journal of Consumer Policy*, vol. 48 (Springer US, 2025), https://doi.org/10.1007/s10603-025-09584-3.
[56]Giancarlo Frosio and Christophe Geiger, "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime," *European Law Journal* 29, no. 1–2 (2023): 31–77, https://doi.org/10.1111/eulj.12475.

gap impedes consumers from effectively suing business actors under Law No. 8/1999 because there is no explicit norm regulating data security standards as part of digital service safety.

This situation gives rise to the provocative criticism that Law No. 27/2022 functions as a "toothless tiger." Normatively, Law No. 27/2022 appears progressive; however, unclear technical norms, weak burden-of-proof rules, and the absence of sanctions capable of producing deterrence make the law ineffective in practice. Administrative sanctions in the form of written warnings, temporary suspension of data processing, data deletion, or administrative fines under Article 57 are important, but insufficient to create a strong deterrent effect, particularly against large companies with significant economic power.[57] Indeed, in many major data breach cases, data controllers have not been subjected to effective sanctions because the supervisory structure is incomplete and there is no independent authority with full power to conduct in-depth investigations and impose proportionate sanctions.[58]

Law No. 27/2022 also does not require business actors to conduct regular independent security audits, even though in countries with strong data protection law such audits are a primary instrument for ensuring compliance.[59] Without independent audits, compliance by business actors depends on self-regulation that is vulnerable to bias and conflicts of interest. When audits are not mandatory, there is no assurance that companies actually implement adequate security standardsadai.[60] In addition, public bodies receive several exemptions under Law No. 27/2022, for example Article 15, which provides exemptions for data processing by public bodies on grounds of national security, public service, or national interest. These exemptions are very broad and potentially violate the principle of equal protection of the law because public bodies are not subject to the same data-control standards as private entities.[61] When a public body experiences a data breach, there is no equivalent accountability mechanism because administrative sanctions cannot be applied to government agencies with the same intensity as to private entities. This creates an asymmetry of legal treatment between public and private data controllers.[62]

Another structural weakness is the absence of adequate procedural mechanisms to handle data breaches as civil wrongs. Law No. 27/2022 does not provide a class action mechanism, even though data breaches commonly occur at mass scale. Without class actions, data breach victims must file individual lawsuits, a nearly impossible option given litigation costs, evidentiary limitations, and uncertainty over compensation. This procedural-law gap weakens the effectiveness of data subjects' rights and reinforces the criticism that Law

[57]Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, 2023).
[58]Sebastian Golla, "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8, no. 1 (2017): 70–78, https://www.jipitec.eu/jipitec/article/view/192.
[59]Raphaël Gellert, "Understanding the Notion of Risk in the General Data Protection Regulation," *Computer Law and Security Review* 34, no. 2 (2018): 279–88, https://doi.org/10.1016/j.clsr.2017.12.003.
[60]Reuben Binns, "Data Protection Impact Assessments : A Meta-Regulatory Approach," *International Data Privacy Law* 7, no. 1 (2017): 22–35.
[61]Lynskey, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy."
[62]Christopher Docksey and Kenneth Propp, "Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective," *Oslo Law Review* 10, no. 1 (2023): 1–34.

No. 27/2022 offers only an "illusion of protection," not substantive protection. Group litigation is essential to guarantee access to justice for victims.[63]

From a constitutional perspective, this condition shows that the state has not fulfilled the principle of due diligence. Due diligence requires the state to prevent, investigate, punish, and provide remedies for human rights violations committed by state and non-state actors.[64] In the context of data breaches, the state fails to prevent because digital security standards have not been enforced effectively and consistently. This failure reflects weak regulatory capacity in guaranteeing the right to privacy as a human right in the digital age.[65] The state also fails to investigate adequately because there is no independent data protection authority with full power to conduct in-depth investigations into data breach incidents and enforce compliance by data controllers.[66] Further, the state fails to impose sanctions because the available administrative sanctions are often disproportionate to the harm caused and do not create deterrence against repeated violations. At the same time, the state also fails to provide redress because compensation mechanisms for data breach victims remain unclear, difficult to access, and not equipped with effective legal procedures to ensure substantive restoration of victims' rights.[67]

Accordingly, the overall data protection framework shows that data breaches constitute structural negligence caused by regulatory ineffectiveness, fragmentation of authority, and the state's inability to adapt law to developments in digital technology. Law No. 27/2022, which should be the principal instrument of data protection, is not yet strong enough to guarantee victims' redress. Meanwhile, Law No. 8/1999 as a consumer protection instrument has not accommodated the special character of data as a modern consumer asset. As a result, society remains vulnerable and lacks adequate access to justice, while business actors and public bodies do not yet face sufficient legal pressure to comply with data protection standards.[68] This condition not only produces violations of constitutional rights but also erodes public trust in the state and the legal system because the law is unable to perform its protective function effectively in the digital era.[69]

3.2. Disharmony, Legal Uncertainty, and Legal Fragmentation

Regulatory disharmony, legal uncertainty, and fragmentation of authority must be understood as problems of layered regulation, not as automatic legal conflict. Law

[63]Bart van der Sloot and Sascha van Schendel, "Procedural Law for the Data-Driven Society," *Information and Communications Technology Law* 30, no. 3 (2021): 304–32, https://doi.org/10.1080/13600834.2021.1876331.
[64]Lorna McGregor, Daragh Murray, and Vivian Ng, "International Human Rights Law as a Framework for Algorithmic Accountability," *International and Comparative Law Quarterly* 68, no. 2 (2019): 309–43, https://doi.org/10.1017/S0020589319000046.
[65]Juliane Kokott and Christoph Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law* 3, no. 4 (2013): 222–28, https://doi.org/10.1093/idpl/ipt017.
[66]Gentile and Lynskey, "Deficient by Design? The Transnational Enforcement of the GDPR."
[67]Jukka Ruohonen and Kalle Hjerppe, "The GDPR Enforcement Fines at Glance," *Information Systems* 106 (2022): 1–11, https://doi.org/10.1016/j.is.2021.101876.
[68]Paul de Hert and Papakonstantinou, "The New General Data Protection Regulation : Still a Sound System for the Protection of Individuals ?"
[69]Maria Tzanou, "Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right," *International Data Privacy Law* 3, no. 2 (2013): 88–99, https://doi.org/10.1093/idpl/ipt004.

No. 27/2022 is the national framework for personal data protection, but it operates within an ecosystem previously shaped by Government Regulation No. 71 of 2019 (PP 71/2019), OJK regulations on cyber resilience and banking information technology, regulations on trade through electronic systems, internal governance standards of state-owned enterprises, and general consumer protection law under Law No. 8/1999. Therefore, the issue is not merely whether one norm annuls another, but whether these various norms have a clear point of coordination when a data breach occurs.

PP 71/2019, for example, requires electronic system operators to maintain confidentiality, integrity, availability, authenticity, authorization, and non-repudiation in the operation of electronic systems. Law No. 27/2022 also imposes data security obligations on controllers. The two do not necessarily conflict; they may be read as mutually complementary: PP 71/2019 governs electronic system governance, while Law No. 27/2022 governs protection of data subjects. However, the absence of clear transitional provisions and coordination mechanisms creates uncertainty over the lead authority, investigation standards, sequencing of sanctions, how findings by cybersecurity authorities should affect civil liability,[70] and whether compliance with one regime may mitigate liability under another.

The same layered-regulation problem arises in the financial services sector and electronic commerce. POJK No. 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks and OJK Circular Letter No. 29/SEOJK.03/2022 on Cyber Resilience and Security for Commercial Banks establish cyber-resilience and information-technology governance obligations for banks, while Minister of Trade Regulation No. 31 of 2023 regulates the obligations of business actors conducting trade through electronic systems, including the duty to conduct electronic commerce safely and responsibly. These instruments need not be treated as conflicting with Law No. 27/2022. The problem is that no meta-regulatory rule determines when OJK becomes the lead authority, when the PDP authority takes over, how victim notifications must be standardized, and how sectoral sanctions relate to compensation for data subjects. As a result, layered regulation may appear complete on paper but fragmented in enforcement.

This fragmentation becomes more serious when applied to state-owned enterprises, which have different internal standard operating procedures, resulting in non-uniform data protection standards even within a single institutional cluster. Some state-owned enterprises adopt international standards such as ISO 27001, while others do not necessarily do so.[71] When a data breach occurs in a state-owned enterprise, it is unclear whether accountability must follow Law No. 27/2022, PP 71/2019, sectoral regulations, or the company's internal SOP. From a constitutional law perspective, this situation creates a regulatory cacophony that obscures the principle of legal certainty as guaranteed by Article 28D paragraph (1) of the 1945

[70]Lee A. Bygrave, "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements," Oslo Law Review 4, no. 2 (2017): 105–120, https://doi.org/10.18261/issn.2387-3299-2017-02-03.
[71]I Jalaludin S, "Terapkan Sistem Manajemen Keamanan Informasi, MIND ID Dapatkan Sertifikasi ISO 27001," kilasbumn.kompas.com, 2022, https://nasional.kompas.com/read/2022/09/15/15282881/terapkan-sistem-manajemen-keamanan-informasi-mind-id-dapatkan-sertifikasi.

Constitution. Legal certainty cannot be achieved when the regulatory structure itself is filled with overlap, disharmony, and the absence of an integrated enforcement structure.

One of the most fundamental institutional weaknesses is the absence of a truly independent personal data protection authority with functional capacity. Independence must not be treated as an end in itself, and independence does not automatically guarantee effectiveness. However, institutional independence is required when an authority must supervise both private and public bodies, investigate incidents involving government-controlled systems, issue corrective orders, and resolve complaints against actors that may possess political or economic power. A ministry within the executive branch may be effective for policy coordination, but it faces structural conflicts of interest when required to investigate or sanction other executive agencies, state-owned enterprises, or national digital programs.

The proper institutional design, therefore, is not independence detached from accountability, but independence combined with accountability. Law No. 27/2022 authority should have protected tenure, transparent appointment procedures, budgetary guarantees, professional expertise, investigative powers, corrective powers, publication of decisions, complaint-handling deadlines, cooperation protocols with OJK, BSSN, the Ministry of Trade, and consumer institutions, as well as judicial review to prevent arbitrariness. In this sense, independence is not a symbolic label, but a functional safeguard enabling the authority to investigate private platforms and public bodies without being absorbed into the same executive hierarchy that may itself become the object of investigation.[72]

Accordingly, the critique advanced here is not that every regulator relating to human rights must always possess formal independent status, but that personal data protection requires functional independence because the regulator directly supervises entities that may include the state itself.[73] Independence must be connected to measurable performance obligations, such as publication of enforcement statistics, reasoned decisions, complaint-handling time limits, cooperation protocols with sectoral regulators, and judicial review to prevent regulatory arbitrariness.

Comparative experience in the European Union, Singapore, and Australia shows that effective data protection generally depends on three institutional characteristics: an authority capable of acting independently, harmonized sectoral standards, and enforcement powers that connect prevention, sanctions, and redress. The GDPR requires independent supervisory authorities and provides a remedial structure that includes compensation, representative actions, and deterrent fines; Singapore's Personal Data Protection Act (PDPA) grants the Personal Data Protection Commission (PDPC) investigative powers and authority to impose financial penalties; while Australia's privacy framework empowers the Office of the Australian Information Commissioner (OAIC) to investigate and seek civil penalties for serious or repeated privacy interferences. These models should not be mechanically

[72]Orla Lynskey, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy," Theoretical Inquiries in Law 20, no. 1 (2019): 189–220, https://doi.org/10.1515/til-2019-0007.
[73]Juliane Kokott and Christoph Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR," International Data Privacy Law 3, no. 4 (2013): 222–28, https://doi.org/10.1093/idpl/ipt017.

transplanted, but they provide benchmarks,[74] for assessing why Indonesia's system remains weak when supervisory design, procedural remedial mechanisms, and the relationship between sanctions and compensation are still incomplete.

Legal uncertainty also arises at the remedial stage. When a data breach occurs in a digital service, consumers must determine whether to complain through PDP supervision, sectoral regulators such as OJK for banking cases, PMSE supervision for e-commerce, BPSK or civil courts under consumer protection law, or ordinary tort litigation. Law No. 27/2022 provides rights and supervisory sanctions, but does not regulate a fast compensation procedure. Law No. 8/1999 provides consumer mechanisms, but was not designed for data harm. PP 71/2019 and sectoral regulations regulate system security, but are not always connected to individual compensation. This fragmentation reduces the effectiveness of redress because victims must navigate several legal doors without one clear priority route.

Thus, regulatory disharmony, legal uncertainty, and the absence of an independent authority are structural problems that obstruct the realization of effective personal data protection.[75] This weakness is not merely technical, but constitutional, because it relates to the fulfillment of human rights, the rule of law, and the state's obligation to protect citizens from increasingly complex digital risks.[76] Without institutional reform, regulatory harmonization, and the establishment of an independent data protection authority, Indonesia's data protection law will remain behind international standards, while society continues to be vulnerable to data breaches, misuse of information, and exploitation in the digital economy.

3.2. Reformulating Personal Data Protection Law and the Digital Consumer Protection Regime

The reformulation of personal data protection law and digital consumer protection in Indonesia is an urgent necessity that cannot be postponed, given that the intensity, frequency, and scale of data breaches continue to rise without being matched by an adequate legal framework.[77] Normative reconstruction must begin with the fundamental recognition that personal data is not merely "information" in an administrative sense, but an object of legal protection with economic value, identity value, and vulnerability value that may directly affect consumer safety.[78] From this perspective, data needs to be classified as a non-physical consumer object/asset, namely, part of digital assets that form the legal relationship between data subjects and business actors. Law No. 8/1999 does not expressly mention personal data as an object of protection, but Article 4 of Law No. 8/1999, which grants the right to comfort,

---

[74]Paul de Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?," Computer Law & Security Review 32, no. 2 (2016): 179–94, https://doi.org/10.1016/j.clsr.2016.02.006.

[75]Andika Putra Wijaya, "Legal Protection of Personal Data in Electronic Transactions in Indonesia after the Enactment of the Personal Data Protection Law," *Journal of Legal and Judicial Studies* 1, no. 1 (2025): 41–46.

[76]Moody Rizqy Syailendra, Gunardi Lie, and Ahmad Sudiro, "Personal Data Protection Law in Indonesia: Challenges and Opportunities," *Indonesia Law Review* 14, no. 2 (2024): 56–72, https://doi.org/10.15742/ilrev.v14n2.4.

[77]Docksey and Propp, "Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective."

[78]Neil Richards and Woodrow Hartzog, "A Duty of Loyalty for Privacy Law," *Washington University Law Review*, 2021, 961–1021, https://doi.org/10.26350/004084_000183.

security, and safety in consuming goods and/or services, may be progressively interpreted to include the use of digital services that require the provision of personal data. Accordingly, data is no longer treated merely as an administrative input for business actors, but as a consumer asset that must be legally protected. This progressive interpretation is increasingly relevant because Article 1, number 1 of Law No. 27/2022 affirms that personal data is data concerning an individual who is identified or identifiable, either separately or in combination with other information, thereby providing a normative basis that data has a direct legal relationship with the individual as rights holder.

The conceptual linkage between Law No. 27/2022 and Law No. 8/1999 within the framework of digital consumer data protection gives rise to the need for harmonization that cannot be fulfilled through a partial or sectoral approach. In the current situation, the two statutes operate separately without systemic integration, even though in many cases the protected object is the same: the interests of data subjects who also occupy the position of consumers. This lack of synchronization creates a regulatory vacuum, especially concerning legal liability for data breaches, where Law No. 27/2022 establishes administrative procedures focused on reactive compliance, while Law No. 8/1999 provides broader compensation mechanisms but has not been formulated for the digital context. Therefore, the establishment of an Integrated Consumer Data Protection Code, whether in the form of a new statute or a comprehensive revision of Law No. 27/2022 and Law No. 8/1999, is necessary to unify personal data protection principles with consumer protection law. This Code must integrate data-processing principles under Law No. 27/2022, such as lawful basis for processing, purpose limitation, data minimization, integrity, and accountability, with consumer protection principles under Law No. 8/1999, such as legal certainty, information transparency, and protection of consumer interests. Such normative integration would enable the formation of a data protection law that not only emphasizes substantive rights of data subjects but also provides a strong and accessible remedial framework for consumers harmed by data breaches.

The proposed Integrated Consumer Data Protection Code should contain at least five operational clauses. First, the Code must define consumer personal data as a digital consumer asset protected by law. Second, the Code must establish a rebuttable presumption that a controller or digital service provider is liable when personal data under its control is exposed and the controller cannot prove compliance with reasonable security standards. Third, the Code must recognize material harm, immaterial harm, mitigation costs, and loss of control as compensable categories, while still allowing courts to filter purely speculative claims. Fourth, the Code must recognize class actions, representative actions by qualified consumer organizations or digital rights organizations, and small-claims procedures for low-value but mass-scale losses. Fifth, the Code must require periodic security audits and data protection impact assessments for high-risk processing, particularly in the financial, health, education, public service, and national digital infrastructure sectors.

One of the most crucial weaknesses of Law No. 27/2022 is the absence of a strict liability mechanism for business actors or data controllers when a data breach occurs. Law No. 27/2022 regulates notification obligations when a failure to protect personal data occurs, but it contains no provision stating that business actors are automatically liable for resulting harm. By contrast, Law No. 8/1999 actually contains the embryo of strict liability through Article 19,

which requires business actors to provide compensation for damage, contamination, or consumer losses resulting from the consumption of goods and/or services. However, that provision was not designed for digital systems and does not anticipate data-based harm such as identity theft, exploitation of behavioral profiles, or indirect economic loss. Therefore, establishing strict liability for data breaches is a normative necessity that can no longer be avoided. This norm is intended to shift the burden of proof from consumers to business actors, so that consumers do not have to prove negligence or complex causal relationships. In data breaches, which are often systemic, complex, and involve layered technologies, ordinary liability schemes are ineffective because victims are in the weakest epistemic and technical position to prove the data controller's fault.[79] Under strict liability, business actors must prove that all prescribed security standards were implemented and that the breach occurred because of force majeure or an unavoidable attack despite optimal security measures.[80]

Further, the compensation mechanism under Law No. 27/2022 should be expanded by imposing punitive damages on business actors or entities that fail to safeguard personal data. Punitive damages are not merely a compensatory instrument, but also a legal instrument to create deterrence and prevent repeated violations. The compensation framework in Article 12 of Law No. 27/2022 merely states that data subjects have the right to obtain compensation for violations of personal data protection, but it provides no formula, minimum threshold, or mechanism for calculating damages. This uncertainty leaves rights enforcement dependent on judicial discretion and tends to generate inconsistent decisions. By introducing punitive damages, business actors would be encouraged to treat data security as a core compliance obligation, not merely an administrative burden.[81] This is consistent with practice in other jurisdictions, such as the United States and the European Union, where punitive or administrative fines function as tools to control corporate behavior that disregards data security.[82]

Another gap in Law No. 27/2022 is the absence of mandatory security audit obligations and independent data protection impact assessments. Article 35 of Law No. 27/2022 only requires data controllers to implement security measures for personal data, but does not detail operational standards or external audit mechanisms. This differs fundamentally from the GDPR, which requires data protection impact assessments for all high-risk processing and mandates measurable technical and organizational measures. The absence of independent audits under Law No. 27/2022 allows data controllers unilaterally to claim that their systems are secure without external verification. Regulatory reform must include mandatory periodic audits by licensed and specially accredited third parties, thereby creating an objective check-

[79]Danielle Keats Citron and Daniel J. Solove, "Privacy Harms," *Boston University Law Review* 102, no. 3 (2022): 793–863, https://doi.org/10.2139/ssrn.3782222.
[80]Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press, 2018).
[81]Margot E. Kaminski, *The Right to Explanation, Explained. In Research Handbook on Information Law and Governance* (Edward Elgar Publishing, 2021).
[82]Jozef Andraško, Matúš Mesarčík, and Ondrej Hamuľák, "The Regulatory Intersections between Artificial Intelligence, Data Protection and Cyber Security: Challenges and Opportunities for the EU Legal Framework," *AI and Society* 36, no. 2 (2021): 623–36, https://doi.org/10.1007/s00146-020-01125-5.

and-balance mechanism.[83] Independent audits are important because many data breaches in Indonesia stem from neglected basic security practices, such as the use of default passwords, unencrypted servers, or the absence of incident monitoring.[84]

The institutional structure of Indonesia's data protection law also requires fundamental reform through the establishment of a truly independent data protection authority. Law No. 27/2022 indeed regulates the creation of a personal data protection authority, but places it under the President with functions that are not yet fully independent, either institutionally or operationally. This model is vulnerable to executive bias, political intervention, and conflicts of interest, especially when the data being managed is public data intersecting with political interests. Compared with the European Data Protection Board in the European Union, the Personal Data Protection Commission in Singapore, or the Office of the Australian Information Commissioner in Australia, Indonesia's system remains behind in terms of independence, investigative mandate, and enforcement authority. Institutional reform must establish an authority with an investigative mandate, administrative inquiry powers, authority to order system suspension, and authority to impose fines proportionate to the scale of the violation. Institutional independence is an absolute prerequisite for ensuring enforcement free from political pressure and for securing accountability among business actors and state institutions.[85]

As part of a victim-centered approach, class actions and small-claims mechanisms for data breach victims must be clearly institutionalized in Indonesian law. Law No. 27/2022 indeed requires notification when a data breach occurs, but does not provide a collective legal route for thousands or millions of victims to claim compensation in a structured manner. In data breach cases, victims are often large groups with relatively small individual losses but very large collective harm. Small-claims procedures provide a fast and affordable path for victims to sue business actors without having to go through a lengthy and costly court process. Meanwhile, class actions are an effective instrument for consolidating victims' interests and creating a balanced bargaining position against large corporations. These two mechanisms would lead to what may be called restorative data justice: a form of justice that not only restores economic losses but also reclaims autonomy over personal data that has been violated.

The concept of restorative data justice requires a paradigm shift from an administrative approach emphasizing formal compliance toward a human-rights-based approach and protection of digital integrity. Redress is not sufficient if it consists only of monetary compensation; it must also include clear risk notification, technical assistance to mitigate impact, credit or identity monitoring support where relevant, transparent forensic summaries, and public assurances that systemic weaknesses have been corrected.

---

[83]N. Helberger et al., "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability," *Journal of Consumer Policy* 45, no. 2 (2022): 175–200, https://doi.org/10.1007/s10603-021-09500-5.

[84]Alessandro Mantelero et al., "The Common EU Approach to Personal Data and Cybersecurity Regulation," *International Journal of Law and Information Technology* 28, no. 4 (2020): 297–328, https://doi.org/10.1093/ijlit/eaaa021.

[85]Charles Raab and Ivan Szekely, "Data Protection Authorities and Information Technology," *Computer Law and Security Review* 33, no. 4 (2017): 421–33, https://doi.org/10.1016/j.clsr.2017.05.002.

Accordingly, the reformulation of data protection law and digital consumer protection must be carried out structurally, conceptually, and institutionally. Expanding the legal framework to recognize data as an object of consumer protection provides a strong normative basis for protecting data subjects' rights. Harmonizing Law No. 27/2022 and Law No. 8/1999 through an Integrated Consumer Data Protection Code would resolve the normative disharmony that has long created legal uncertainty. The application of strict liability, punitive damages, independent audits, and data protection impact assessments would strengthen accountability standards for business actors and public bodies. The establishment of an independent data protection authority would safeguard the integrity of law enforcement. In addition, class actions and small-claims mechanisms would strengthen the victim-centered orientation of the law, allowing restorative data justice to be realized as a new paradigm of personal data protection in Indonesia. Collectively, all these elements would form the foundation of a modern, integrated, and consumer-oriented data protection system capable of responding to the challenges of the digital economy while guaranteeing constitutional protection in a data-driven society.

4. Conclusions

The legal framework for personal data protection and digital consumer protection in Indonesia operates through overlapping regimes, but it has not been adequately coordinated. This article affirms that the issue is not always a direct conflict of norms; in many respects, Law No. 27/2022, Law No. 8/1999, PP 71/2019, OJK cyber-resilience regulations, and PMSE regulations can be applied simultaneously. The deeper weakness lies in incomplete remedies, institutional uncertainty, and the absence of procedural rules determining the lead authority, burden of proof, causation standards, compensation mechanisms, and collective redress routes. Law No. 27/2022 is *lex specialis* for data-processing obligations, but it has not yet become a complete *lex specialis* for digital consumer harm because it does not comprehensively regulate compensation, class actions, small claims, punitive or deterrent damages, or rebuttable presumptions of causation. Law No. 8/1999 remains normatively relevant because personal data is now embedded in the safety and quality of digital services, but that statute must be reconstructed to recognize data as a consumer asset. The Tokopedia, Bukalapak, BPJS Kesehatan, KPU voter data, Bank Syariah Indonesia, and PDNS 2 cases show that Indonesia's system can mobilize administrative coordination and operational recovery, but has not yet produced predictable and victim-oriented redress. Therefore, reform must be directed toward the establishment of an Integrated Consumer Data Protection Code, a risk-based causation model, strict or presumptive liability for data controllers, mandatory independent audits and data protection impact assessments, class actions and small-claims mechanisms, and an independent yet accountable PDP Authority with investigative and corrective powers. Only through these reforms can Indonesia move from symbolic compliance toward data justice that is substantive, deterrent, and restorative.

5. Acknowledgements

The author gratefully acknowledges the financial support provided by Beasiswa Pendidikan Indonesia (The Indonesian Education Scholarship); Pusat Pelayanan Pembiayaan dan Asesmen Pendidkan Tinggi (Center for Higher Education Funding and Assessment), Ministry of Higher Education, Science, and Technology of Republic Indonesia; Lembaga

Pengelola Dana Pendidikan (Endowment Fund for Education Agency), Ministry of Finance of Republic Indonesia. This support contributed to the completion of the research and the publication of this scholarly work.

6. Funding (optional)

-

7. References

Aditya, Nicholas Ryan. "Pratikno: Tak Ada Indikasi Kebocoran 58 Juta Data Siswa, Tapi..." nasional.kompas.com, 2026. https://nasional.kompas.com/read/2026/02/10/12312261/pratikno-tak-ada-indikasi-kebocoran-58-juta-data-siswa-tapi.

Adu, Inggret. "Personal Data Protection in E-Commerce Platforms : Legal Challenges , Regulatory Frameworks , and the Path toward Digital Consumer Trust." Priviet Social Sciences Journal 6, no. 5 (2026): 118–128.

Alsenoy, Brendan Van. "Liability under EU Data Protection Law From Directive 95/46 to the General Data Protection Regulation." Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2, no. d (2016): 271–88.

Andraško, Jozef, Matúš Mesarčík, and Ondrej Hamuľák. "The Regulatory Intersections between Artificial Intelligence, Data Protection and Cyber Security: Challenges and Opportunities for the EU Legal Framework." AI and Society 36, no. 2 (2021): 623–36. https://doi.org/10.1007/s00146-020-01125-5.

Aribawa, Muhammad Yustino. "Legal Certainty of Home Industry Food Through National Agency of Drug And Food Control's Post Market In View From Law No. 8 of 1999 Concerning Consumer Protection." Jurnal Hukum Bisnis Bonum Commune 6, no. 1 (2023): 21–29.

Balkin, Jack M. "Information Fiduciaries and the First Amendment." U.C. Davis Law Review 49, no. 4 (2016): 1183.

Basyari, Iqbal, and Nikolaus Harbowo. "Nvestigasi Dugaan Kebocoran Data Pemilih Dituntut Transparan." www.kompas.id, 2023. https://www.kompas.id/artikel/investigasi-dugaan-kebocoran-data-pemilih-dituntut-transparan.

Bhakti, Agus, Arfin Sudirman, R. Widya Setiabudi, and Arry Bainus Sumadinata. "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions : A Case Study in Indonesia." Journal of Human Security 20, no. 1 (2024): 109–17.

Binns, Reuben. "Data Protection Impact Assessments : A Meta-Regulatory Approach." International Data Privacy Law 7, no. 1 (2017): 22–35.

Bradford, Anu. Digital Empires: The Global Battle to Regulate Technology. Oxford University Press, 2023.

Bygrave, Lee A. "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements." Oslo Law Review 4, no. 2 (2017): 105–1020. https://doi.org/https://doi.org/10.18261/issn.2387-3299-2017-02-03.

———. "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements." Oslo Law Review 4, no. 2 (2017): 105–20. https://doi.org/10.18261/issn.2387-3299-2017-02-03.

Citron, Danielle Keats, and Daniel J. Solove. "Privacy Harms." Boston University Law Review 102, no. 3 (2022): 793–863. https://doi.org/10.2139/ssrn.3782222.

Cohen, Julie E. Between Truth and Power. Oxford University Press, 2019.

Dachlan, Andrew Ardiyanto, Alya Nabila, Nabilatul Alimah Putri, and Nabilah Nurmasitha. "Pertanggungjawaban Hukum Pemerintah Dalam Kebocoran Data Pribadi Pada Penyelenggaraan Pusat Data Nasional." Jurnal Hukum Samudra Keadilan 20, no. 1 (2025): 109–24.

Dewi, Intan Rakhmayanti. "13 Juta Data Milik Bukalapak Diduga Dijual Di Dark Web." www.tekno.sindonews.com, 2020. https://tekno.sindonews.com/read/19589/207/13-juta-data-milik-bukalapak-diduga-dijual-di-dark-web-1588770317.

———. "Komdigi Jawab Isu Data 13 Universitas Di Indonesia Bocor." www.cnbcindonesia.com, 2026. https://www.cnbcindonesia.com/tech/20260123101312-37-704671/komdigi-jawab-isu-data-13-universitas-di-indonesia-bocor.

Docksey, Christopher, and Kenneth Propp. "Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective." Oslo Law Review 10, no. 1 (2023): 1–34.

Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiro Júnior. "Special Strict Civil Liability in Brazil's General Data Protection Law." Brazilian Journal of Law, Technology and Innovation 2, no. 2 (2024): 98–128. https://doi.org/10.59224/bjlti.v2i2.98-128.

Elizalde, F. de. Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law. Journal of Consumer Policy. Vol. 48. Springer US, 2025. https://doi.org/10.1007/s10603-025-09584-3.

Firdaus, Achmad. "Kasus Kebocoran Data Pribadi Di Indonesia: 10 Kejadian Terbesar Yang Perlu Diketahui." www.medcom.id, 2024. https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus-kebocoran-data-pribadi-di-indonesia-10-kejadian-terbesar-yang-perlu-diketahui.

Frosio, Giancarlo, and Christophe Geiger. "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime." European Law Journal 29, no. 1–2 (2023): 31–77. https://doi.org/10.1111/eulj.12475.

Garner, Bryan A., and Antonin Scalia. Reading Law: The Interpretation of Legal Texts. West Group, 2011.

Gellert, Raphaël. "Understanding the Notion of Risk in the General Data Protection Regulation." Computer Law and Security Review 34, no. 2 (2018): 279–88. https://doi.org/10.1016/j.clsr.2017.12.003.

Gentile, Giulia, and Orla Lynskey. "Deficient by Design? The Transnational Enforcement of the GDPR." International & Comparative Law Quarterly 71, no. October (2022): 799–830. https://doi.org/10.1017/S0020589322000355.

Golla, Sebastian. "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR." Journal of Intellectual Property, Information Technology and E-Commerce Law 8, no. 1 (2017): 70–78. https://www.jipitec.eu/jipitec/article/view/192.

Hart, H. L. A., and Tony Honoré. Causation in the Law. Second Edi. Oxford: Clarendon Press, 1985.

Hayati, Adis Nur. "The Issue of Dark Patterns in Digital Platforms: The Challenge for Indonesia's Consumer Protection Law." Asian Journal of Law and Society 11, no. 4 (2024): 453–465.

Helberger, N., M. Sax, J. Strycharz, and H.-W. Micklitz. "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability." Journal of Consumer Policy 45, no. 2 (2022): 175–200. https://doi.org/10.1007/s10603-021-09500-5.

Hert, Paul de, and Vagelis Papakonstantinou. "The New General Data Protection Regulation : Still a Sound System for the Protection of Individuals ?" Computer Law & Security Review: The International Journal of Technology Law and Practice 32, no. 2 (2016): 179–94. https://doi.org/10.1016/j.clsr.2016.02.006.

Hetharie, Yosia, Isis Ikhwansyah, Ema Rahmawati, and Valentino Dinatra Soplantila. "Hybrid Model of Personal Data Protection for Consumers in Digital MSMEs: A Comparative Study of Indonesian and Chinese Regulations." Journal of Law and Legal Reform 6, no. 4 (2025): 2015–2058.

Ibrahim, Johnny. Teori Dan Metodologi Penelitian Hukum Normatif. Bayumedia Publishing, 2006.

Januarita, Ratna, Indra Fajar Alamsyah, and Arif Perdana. "Guardians of Data: TruMe Life's Continuous Quest for Data Protection." Journal of Information Technology Teaching Cases 15, no. 2 (2025): 254–64. https://doi.org/10.1177/20438869241242141.

Kaminski, Margot E. The Right to Explanation, Explained. In Research Handbook on Information Law and Governance. Edward Elgar Publishing, 2021.

Kementerian Komunikasi dan Informatika. "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware." www.komdigi.go.id, 2024. https://www.komdigi.go.id/berita/berita-pemerintahan/detail/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware.

———. "Siaran Pers No. 63/HM/KOMINFO/05/2020 Tentang Demi Melindungi Data Pengguna, Kominfo Minta Tokopedia Lakukan Investigasi Internal." www.komdigi.go.id, 2020. https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-63-hm-kominfo-05-2020-tentang-demi-melindungi-data-pengguna-kominfo-minta-tokopedia-lakukan-investigasi-internal.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. "Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kemkominfo Usut Tuntas." www.menpan.go.id, 2021. https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas.

Kokott, Juliane, and Christoph Sobotta. "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR." International Data Privacy Law 3, no. 4 (2013): 222–28. https://doi.org/10.1093/idpl/ipt017.

Komisi Pemilihan Umum. "Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU." www.kpu.go.id, 2023. https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu.

Kuner, Christopher. "Data Protection Law and International Jurisdiction on the Internet(Part 1)." International Journal of Law and Information Technology 18, no. 2 (2010): 176–93. https://doi.org/10.1093/ijlit/eaq002.

Kusuma, Oktaria Wim, and Abraham Ferry Rosando. "Urgensi Perlindungan Hukum Terhadap Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online." Jurnal Hukum Bisnis Bonum Commune 5, no. 1 (2022): 123–41.

Lintvedt, Mona Naomi. "Putting a Price on Data Protection Infringement." International Data Privacy Law 12, no. 1 (2022): 1–15.

Lynskey, Orla. "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy." Theoretical Inquiries in Law 20, no. 1 (2019): 189–220. https://doi.org/10.1515/til-2019-0007.

———. The Foundations of EU Data Protection Law. Oxford University Press, 2015.

MacCormick, Neil. Rhetoric and the Rule of Law: A Theory of Legal Reasoning. Oxford University Press, 2005.

Malgieri, Gianclaudio, and Jędrzej Niklas. "Vulnerable Data Subjects." Computer Law and Security Review 37, no. 788039 (2020): 1–16. https://doi.org/10.1016/j.clsr.2020.105415.

Mantelero, Alessandro. Beyond Data. In Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI. TMC Asser Press, 2020.

Mantelero, Alessandro, Giuseppe Vaciago, Maria Samantha Esposito, and Nicole Monte. "The Common EU Approach to Personal Data and Cybersecurity Regulation." International Journal of Law and Information Technology 28, no. 4 (2020): 297–328. https://doi.org/10.1093/ijlit/eaaa021.

Marzuki, Mahmud. Penelitian Hukum: Edisi Revisi. Prenada Media, 2017.

McGregor, Lorna, Daragh Murray, and Vivian Ng. "International Human Rights Law as a Framework for Algorithmic Accountability." International and Comparative Law Quarterly 68, no. 2 (2019): 309–43. https://doi.org/10.1017/S0020589319000046.

Novianty, Dythia. "Peneliti: Indonesia Peringkat 5 Global Paling Berisiko Kena Serangan Siber." www.suara.com, 2022. https://www.suara.com/tekno/2022/12/01/143251/peneliti-indonesia-peringkat-5-global-paling-berisiko-kena-serangan-siber#.

Otoritas Jasa Keuangan. "Press Release: Bank Syariah Indonesia Operates Back to Normal, Public Can Rest Assured." https://ojk.go.id, 2023. https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/Bank-Syariah-Indonesia-Operates-Back-To-Normal%2C-Public-Can-Rest-Assured.aspx?

Pauwelyn, Joost. Conflict of Norms in Public International Law: How WTO Law Relates to Other Rules of International Law. Cambridge University Press, 2009.

Raab, Charles, and Ivan Szekely. "Data Protection Authorities and Information Technology." Computer Law and Security Review 33, no. 4 (2017): 421–33. https://doi.org/10.1016/j.clsr.2017.05.002.

Ramli, Rully R. "Soal Dugaan Kebocoran Data SIM Card, Telkomsel: Data Yang Tersimpan Dalam Sistem Internal Tetap Aman." money.kompas.com, 2022. https://money.kompas.com/read/2022/09/02/134500926/soal-dugaan-kebocoran-data-sim-card-telkomsel--data-yang-tersimpan-dalam.

Richards, Neil, and Woodrow Hartzog. "A Duty of Loyalty for Privacy Law." Washington University Law Review, 2021, 961–1021. https://doi.org/10.26350/004084_000183.

Rinjani, Muhamad Adri, and Ricky Firmansyah. "Hambatan Implementasi UU 27 / 2022 Dan Strategi Penguatan Perlindungan Data Pribadi Di Indonesia." Jurnal Analisis Hukum 8, no. 1 (2025): 70–83.

Rosadi, Sinta Dewi, and Pratama Garry Gumelar. "Urgensi Perlindungan Data Privasidalam Era Ekonomi Digital Di Indonesia." Veritas et Justitia 4, no. 1 (2018): 88–110. https://doi.org/10.25123/vej.2916.

Ruohonen, Jukka, and Kalle Hjerppe. "The GDPR Enforcement Fines at Glance." Information Systems 106 (2022): 1–11. https://doi.org/10.1016/j.is.2021.101876.

S, I Jalaludin. "Terapkan Sistem Manajemen Keamanan Informasi, MIND ID Dapatkan Sertifikasi ISO 27001." kilasbumn.kompas.com, 2022. https://nasional.kompas.com/read/2022/09/15/15282881/terapkan-sistem-manajemen-keamanan-informasi-mind-id-dapatkan-sertifikasi.

Sahetapy, Wilma Laura. "Perlindungan Data Pribadi Anak Dalam E-Commerce Di Masa Pandemi Covid-19." Jurnal Hukum Bisnis Bonum Commune 4, no. 2 (2021): 214–25.

Setiawati, Susi. "Tak Cuma Kemhan Pak Anies, Ini Daftar Instansi Yang Diserang Hacker." www.cnbcindonesia.com, 2024. https://www.cnbcindonesia.com/research/20240108091525-128-503641/tak-cuma-kemhan-pak-anies-ini-daftar-instansi-yang-diserang-hacker.

Silalahi, Johan Alfred Sarades, Yuspika Yuliana Purba, and Muhammad Fadly Nasution. "Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana Di Indonesia." Jurnal Minfo Polgan 14, no. 2 (2025): 604–13.

Sinclair, Sir Ian McTaggart. The Vienna Convention on the Law of Treaties. Manchester University Press, 1984.

Sloot, Bart van der, and Sascha van Schendel. "Procedural Law for the Data-Driven Society." Information and Communications Technology Law 30, no. 3 (2021): 304–32. https://doi.org/10.1080/13600834.2021.1876331.

Soekanto, Soerjono, and Sri Mamudji. Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Raja Grafindo Persada, 2010.

Solove, Daniel J. "Introduction: Privacy Self-Management and the Consent Dilemma." Harvard Law Review 126, no. 7 (2013): 1880–1903.

———. "The Myth of the Privacy Paradox." George Washington Law Review 89, no. 1 (2021): 1–51. https://doi.org/https://doi.org/10.2139/ssrn.3536265.

———. "The Myth of the Privacy Paradox." George Washington Law Review 89, no. 1 (2021): 1–51. https://doi.org/10.2139/ssrn.3536265.

Strugala, Radoslaw. "Art. 82 GDPR: Strict Liability or Liability Based on Fault?" European Journal of Privacy Law & Technologies, 2020, 71–79.

Syailendra, Moody Rizqy, Gunardi Lie, and Ahmad Sudiro. "Personal Data Protection Law in Indonesia: Challenges and Opportunities." Indonesia Law Review 14, no. 2 (2024): 56–72. https://doi.org/10.15742/ilrev.v14n2.4.

Tzanou, Maria. "Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right." International Data Privacy Law 3, no. 2 (2013): 88–99. https://doi.org/10.1093/idpl/ipt004.

Wachter, Sandra, and Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." Columbia Business Law Review 2 (2019): 1–129. https://doi.org/10.22161/ijels.105.78.

Wakang, Aisyah Amira. "Daftar Status Layanan Instansi Yang Terdampak Serangan Siber PDNS per 26 Juni." www.tempo.co, 2024. https://www.tempo.co/hukum/daftar-status-layanan-instansi-yang-terdampak-serangan-siber-pdns-per-26-juni-45170.

Waldman, Ari Ezra. Privacy as Trust: Information Privacy for an Information Age. Cambridge University Press, 2018.

Wijaya, Andika Putra. "Legal Protection of Personal Data in Electronic Transactions in Indonesia after the Enactment of the Personal Data Protection Law." Journal of Legal and Judicial Studies 1, no. 1 (2025): 41–46.

Wijayaatmaja, Yakub Pryatama. "Kebocoran Data PDN Dianggap Pintu Bencana Nasional Keamanan Siber." mediaindonesia.com, 2024. https://mediaindonesia.com/politik-dan-hukum/681701/kebocoran-data-pdn-dianggap-pintu-bencana-nasional-keamanan-siber.

Yanti, Musrika. "Analisis Tanggung Jawab Perdata Dalam Kebocoran Data: Sinkronisasi UU Perlindungan Data Pribadi Dan KUH Perdata." Jurnal Ilmu Sosial Dan Humaniora 1, no. 4 (2025): 1539–1549.

Zainuddin, Ali. Metode Penelitian Hukum. Sinar Grafika, 2021.

Zuboff, Shoshana. "The Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." Journal of Information Technology 30, no. 1 (2015): 75–89. https://doi.org/10.1057/jit.2015.5.