



TOWARD A VICTIM-ORIENTED DIGITAL JUSTICE MODEL: LEGAL PROTECTION FOR PERSONAL DATA MISUSE UNDER THE PERSONAL DATA PROTECTION LAW

Nur Khalimatus Sa'diyah

Universitas Wijaya Kusuma Surabaya, Indonesia, Email: nurkhalimatus.uwks@gmail.com

Raden Besse Kartoningrat

Universitas Wijaya Kusuma Surabaya, Indonesia, Email: rbkartoningrat12@gmail.com

Umi Enggarsasi

Universitas Wijaya Kusuma Surabaya, Indonesia, Email: umnggarsasi12@gmail.com

ARTICLE INFO

Keywords:

Access to Justice; Digital Justice Model; Legal Enforcement Gaps; Personal Data Misuse; Victim Protection.

DOI :

10.26532/jh.v42i2.48829

ABSTRACT

This study examines legal protection for victims of personal data misuse in Indonesia within the context of Society 5.0 by addressing three objectives: analyzing existing legal protections under the Personal Data Protection (PDP) Law, identifying gaps between normative regulation and law enforcement practice, and formulating a victim-oriented digital justice model. Using a normative and conceptual approach, this study analyzes Law Number 27 of 2022 and related regulations through qualitative descriptive methods. The findings reveal significant structural weaknesses in Indonesia's personal data protection regime. Normatively, the PDP Law has not explicitly positioned victims as rights-bearing subjects entitled to restitution, compensation, and digital rehabilitation. Practically, enforcement remains compliance-oriented, relying heavily on administrative sanctions while neglecting victims' access to justice, redress, and recovery. Institutional fragmentation, limited evidentiary access, and the absence of an independent data protection authority further weaken victim protection. This study proposes a victim-oriented digital justice model that integrates rights-based enforcement, restorative justice principles, and international human rights standards, particularly the UN Basic Principles on Remedy and Reparation. The model emphasizes legal recognition of victims, effective access to justice, and comprehensive redress mechanisms to ensure meaningful protection and restoration of victims' rights in the digital era.

1. Introduction

The global acceleration of digital transformation has fundamentally changed the way societies build social interactions, conduct economic exchanges, and organize governance.¹ Digital technology now serves as a key infrastructure in everyday life, from communications and economic transactions to education, to healthcare and public administration. While this transformation brings efficiency and innovation, it has also given rise to new and previously unknown forms of vulnerability, particularly related to the collection, processing, and circulation of personal data.² It is in this context that the Japanese government introduced the concept of Society 5.0, a vision of a super-intelligent society that integrates artificial intelligence, big data, the Internet of Things, and cyber-physical systems with the primary goal of improving human well-being.³ Unlike the previous industrial paradigm that emphasized productivity and automation, Society 5.0 firmly places humans at the center, with technology positioned as a means to strengthen dignity, inclusivity, and social justice.⁴

However, the realization of Society 5.0 faces serious legal and ethical challenges, particularly regarding the governance and protection of personal data. As digital systems increasingly rely on large-scale data extraction and algorithmic decision-making, personal data has transformed into a strategic economic and political asset that underpins digital markets and public administration.⁵ This transformation increases the risks of data misuse, identity theft, excessive surveillance, and privacy violations, particularly in countries with limited regulatory and law enforcement capacity.⁶ These risks directly impact individual autonomy, security, and social participation, potentially contradicting the human-centered principles at the heart of Society 5.0.⁷

In Indonesia, the acceleration of digitalization has exposed structural weaknesses

¹ Florian Cech, and Hilda Tellioglu., Impact of the digital transformation: an online real-time delphi study, *arXiv preprint arXiv:1904.11411*, no.1, 2019.

² David Lyon., Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society*, Vol.1, no.2, 2014, page.203.

³ Carolina Narvaez Rojas, Gustavo Adolfo Alomia Peñafiel, Diego Fernando Loaiza Buitrago, and Carlos Andrés Tavera Romero., Society 5.0: A Japanese concept for a superintelligent society, *Sustainability*, Vol.13, no.12, 2021, page.6567. See too, UNESCO., Japan Pushing Ahead with Society 5.0 to Overcome Chronic Social Challenges, *UNESCO*, February 21, 2019.

⁴ Omer Tene, and Jules Polonetsky., Big data for all: Privacy and user control in the age of analytics, *Nw. J. Tech. & Intell. Prop.*, Vol.11, no.2, 2012, page.239.

⁵ Linnet Taylor., What is data justice? The case for connecting digital rights and freedoms globally, *Big Data & Society*, Vol.4, no.2, 2017, page.336.

⁶ Charukeshi Bhatt, and Anirudh Burman., Data Protection Regulation in the Global South, *Carnegie Endowment for International Peace*, February 21, 2024. See too, Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.25; Martin Tisné., The Data Delusion: Protecting Individual Data Isn't Enough When the Harm Is Collective, Edited by Marietje Schaake, *Luminate*, July 2020.

⁷ Michele De Donno, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone, and Manuel Mazzara., Cyber-storms come from clouds: Security of cloud computing in the IoT era, *Future Internet*, Vol.11, no.6, 2019, page.127. See too, Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre De Montjoye., Estimating the success of re-identifications in incomplete datasets using generative models, *Nature communications*, Vol.10, no.1, 2019, page.3070.

in personal data governance and protection. Empirical evidence shows that large-scale personal data leaks occur repeatedly, in both the public and private sectors, involving millions of data subjects. One prominent example is the alleged population data leak from the Directorate General of Population and Civil Registration (*Dukcapil*), which involved hundreds of millions of data records, including National Identification Numbers (*Nomer Induk Kependudukan*/NIK), names, and dates of birth, which were traded on illegal online forums.⁸ Furthermore, ransomware attacks on major financial institutions have also compromised the personal and financial data of millions of customers, increasing the risk of identity theft and digital fraud.⁹ National cybersecurity monitoring data even shows that Indonesia is among the countries with the highest data leak rates, with tens of millions of digital accounts exposed in recent years.¹⁰

This phenomenon confirms that personal data breaches in Indonesia are not isolated incidents, but rather a structural and recurring problem. The impacts extend beyond technical disruptions to significant harm to individuals. Research shows that data breach victims experience financial loss, reputational damage, and psychological distress in the form of prolonged anxiety and insecurity, ultimately impacting their social and economic participation.¹¹ Therefore, personal data protection cannot be understood solely as a technical or administrative issue, but rather as a matter of legal justice and human rights protection.

In response to these increasing risks, Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Normatively, the PDP Law adopts key data protection principles consistent with international practice, such as lawful processing, data subject consent, purpose limitation, and recognition of data subject rights.¹² Comparative studies show that this approach reflects global

⁸ Aditya Widya Putri., Data pribadi terserak, nasib sial masyarakat hadapi kebocoran data, *Katadata.co.id*, July 31, 2023.

⁹ Ahmad Wijaya., Kebocoran data jadi ancaman serius merugikan individu dan Perusahaan, *ANTARA News*, May 23, 2024.

¹⁰ Rita Puspita Sari., RI masuk 10 besar kebocoran data, hampir 94,22 juta akun bocor, *CSIRT Indonesia*, November 29, 2024.

¹¹ Christopher R. Sears, and Daniel R. Cunningham., Individual differences in psychological stress associated with data breach experiences, *Journal of Cybersecurity and Privacy*, Vol.4, no.3, 2024, page.610. See too, Fiona Spanca, and Armend Salihu., Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age, In *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, New York, IEEE, 2024, Page.5; Eric Bachura, Rohit Valecha, Rui Chen, and H. Raghav Rao., The OPM data breach: An investigation of shared emotional reactions on Twitter, *MIS quarterly*, Vol.46, no.2, 2022, page.892; Mark Button, Dean Blackburn, Lisa Sugiura, David Shepherd, Richard Kapend, and Victoria Wang., Victims of cybercrime: Understanding the impact through accounts, In *Cybercrime in context: The human factor in victimization, offending, and policing*, Cham, Springer International Publishing, 2021, page.142; Danielle Keats Citron, and Daniel J. Solove., Privacy harms, *BUL Rev.* no.102, 2022, page.793.

¹² Asep Mahbub Junaedi., Urgensi perlindungan data pribadi dalam era digital: analisis Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi, *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, Vol.5, no.2, 2025, page.250.

trends influenced by the European Union's General Data Protection Regulation (GDPR) model.¹³ Normatively, the ratification of the PDP Law represents an important milestone in strengthening national digital governance.¹⁴

However, there is a significant gap between normative recognition and the reality of implementation, particularly in terms of victim protection and redress mechanisms. Despite continued large-scale data breaches, law enforcement under the Personal Data Protection Law remains very limited. As of 2024, only three criminal cases involving personal data protection violations had been officially processed since the law's enactment.¹⁵ This disparity between the magnitude of the violations and the limited legal redress efforts demonstrates the weakness of victim protection mechanisms.

The phenomenological gap in personal data protection in Indonesia becomes increasingly apparent in the post-data breach phase. While investigations and administrative sanctions against data controllers are sometimes announced, victims are generally not actively involved in the recovery process. The Personal Data Protection Law (PDP Law) does not yet provide an operational mechanism that guarantees automatic notification, restitution, compensation, or rehabilitation for victims, so recovery relies on civil lawsuits or criminal reports that are expensive, complex, and difficult to access.¹⁶ Consequently, access to justice is enjoyed by only a small proportion of victims. This situation indicates that the personal data protection regime is still oriented towards administrative compliance, rather than protecting victims' rights.¹⁷ The power imbalance between victims and digital corporations, in terms of control over technology, legal resources, and evidence, further weakens the principle of equality before the law and contradicts the vision of Society 5.0, which places human dignity at the center of digital development.¹⁸

From an academic perspective, this situation reflects a largely unaddressed research gap. Most studies on personal data protection still focus on regulatory design, cybersecurity, and institutional governance.¹⁹ Conversely, empirical

¹³ Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh., Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations, *IT Research Journal*, 2024.

¹⁴ Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.23. See too, Kirsten Martin, and Katie Shilton., Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications, *Journal of the Association for Information Science and Technology*, Vol.67, no.8, 2016, page.232.

¹⁵ Mediana., There have only been three criminal cases of personal data protection violations, *Kompas.id*, August 20, 2024.

¹⁶ Umi Enggarsasi, Nur Khalimatus Sa'diyah, and Pratama Alifiandi Martio., Legal Safeguards for Victims of Data Dissemination Crimes and Cybercrime Protection, *Jurnal Hukum*, Vol.40, no.2, 2024, page.260.

¹⁷ Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.27.

¹⁸ Danielle Keats Citron, and Daniel J. Solove., Privacy harms, *BUL Rev.* no.102, 2022, page.795.

¹⁹ Andriyanto Adhi Nugroho, Atik Winanti, and Surahmad Surahmad., Personal Data Protection in Indonesia: Legal Perspective, *International Journal of Multicultural and Multireligious Understanding*, Vol.7, no.7, 2020, page.184. See too, Nawal Sholehuddin, Surianom Miskam,

studies on victims' experiences, the effectiveness of remedies, and justice outcomes are relatively limited, particularly in developing country contexts.²⁰ As a result, the realities experienced by victims have not been adequately accommodated in legal discourse.

Within the framework of Society 5.0, which emphasizes a human-centered approach, this situation poses a serious problem. When victims of personal data misuse do not receive effective remedies, the benefits of digital transformation are concentrated on institutions and corporations, while the risks are borne by individuals. This situation clearly contradicts the principles of Society 5.0, which places humans at the center of technological innovation.²¹

Therefore, this study adopts a victim-centered digital justice approach. This approach demands an adaptive legal response to technological developments such as artificial intelligence, big data, and biometric systems, which have the potential to magnify the impact of privacy violations.²² The concepts of privacy by design and legal by design are crucial to ensuring that human rights protection principles are integrated from the design stage of digital systems.²³

Furthermore, victim-centered personal data protection is closely linked to issues of digital literacy and inclusion. Research shows that groups with low levels of digital literacy tend to be more vulnerable to data misuse and have more limited access to legal redress mechanisms.²⁴ Without inclusive legal mechanisms and increased public awareness, digital transformation risks deepening structural

Farah Mohd Shahwahid, Tuan Nurhafiza Raja Abdul Aziz, and Naqibah Mansor., A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN, *Journal of Muwafaqat*, Vol.7, no.1, 2024, page.31; Colin J. Bennett, and Charles D. Raab., Revisiting the governance of privacy: Contemporary policy instruments in global perspective, *Regulation & Governance*, Vol.14, no.3, 2020, page.452.

²⁰ Linnet Taylor., What is data justice? The case for connecting digital rights and freedoms globally, *Big Data & Society*, Vol.4, no.2, 2017, page.337.

²¹ Umi Enggarsasi, Nur Khalimatus Sa'diyah, and Pratama Alifiandi Martio., Legal Safeguards for Victims of Data Dissemination Crimes and Cybercrime Protection, *Jurnal Hukum*, Vol.40, no.2, 2024, page.261.

²² Urs Gasser, and Virgilio AF Almeida., A layered model for AI governance. *IEEE Internet Computing*, Vol.21, no.6, 2017, page.59. See too, Vijay Keswani, and L. Elisa Celis., Algorithmic Fairness from the Perspective of Legal Anti-discrimination Principles, In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, vol.7, 2024, page.728.

²³ Ann Cavoukian., Privacy by design: The 7 foundational principles, *Information and privacy commissioner of Ontario, Canada*, Vol.5, no.9, 2009, page.15. Richmond Y. Wong, and Deirdre K. Mulligan., Bringing design to the privacy table: Broadening design in privacy by design through the lens of HCI. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, 2019, page.14.

²⁴ Sonia Livingstone, and Ellen Helsper., Gradations in digital inclusion: Children, young people and the digital divide, *New media & society*, Vol.9, no.4, 2007, page.677. See too, Yong Jin Park., Digital literacy and privacy behavior online, *Communication research*, Vol.40, no.2, 2013, page.222.

inequalities rather than achieving justice.²⁵

Based on these conditions, the urgency of this research lies in the real and ongoing phenomenon of rampant personal data leaks that are not accompanied by effective victim protection and redress, despite the existence of a formal legal framework. This situation raises fundamental questions about whether the personal data protection regime in Indonesia truly functions as an instrument of digital justice or is merely a symbolic norm.²⁶

Therefore, this research aims to critically examine the effectiveness of the legal framework for personal data protection in Indonesia in the era of Society 5.0, with a primary focus on victims of personal data misuse. Through an integration of normative legal analysis and empirical findings, this research seeks to identify structural weaknesses that hinder the realization of victim-oriented legal protection and formulate a more responsive and equitable model of digital justice.

Based on the description above, this study poses three research questions as follows:

1. What are the provisions and forms of legal protection for victims of personal data misuse under the Personal Data Protection Law in Indonesia in the context of Society 5.0?
2. What are the gaps between normative provisions and law enforcement practices in ensuring redress and access to justice for victims of personal data misuse?
3. How can a victim-oriented digital justice model be formulated to strengthen protection, restitution, and justice within the personal data protection regime in Indonesia?

2. Research Methods

This study uses a normative-conceptual legal research design to analyze legal protection for victims of personal data misuse in the context of digital transformation and Society 5.0. A normative approach is used to examine the substance of positive legal regulations in Indonesia, specifically Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), as the primary regime for personal data protection, including the rights of data subjects, the obligations of

²⁵ Emmy Latifah, Anis H. Bajrektarevic, and Moch Najib Imanullah., The shifting of alternative dispute resolution: From Traditional form to the online dispute resolution, *Brawijaya Law Journal*, Vol.6, no.1, 2019, page.30. See too, Sonia Livingstone, and Ellen Helsper., Gradations in digital inclusion: Children, young people and the digital divide, *New media & society*, Vol.9, no.4, 2007, page.675; Hulman Panjaitan, Junimart Girsang, Moermahadi Soerja Djanegara, and Md Hasnath Kabir Fahim., Strengthening Consumer Protection in Digital Transactions: A Legal Perspective on Click-Wrap Agreements Under the Consumer Protection Law, *Jurnal Hukum UNISSULA*, Vol.41, no.3, 2025, page.672.

²⁶ Sonia Livingstone, and Amanda Third., Children and young people's rights in the digital age: An emerging agenda. *New media & society*, Vol.19, no.5, 2017, page.660. See too, David Lyon., Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society*, Vol.1, no.2, 2014, page.205; Shoshana Zuboff., The age of surveillance capitalism, In *Social theory re-wired*, Oxfordshire, Routledge, 2023; page.208.

data controllers and processors, and administrative, civil, and criminal sanctions. The normative analysis also includes Article 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia as the constitutional basis for the protection of personal rights, the Electronic Information and Transactions (ITE) Law and its amendments through Law Number 1 of 2024, Government Regulation Number 71 of 2019 concerning the Protection of Personal Data, Article 1365 of the Civil Code concerning unlawful acts, and the National Criminal Code, effective in 2026, as a strengthening of the criminal data protection regime.

Furthermore, a conceptual approach is used to develop a victim-oriented digital justice model as an alternative normative framework to address the limitations of existing regulations. This approach refers to international principles, including the European Union's General Data Protection Regulation (GDPR) as a model for rights-based protection and victim compensation, the International Covenant on Civil and Political Rights (ICCPR) regarding the right to privacy, and the UN Basic Principles on the Right to a Remedy and Reparation (2005), which affirm victims' rights to restitution, rehabilitation, and guarantees of non-repetition. The protection of vulnerable groups, particularly children, is analyzed by referring to General Comment No. 16 of the UN Committee on the Rights of the Child.

Data analysis was conducted qualitatively and descriptively through a review of primary and secondary legal materials and practices related to personal data misuse, using deductive reasoning to formulate a legal protection model that positions victims as the primary subjects of digital justice.

3. Results and Discussion

3.1. Legal Protection for Victims under Indonesia's Personal Data Protection Law in the Society 5.0 Era

In Indonesia, the recognition of personal data as an object of legal protection is explicitly reflected in Law Number 27 of 2022 concerning Personal Data Protection (*Undang Undang Perlindungan Data Pribadi*/PDP Law).²⁷ Normatively, this law marks a significant paradigm shift from a sectoral approach to a comprehensive, rights-based data protection regime, in line with the constitutional guarantee of Article 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia, which recognizes the right to ownership and protection of individual personal rights.

Within the human-centered framework of Society 5.0, the existence of the PDP Law demonstrates the state's commitment to adapting its legal system to the

²⁷ Asep Mahbub Junaedi., Urgensi perlindungan data pribadi dalam era digital: analisis Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi, *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, Vol.5, no.2, 2025, page.251. See too, Diah Putri Hasian, and Annisa Fitria., Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome, *Arus Jurnal Sosial dan Humaniora*, Vol.5, no.2, 2025, page.423.

increasingly complex digital reality.²⁸ The PDP Law systematically regulates personal data subjects, data controllers and processors, data processing principles, consent, data subject rights, and administrative, civil, and criminal sanctions for violations. These provisions are reinforced by supporting regulations such as Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments (*Undang Undang Informasi dan Transaksi Elektronik/UU ITE*), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (*Peraturan Pemerintah Pelaksanaan Sistem dan Transaksi Elektronik/PP PSTE*), and various sectoral regulations in the fields of health, finance, and population administration.

However, when viewed from a victim protection perspective, this legal framework still exhibits structural limitations. The PDP Law was primarily designed as a regulatory and preventive instrument that emphasizes data controller compliance and breach prevention.²⁹ While it contains provisions for civil compensation and criminal sanctions, this law does not explicitly stipulate a victim recovery mechanism that is easily accessible, structured, and oriented to the victim's needs. It lacks detailed regulations regarding compensation claim procedures, psychological recovery, digital identity rehabilitation, or post-data breach restorative mechanisms.

This situation reflects a classic problem in cyber law: the legal system's tendency to treat misuse of personal data as merely an administrative or technical violation, rather than a crime that directly impacts the human rights and dignity of victims.³⁰ As a result, victims are often positioned passively as objects of normative protection, rather than as legal subjects with an active right to redress. Conceptually, the legal status of victims in cases of personal data misuse should encompass three main elements: legal recognition, access to justice, and the right to redress.³¹ In practice in Indonesia, these three elements have not been optimally integrated. The Personal Data Protection Law (PDP) does not provide an explicit definition of "victim of personal data misuse," so recognition of victim status remains implicit and dependent on the interpretation of law enforcement officials. This results in victims' limited access to redress mechanisms and participation in the legal process.

Furthermore, the criminal justice system tends to focus on perpetrators and institutional compliance, while the needs of victims are often marginalized. This

²⁸ Carolina Narvaez Rojas, Gustavo Adolfo Alomia Peñafiel, Diego Fernando Loaiza Buitrago, and Carlos Andrés Tavera Romero., Society 5.0: A Japanese concept for a superintelligent society, *Sustainability*, Vol.13, no.12, 2021, page.6569.

²⁹ Yedija Otniel Purba, and Agus Mauluddin., Kejahatan siber dan kebijakan identitas kependudukan digital: Sebuah studi tentang potensi pencurian data online, *Jurnal CIC Lembaga Riset dan Konsultan Sosial*, Vol.5, no.2, 2023, page.58.

³⁰ Richard E. Susskind., *Tomorrow's lawyers: An introduction to your future*. Oxford, Oxford University Press, 2023, page.12. See too, Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.24.

³¹ Iyaloo N. Waiganjo., and Linekela S. Nandjenda., Unveiling Insider Threats: Examining Vulnerabilities in an Organizational Structure: A Case Study of NamPost, *Open Access Library Journal*, Vol.12, no.1, 2025, page.5.

phenomenon aligns with criticisms in victimology literature that modern legal systems remain offender-oriented and inadequately accommodate the principles of victim-oriented justice.³² In the context of data crimes, the impacts experienced by victims are not only material but also include reputational damage, psychological trauma, and loss of control over digital identities.

Internationally, protection for victims of data misuse has received more progressive recognition. General Comment Number 16 The UN Committee on the Rights of the Child affirms that the protection of personal data is part of children's rights, and recognizes the potential for serious psychological and social impacts from data misuse, particularly for vulnerable groups.³³ Similar principles are also reflected in the Basic Principles and Guidelines on the Right to a Remedy and Reparation (2005), which affirms the rights of victims to compensation, rehabilitation, and guarantees of non-recurrence.

At the regional level, the European Union's General Data Protection Regulation (GDPR) explicitly recognizes the right of data breach victims to seek compensation from unlawful data controllers or processors.³⁴ While implementing this right is not always straightforward, particularly in proving non-material losses, the GDPR nonetheless represents a more victim-oriented legal model compared to many legal regimes in developing countries.³⁵

Indonesia itself has become a party to various international instruments relevant to data protection and human rights, such as the International Covenant on Civil and Political Rights (ICCPR), which guarantees the right to privacy, and various UN principles on justice for victims of crime.³⁶ However, the internalization of these principles into national law, particularly in the context of digital crime, remains partial and has not been systematically institutionalized.

In the context of Society 5.0, this limitation becomes even more problematic. Society 5.0 positions technology as a means to improve human well-being, not

³² Jonathan Doak., *Victims' rights, human rights and criminal justice: Reconceiving the role of third parties*, London, Bloomsbury Publishing, 2008, page.43. See too, Yesi Nurmantiyas Sari, Rizal Nugroho, and Al Khanif., Land acquisition for public interests: A review from the human rights context, *Indon. JLS*, Vol.1, 2020, page.23.

³³ Paula Gerber, Joanna Kyriakakis, and Katie O'Byrne., General Comment 16 on state obligations regarding the impact of the business sector on children's rights: what is its standing, meaning and effect?. *Melb. J. Int'l L.* no.14, 2013, page.93. See too, William Mougayar., *The business blockchain: promise, practice, and application of the next Internet technology*, New Jersey, John Wiley & Sons, 2016.

³⁴ Paul Voigt, and Axel Von dem Bussche., *The eu general data protection regulation (gdpr), A practical guide, 1st ed.*, Cham: Springer International Publishing, Vol.10, no.31, 2017, page.104.

³⁵ Lee Andrew Bygrave., *Data privacy law: an international perspective*, Oxford, Oxford University Press, 2014, page.23.

³⁶ Awalia Safinatunnajah, Mahrus Ali, and Papontee Teeraphan., Compliance of the Subjective Terms of Detention in Criminal Procedure with International Covenant on Civil and Political Rights, *Lex Publica*, Vol.9, no.2, 2022, page.93. See too, Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah., Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment, *Hasanuddin Law Review*, Vol.10, no.1, 2025, page.15.

merely economic efficiency. While personal data serves as a primary commodity in the digital economy, weak victim protection contradicts the vision of a human-centered society. The inability of the law to provide effective redress mechanisms has the potential to erode public trust in the state and digital institutions.³⁷

Another issue that exacerbates the plight of victims is unequal access to digital justice. Not all individuals have sufficient legal and digital literacy to recognize that they have been victims of data misuse, let alone navigate complex legal procedures.³⁸ This phenomenon has given rise to the concept of digital vulnerability, a condition of structural vulnerability experienced by certain groups due to social, economic, and technological limitations. In this context, data misuse not only causes individual harm but also deepens structural injustice.

Indonesia's national legal framework essentially provides a number of protection instruments that can be used by victims of personal data misuse. One of the most commonly used instruments is a civil lawsuit under Article 1365 of the Civil Code, which regulates unlawful acts. This article provides a legal basis for victims to claim compensation for any unlawful act that results in losses, including material and immaterial losses. However, in practice, this mechanism places the burden of proof entirely on the victim, who must prove the elements of the unlawful act, fault, loss, and causal relationship. In cases of misuse of personal data involving complex digital systems, proving the elements of fault and causal relationship becomes technically very difficult, so that protection through Article 1365 of the Civil Code is reactive, individual, and less effective as a systemic protection instrument.

In addition to civil proceedings, Law Number 27 of 2022 concerning Personal Data Protection provides provisions regarding data subject rights and administrative sanctions.³⁹ Articles 4 through 16 of the Personal Data Protection Law regulate data subject rights, including the right to information, the right to access, the right to rectification, the right to data deletion, and the right to withdraw consent. While these provisions are important in the context of preventing and correcting violations, they are primarily administrative in nature and are not directly designed as a redress mechanism for victims. The Personal Data Protection Law also stipulates the obligation to provide compensation, as stipulated in Article 58

³⁷ Jason RC. Nurse, Nikki Williams, Emily Collins, Niki Panteli, John Blythe, and Ben Koppelman., Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In *International Conference on Human-Computer Interaction*, Cham: Springer International Publishing, 2021, page.588.

³⁸ Mark Graham, and William H. Dutton., eds. *Society and the internet: How networks of information and communication are changing our lives*, Oxford, Oxford University Press, 2019, page.62. See too, Mireille Hildebrandt., *Law for computer scientists and other folk*, Oxford, Oxford University Press, 2020; Anil Jain, Ruud Bolle, and Sharath Pankanti., Introduction to biometrics. In *Biometrics: personal identification in networked society*, Boston, MA, Springer US, 2011, page.24.

³⁹ Asep Mahbub Junaedi., Urgensi perlindungan data pribadi dalam era digital: analisis Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi, *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, Vol.5, no.2, 2025, page.250. See too, Nawal Sholehuddin, Surianom Miskam, Farah Mohd Shahwahid, Tuan Nurhafiza Raja Abdul Aziz, and Naqibah Mansor., A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Pribadi di Negara-negara ASEAN, *Journal of Muwafaqat*, Vol.7, no.1, 2024, page.28.

paragraph (1), to parties who violate the law and cause losses, with dispute resolution through the courts or alternative dispute resolution methods as stipulated in Article 58 paragraph (2).⁴⁰ However, this law does not establish specific procedures for victim claims, standards for calculating losses, or the state's obligation to provide legal assistance or support to victims. The administrative sanctions stipulated in Article 57 of the Personal Data Protection Law, such as written warnings, temporary suspension of data processing, deletion of data, and administrative fines, are more oriented towards data controller compliance than towards redressing victims' rights. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions strengthens the technical obligations of electronic system administrators through Articles 14 and 15, which mandate protection of the confidentiality, integrity, and availability of personal data, as well as the implementation of system security principles. Article 20 paragraph (1) also requires notification to data owners in the event of a data breach. While these provisions are important in the context of transparency and prevention, the PP PSTE does not regulate victims' rights to compensation, rehabilitation, or other remedies.

From a criminal law perspective, the PDP Law, through Articles 67 to 73, regulates criminal sanctions for the unlawful collection, disclosure, and use of personal data. Meanwhile, Law Number 1 of 2024, as the Second Amendment to the ITE Law, affirms the protection of privacy rights in Article 26 and criminal sanctions in Articles 45 and 45A. While these criminal provisions are important for deterrence and law enforcement, their primary focus remains on punishing perpetrators, without providing restitution or criminal compensation mechanisms for victims. As a result, despite the availability of various legal instruments, victims of personal data abuse still have to rely on individual initiative to seek justice, with the burden of costs, time, and evidence often disproportionate to the losses suffered.⁴¹ Therefore, victims of data misuse must be recognized not only as victims of legal violations but also as subjects of human rights violations entitled to effective redress by the state.

3.2. The Gap between Legal Norms and Law Enforcement Practices in Personal Data Protection

Data vulnerabilities are increasing with the data-driven economy, where digital companies intensively utilize profiling and behavioral analysis techniques. These practices often create an unequal relationship between digital service providers and users, potentially violating the principles of privacy, purpose limitation, and

⁴⁰ Asep Mahbub Junaedi., Urgensi perlindungan data pribadi dalam era digital: analisis Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi, *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, Vol.5, no.2, 2025, page.254.

⁴¹ Richmond Y. Wong, and Deirdre K. Mulligan., Bringing design to the privacy table: Broadening design in privacy by design through the lens of HCI. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, 2019, page.12. See too, Linnet Taylor., What is data justice? The case for connecting digital rights and freedoms globally, *Big Data & Society*, Vol.4, no.2, 2017, page.335.

data minimization.⁴² In the context of a developing country like Indonesia, these challenges are exacerbated by the digital literacy gap, limited institutional resources, and weak data security and governance standards in many public and private institutions.⁴³ These conditions create the potential for systemic and repeated violations, particularly by entities with power over digital infrastructure.

Furthermore, the cross-border nature of data flows creates complex legal issues due to differences in data protection standards between countries and the lack of effective harmonization of international law.⁴⁴ Various digital transformation trends such as the low-security IoT, cloud computing with its risk of server misconfiguration, opaque and discriminatory AI and machine learning, and big data that can still identify individuals even after being anonymized increasingly emphasize that data protection risks are not merely technical issues, but also legal and justice issues.⁴⁵ In this situation, without an effective regulatory framework and strong law enforcement practices, victims of personal data misuse are in a

⁴² Organisation for Economic Co-operation and Development., *Digital transformation in the age of COVID-19: Building resilience and bridging divides*, OECD Policy Responses to Coronavirus COVID-19, 2020. See too, Jason RC. Nurse, Nikki Williams, Emily Collins, Niki Panteli, John Blythe, and Ben Koppelman., Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In *International Conference on Human-Computer Interaction*, Cham: Springer International Publishing, 2021, page.589. Zeynep Tufekci., Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency, *Colo. Tech. LJ* no.13, 2015, page.203.

⁴³ Ann Cavoukian., Privacy by design: The 7 foundational principles, *Information and privacy commissioner of Ontario, Canada*, Vol.5, no.9, 2009, page.12. See too, Andriyanto Adhi Nugroho, Atik Winanti, and Surahmad Surahmad., Personal Data Protection in Indonesia: Legal Perspective, *International Journal of Multicultural and Multireligious Understanding*, Vol.7, no.7, 2020, page.184. Michele De Donno, Alberto Giarretta, Nicola Dragoni, Antonio Bucchiarone, and Manuel Mazzara., Cyber-storms come from clouds: Security of cloud computing in the IoT era, *Future Internet*, Vol.11, no.6, 2019, page.128. See too, Giuseppe D'Acquisto, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, and Athena Bourka., Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics, *arXiv preprint arXiv:1512.06000* no.2, 2015, page.258.; Deni Anggreani Sutomo., The Impact of Digital Transformation on Economic Growth in Developing Countries: A Case Study of Indonesia, *Innovative: Journal Of Social Science Research*, Vol.5, no.3, 2025, page.6096.

⁴⁴ Christopher Kuner., *Transborder data flows and data privacy law*, Oxford, Oxford University Press, 2013, page.51. See too, Greenleaf, Graham., Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey, *Privacy Laws & Business International Report*, no.145, 2017, page.11.

⁴⁵ Jef Ausloos., The 'right to be forgotten'—worth remembering?, *Computer law & security review*, Vol.28, no.2, 2012, page.148. See too, Vijay Keswani, and L. Elisa Celis., Algorithmic Fairness from the Perspective of Legal Anti-discrimination Principles, In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, vol.7, 2024, page.728; Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre De Montjoye., Estimating the success of re-identifications in incomplete datasets using generative models, *Nature communications*, Vol.10, no.1, 2019, page.3071; Zahidah Mohamad Said, and Mohamad Fadli Zolkipli., Internet of Things (IoT): A Study of Security Issues and Challenges, *Int. J. Recent Contributions Eng. Sci. IT* Vol.10, no.2, 2022, page.21; Subashini, and Veeraruna Kavitha., A survey on security issues in service delivery models of cloud computing, *Journal of network and computer applications*, Vol.34, no.1, 2011, page.7.

highly vulnerable position.⁴⁶

However, personal data protection in Indonesia demonstrates a clear gap between normatively constructed legal norms (*das sollen*) and their enforcement practices (*das sein*).⁴⁷ Normatively, Indonesia already has a relatively comprehensive regulatory framework through Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), the Law on Information and Electronic Transactions and its amendments, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), as well as strengthening the criminal regime through the National Criminal Code which will be effective in 2026.⁴⁸ However, the existence of these legal instruments has not been fully implemented effectively in the practice of protecting victims of personal data misuse.

The gap in legal protection for victims of personal data breaches in Indonesia is reflected in the repeated large-scale data breach incidents in recent years. One of the most prominent cases was the 2021 BPJS Kesehatan data breach, which allegedly involved the data of more than 279 million Indonesians, which was traded on the darknet.⁴⁹ Despite this incident's widespread and systemic impact, the state's response at the time focused primarily on administrative clarification, internal audits, and official statements, without any mechanism for restitution, compensation, or digital identity rehabilitation for the victims.⁵⁰ To date, there is no systematic victim redress scheme, either in the form of compensation, continued protection from identity theft, or integrated legal assistance for the millions of affected data subjects.

Recent empirical data reinforces this situation. The CSIRT Indonesia report shows that Indonesia is among the top ten countries with the largest data breaches in the world, with nearly 94.22 million accounts compromised in 2024 alone.

⁴⁶ Desta Lesmana, Mochammad Afifuddin, and Agus Adriyanto., Challenges and cybersecurity threats in digital economic transformation, *International Journal of Humanities Education and Social Sciences*, Vol.2, no.6, 2023, page.242. See too, Eduardo Stefani, Ivanir Costa, Marcos Antonio Gaspar, Roberto de Souza Goes, Rogerio Carlos Monteiro, Breno Ribeiro Petrili, and Alexandre de Paula Pereira., Information Security Risk Framework for Digital Transformation Technologies, *Systems*, Vol.13, no.1, 2025, page.37.

⁴⁷ Sinta Dewi Rosadi., Protecting privacy on personal data in digital economic era: Legal framework in Indonesia, *Brawijaya Law Journal*, Vol.5, no.1, 2018, page.147. See too, Putu Aryan Darma Sukerta, and Andri Sutrisno., Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks, *Constitutional Law Review*, no.3, 2024, page.142.

⁴⁸ Asep Mahbub Junaedi., Urgensi perlindungan data pribadi dalam era digital: analisis Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi, *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, Vol.5, no.2, 2025, page.256.

⁴⁹ BBC Indonesia., BPJS Kesehatan: Data ratusan juta peserta diduga bocor - Otomatis yang dirugikan masyarakat, kata pakar, *BBC News Indonesia*, May 21, 2021. See too, Arundati Swastika Waranggani., Data BPJS Kesehatan Bocor, Risiko Keamanan Data Pribadi Mengancam, *Cloud Computing Indonesia*, May 25, 2021.

⁵⁰ Aditya Widya Putri., Data pribadi terserak, nasib sial masyarakat hadapi kebocoran data, *Katadata.co.id*, July 31, 2023. See too, Ahmad Wijaya., Kebocoran data jadi ancaman serius merugikan individu dan Perusahaan, *ANTARA News*, May 23, 2024.

However, criminal law enforcement for personal data protection violations remains very limited. A report noted that to date, only three criminal cases have been processed under the personal data protection regime, demonstrating a weak focus on victims' interests in law enforcement.⁵¹ This situation reveals that victims of cybercrime and personal data misuse in Indonesia generally lack effective legal protection and must pursue independent legal remedies that are expensive, complex, and difficult to access.⁵²

Normatively, the ITE Law, as most recently amended by Law Number 1 of 2024, provides a criminal legal basis for privacy violations and misuse of electronic data, specifically through Article 26, which affirms personal data protection as part of the right to privacy, and Articles 45 and 45A, which regulate criminal sanctions. Moreover, PDP Law contains provisions for administrative and criminal sanctions in Articles 57 to 71, including the threat of up to six years' imprisonment and a maximum fine of six billion rupiah. However, the effectiveness of these provisions depends heavily on the institutional capacity and courage of law enforcement to prosecute violations. On the other hand, the PP PSTE, through Articles 14 and 15, requires electronic system administrators to guarantee the security and confidentiality of personal data, and Article 20 paragraph (1) mandates notification of data breaches to data owners. While these notification provisions are important for transparency, in practice, notifications are often limited, delayed, or not accompanied by adequate information regarding the risks and remedial measures for victims.

This gap between norms and practices is also inextricably linked to the context of the rapid digital transformation. Technological developments such as the Internet of Things (IoT), cloud computing, artificial intelligence, big data analytics, and digital identity have expanded the scale and complexity of personal data processing.⁵³ Many public and private institutions in Indonesia have adopted digital technologies without adequate security system readiness, increasing the risk of data breaches due to negligence, server misconfiguration, or weak internal controls.

The digital transformation following the COVID-19 pandemic has further exacerbated these vulnerabilities. The massive digitization of the education, healthcare, banking, and public service sectors has been carried out, often without

⁵¹ Mediana., There have only been three criminal cases of personal data protection violations, *Kompas.id*, August 20, 2024.

⁵² Umi Enggarsasi, Nur Khalimatus Sa'diyah, and Pratama Alifiandi Martio., Legal Safeguards for Victims of Data Dissemination Crimes and Cybercrime Protection, *Jurnal Hukum*, Vol.40, no.2, 2024, page.264.

⁵³ Giuseppe D'Acquisto, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, and Athena Bourka., Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics, *arXiv preprint arXiv:1512.06000* no.2, 2015, page.259. See too, Michele De Donno, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone, and Manuel Mazzara., Cyber-storms come from clouds: Security of cloud computing in the IoT era, *Future Internet*, Vol.11, no.6, 2019, page.130.

comprehensive security audits.⁵⁴ This situation has led to a surge in cases of data breaches, identity theft, and misuse of personal information, which in turn exposes the imbalance between the speed of technology adoption and the readiness of legal systems and enforcement institutions.

In the context of a developing country like Indonesia, this gap is exacerbated by low digital literacy and public legal awareness.⁵⁵ Many victims are unaware that they have been subjected to a data breach or are unaware of the legal mechanisms available to pursue their rights. This situation creates what is known as digital vulnerability, a situation in which certain individuals or groups become highly vulnerable to data exploitation due to social, economic, and technological limitations.⁵⁶

Furthermore, the cross-border nature of data flows adds to the complexity of law enforcement. Many digital platforms operating in Indonesia are based overseas, giving rise to jurisdictional issues and differing data protection standards.⁵⁷ Existing regulations do not explicitly guarantee victims' rights to legal aid, compensation, and protection from re-victimization. The data breach notification provisions in the PP PSTE require notification to data owners, but in practice, this is often delayed, limited, and lacking adequate risk information and remedial measures.⁵⁸ As a result, victims remain vulnerable to identity theft, digital fraud, and post-incident psychological distress.⁵⁹ Moreover, the lack of harmony in international regulations

⁵⁴ Organisation for Economic Co-operation and Development., *Digital transformation in the age of COVID-19: Building resilience and bridging divides*, OECD Policy Responses to Coronavirus COVID-19, 2020.

⁵⁵ Andriyanto Adhi Nugroho, Atik Winanti, and Surahmad Surahmad., Personal Data Protection in Indonesia: Legal Perspective, *International Journal of Multicultural and Multireligious Understanding*, Vol.7, no.7, 2020, page.185. See too, Yong Jin Park., Digital literacy and privacy behavior online, *Communication research*, Vol.40, no.2, 2013, page.221; Giosita Kumalaratri., Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia, *Jurnal Hukum*, Vol.37, no.1, 2021, page.8.

⁵⁶ Ann Cavoukian., Privacy by design: The 7 foundational principles, *Information and privacy commissioner of Ontario, Canada*, Vol.5, no.9, 2009, page.13.

⁵⁷ Christopher Kuner., *Transborder data flows and data privacy law*, Oxford, Oxford University Press, 2013, page.52. See too, Daniel J. Solove, *The digital person: Technology and privacy in the information age*, New York, NYU Press, 2004; Greenleaf, Graham., Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey, *Privacy Laws & Business International Report*, no.145, 2017, page.12; Luyao Sun., Overview of regulations on cross border data flow, *Academic Journal of Science and Technology*, Vol.8, no.1, 2023, page.173; Joseph V. DeMarco., US Federal Trade Commission hosts public forum on facial recognition technology, 2012, page.249.

⁵⁸ Chlotia Garrison, and Clovia Hamilton., A comparative analysis of the EU GDPR to the US's breach notifications, *Information & Communications Technology Law*, Vol.28, no.1, 2019. See too, Umi Enggarsasi, Nur Khalimatus Sa'diyah, and Pratama Alifiandi Martio., Legal Safeguards for Victims of Data Dissemination Crimes and Cybercrime Protection, *Jurnal Hukum*, Vol.40, no.2, 2024, page.265.

⁵⁹ Christopher R. Sears, and Daniel R. Cunningham., Individual differences in psychological stress associated with data breach experiences, *Journal of Cybersecurity and Privacy*, Vol.4, no.3, 2024, page.612. See too, Mark Button, Dean Blackburn, Lisa Sugiura, David Shepherd, Richard

often makes national law enforcement ineffective in reaching perpetrators or data controllers located outside of Indonesia.

3.3. Developing a Victim-Centered Digital Justice Model for Personal Data Protection

A victim-centered digital justice model within Indonesia's personal data protection regime must be formulated by reorienting the legal framework around three interrelated pillars: legal recognition of victims, access to justice, and the right to redress (Table 1). These three pillars are fundamental prerequisites for transforming personal data protection from an administrative compliance regime to a rights-based justice system aligned with the human-centered values of Society 5.0.⁶⁰

The first and most fundamental pillar is legal recognition of victims. Currently, the Personal Data Protection Law (PDP Law) does not explicitly define "victims of personal data misuse." This normative gap creates ambiguity regarding who qualifies as a victim and whether aggrieved data subjects have legally enforceable rights beyond mere normative protection as data owners. In practice, victim status often depends on the interpretation of law enforcement officials or judges, resulting in inconsistent application and legal uncertainty. This lack of explicit recognition weakens victims' normative standing and hinders access to redress mechanisms, particularly in cases of large-scale data breaches impacting millions of individuals.⁶¹ Therefore, a victim-centered reformulation demands the inclusion of a clear legal definition of victims as subjects of rights, in line with international human rights standards that place recognition as a primary prerequisite for redress and reparation.⁶²

Legal recognition must also go beyond formal recognition and include meaningful victim participation in the law enforcement process. The dominance of administrative compliance-based enforcement approaches—through sanctions in the form of warnings and fines—indicates that current regulatory practices place more emphasis on institutional control than victim redress. Even when administrative sanctions are imposed, victims' rights are often not restored. This

Kapend, and Victoria Wang., Victims of cybercrime: Understanding the impact through accounts, In *Cybercrime in context: The human factor in victimization, offending, and policing*, Cham, Springer International Publishing, 2021, page.145.

⁶⁰ Carolina Narvaez Rojas, Gustavo Adolfo Alomia Peñafiel, Diego Fernando Loaiza Buitrago, and Carlos Andrés Tavera Romero., Society 5.0: A Japanese concept for a superintelligent society, *Sustainability*, Vol.13, no.12, 2021, page.6569. See too, Vivi Indra Amelia Nasution, Isna Yuliani, Tora Akadira, and Eha Saleha., Transforming Governance: Indonesia's Digital Leap, In *Proceedings of the 6th Open Society Conference (OSC 2024)*, vol.894, Berlin, Springer Nature, 2024, page.190.

⁶¹ Sinta Dewi Rosadi., Protecting privacy on personal data in digital economic era: Legal framework in Indonesia, *Brawijaya Law Journal*, Vol.5, no.1, 2018, page.147. See too, Nawal Sholehuddin, Surianom Miskam, Farah Mohd Shahwahid, Tuan Nurhafiza Raja Abdul Aziz, and Naqibah Mansor., A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN, *Journal of Muwafaqat*, Vol.7, no.1, 2024, page.33.

⁶² Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.29.

situation reinforces the perception that personal data protection is treated solely as a technical regulatory instrument, rather than a justice mechanism. This orientation contradicts the comparative privacy governance model, which emphasizes rights-based law enforcement and victim inclusion as key elements.⁶³

Table 1. Reformulation of the Legal Protection Model for Victims of Personal Data Misuse

Main Issue	Weaknesses (Regulatory or Implementation)	Impact on Victims	Required Reformulation (Victim-Oriented)
Absence of an explicit definition of victims	The Personal Data Protection Law (PDP Law) does not define "victims of personal data misuse"	Victim status is ambiguous; access to remedies depends on law enforcers' interpretation	Inclusion of an explicit legal definition of victims in the PDP Law as rights-bearing subjects
Unstructured recovery mechanisms	The PDP Law only generally regulates compensation without clear procedures	Victims must file lawsuits independently (costly and complex)	Establishment of a dedicated victim recovery mechanism (compensation, restitution, digital rehabilitation)
Heavy burden of proof in civil litigation	Article 1365 of the Indonesian Civil Code places the full burden of proof on victims	Civil lawsuits are ineffective for data-related crimes	Limited reversal of the burden of proof for large-scale data breaches
Administrative compliance-oriented enforcement	Administrative sanctions dominate (warnings, fines)	Victims' rights remain unfulfilled despite sanctions against offenders	Shift from compliance-based to rights-based enforcement
Absence of restitution in criminal law	The PDP Law and the ITE Law focus on punishment	Victims do not receive compensation	Integration of victim restitution into criminal judgments for data-related crimes
Ineffective data breach notification	Government Regulation on PSTE does not regulate notification standards or deadlines	Victims are unaware of risks and mitigation measures	Standardization of meaningful notifications (timely, risk-based, actionable)
No digital identity rehabilitation	Regulations focus solely on technical prevention	Victims are vulnerable to re-victimization	Introduction of post-breach digital identity rehabilitation schemes
Institutional fragmentation	Authorities are dispersed; no fully operational independent Data Protection Authority (DPA)	Weak and inconsistent enforcement	Acceleration of the establishment of an independent PDP Authority
Minimal law	Few cases are	Impunity for major	Prioritization of

⁶³ Colin J. Bennett, and Charles D. Raab., Revisiting the governance of privacy: Contemporary policy instruments in global perspective, *Regulation & Governance*, Vol.14, no.3, 2020, page.453.

Main Issue	Weaknesses (Regulatory or Implementation)	Impact on Victims	Required Reformulation (Victim-Oriented)
enforcement	processed despite massive violations	offenders	enforcement against systemic and large-scale violations
Victim–corporation power imbalance	Corporations dominate technology and evidence	Unequal access to justice	Mandatory digital evidence disclosure obligations for data controllers
Low digital legal literacy	No state-supported assistance for victims	Victims are unaware of their rights	Specialized legal aid schemes for data breach victims
No guarantees of non-recurrence	Law does not regulate victim-based recurrence prevention	Repeated data breaches	Integration of guarantees of non-repetition (mandatory audits, remedial orders)
Misalignment with international human rights	ICCPR principles and UN Victims’ standards are not internalized	Partial protection	Harmonization of the PDP Law with the UN Basic Principles on Remedy and Reparation
Absence of a restorative approach	The legal system is predominantly retributive	Psychological trauma remains unaddressed	Adoption of a restorative digital justice model

The second pillar, access to justice, reveals deeper structural barriers for victims of personal data misuse. One key obstacle is the lack of a structured victim redress mechanism. The PDP Law only regulates compensation in general terms without providing clear and accessible procedures. As a result, victims are forced to pursue civil lawsuits independently, which in practice is expensive, time-consuming, and technically complex. This burden becomes even more disproportionate in data breach cases involving digital infrastructure such as cloud computing and the Internet of Things, where technological complexity and the opacity of evidence are inherent.⁶⁴

This barrier to access to justice is exacerbated by the heavy burden of proof in civil lawsuits under Article 1365 of the Indonesian Civil Code, which places the entire burden of proof on the victim, including the elements of fault, damages, and causal relationships. In the context of data crimes, where evidence is controlled by corporations and the impact of losses is often immaterial, delayed, or probabilistic, this provision renders civil lawsuits ineffective. Comparative studies indicate that a limited reversal of the burden of proof in cases of large-scale or

⁶⁴ Michele De Donno, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone, and Manuel Mazzara., *Cyber-storms come from clouds: Security of cloud computing in the IoT era, Future Internet*, Vol.11, no.6, 2019, page.130. See too, Eduardo Stefani, Ivanir Costa, Marcos Antonio Gaspar, Roberto de Souza Goes, Rogerio Carlos Monteiro, Breno Ribeiro Petrili, and Alexandre de Paula Pereira., *Information Security Risk Framework for Digital Transformation Technologies, Systems*, Vol.13, no.1, 2025, page.38.

systemic data breaches is necessary to correct structural inequalities and ensure substantive equality before the law.⁶⁵

The third pillar, the right to redress, encompasses restitution, compensation, rehabilitation, satisfaction, and guarantees of non-repetition. In the Indonesian context, this pillar remains the weakest aspect. The PDP Law and the ITE Law focus more on criminal penalties and administrative sanctions, without integrating victim restitution into criminal decisions. As a result, even when perpetrators are sanctioned, victims often receive neither material nor symbolic reparations. This gap contradicts international standards on victims' rights and has the potential to erode public trust in the legal system.⁶⁶

The absence of an effective data breach notification mechanism also undermines the right to redress. The Government Regulation on Data Protection and Redress does not establish standards for the substance, deadlines, or quality of information in data breach notifications. In practice, victims are often unaware of the risks they face or the mitigation measures they can take. A comparative study of GDPR-based data protection regimes confirms that timely, risk-based, and actionable notification is a crucial foundation for victim protection and redress.⁶⁷

Furthermore, existing regulations still focus on technical prevention, neglecting post-incident redress. The absence of a digital identity rehabilitation scheme leaves victims vulnerable to revictimization, especially given the high risk of re-identification and further misuse of personal data.⁶⁸ Therefore, a victim-oriented digital justice model must include post-leak rehabilitation mechanisms, such as identity monitoring, credential replacement, and digital risk counseling.

The right to redress also requires guarantees of non-recurrence. However, positive law does not yet regulate victim-oriented recurrence prevention mechanisms. The absence of audit requirements, structural repair orders, and remedial orders allows data breaches to recur without systemic correction. Integrating non-recurrence guarantees into law enforcement is crucial for preventing future losses and restoring victims' trust in digital governance.⁶⁹

This shows that overall, the legal system's dominant retributive orientation fails to

⁶⁵ Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.31. Putu Aryan Darma Sukerta, and Andri Sutrisno., Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks, *Constitutional Law Review*, no.3, 2024, page.145.

⁶⁶ Graham Greenleaf., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report*, no.169, 2021, page.32.

⁶⁷ Chlotia Garrison, and Clovia Hamilton., A comparative analysis of the EU GDPR to the US's breach notifications, *Information & Communications Technology Law*, Vol.28, no.1, 2019.

⁶⁸ Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre De Montjoye., Estimating the success of re-identifications in incomplete datasets using generative models, *Nature communications*, Vol.10, no.1, 2019, page.3073.

⁶⁹ Colin J. Bennett, and Charles D. Raab., Revisiting the governance of privacy: Contemporary policy instruments in global perspective, *Regulation & Governance*, Vol.14, no.3, 2020, page.455.

address the psychological and social impacts experienced by victims of personal data misuse. Trauma, a sense of loss of control, and the damage to public trust are often not adequately addressed. Therefore, the application of a digital restorative justice approach is relevant, through mechanisms such as mediation, admission of guilt by the perpetrator, relationship restoration, and a commitment to system improvement. This approach aligns with the development of digital dispute resolution models and a human-centered justice paradigm.⁷⁰

Thus, strengthening the protection of victims of personal data abuse in Indonesia's legal regime requires a reformulation that is firmly victim-oriented, integrating legal recognition, access to justice, and the right to redress into normative design and law enforcement practices. The first fundamental reformulation is the inclusion of an explicit definition of victims of personal data abuse in the Personal Data Protection Law (PDP Law). This definition must position victims as legal subjects and subjects of rights, not merely objects of administrative protection. This recognition aligns with the principles of the UN General Assembly Resolution 60/147, the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, which emphasize that recognition of victim status is a prerequisite for access to effective redress.⁷¹

The next reformulation is the establishment of a specific, structured, and accessible victim redress mechanism, encompassing compensation, restitution, and digital identity rehabilitation. Reliance on individual civil lawsuits is inadequate to address large-scale data breaches with collective impacts, as seen in the BPJS Kesehatan case, which harmed hundreds of millions of Indonesians.⁷² Therefore, a recovery mechanism needs to be designed as a dedicated, accessible scheme without excessive costs and technical burdens, as recommended in international cybercrime victim protection practices.⁷³

To strengthen access to justice, a limited reversal of the burden of proof is

⁷⁰ Emmy Latifah, Anis H. Bajrektarevic, and Moch Najib Imanullah., The shifting of alternative dispute resolution: From Traditional form to the online dispute resolution, *Brawijaya Law Journal*, Vol.6, no.1, 2019, page.30. See too, Sonia Livingstone, and Amanda Third., Children and young people's rights in the digital age: An emerging agenda, *New media & society*, Vol.19, no.5, 2017, page.663.

⁷¹ Theo Van Boven., Victims' Rights to a Remedy and Reparation: The United Nations Principles and Guidelines, In *Reparations for Victims of Genocide, War Crimes and Crimes against Humanity*, Leiden, Brill Nijhoff, 2020, page.21. See too, Theo Van Boven., The United Nations basic principles and guidelines on the right to a remedy and reparation for victims of gross violations of international human rights law and serious violations of international humanitarian law, *United Nations Audiovisual Library of International Law* no. 7, 2010; E. Christine Evans., *The right to reparation in international law for victims of armed conflict*, No. 91. Cambridge, Cambridge University Press, 2012.

⁷² BBC Indonesia., BPJS Kesehatan: Data ratusan juta peserta diduga bocor - Otomatis yang dirugikan masyarakat, kata pakar, *BBC News Indonesia*, May 21, 2021. See too, Arundati Swastika Waranggani., Data BPJS Kesehatan Bocor, Risiko Keamanan Data Pribadi Mengancam, *Cloud Computing Indonesia*, May 25, 2021.

⁷³ Mark Button, Dean Blackburn, Lisa Sugiura, David Shepherd, Richard Kapend, and Victoria Wang., Victims of cybercrime: Understanding the impact through accounts, In *Cybercrime in context: The human factor in victimization, offending, and policing*, Cham, Springer International Publishing, 2021, page.147.

necessary in cases of large and systemic data breaches. In the context of data crimes, it is nearly impossible for victims to prove technical errors and causality that are entirely within the control of the data controller. This approach aligns with developments in comparative data protection law that recognize the structural inequalities between victims and digital corporations.⁷⁴ This reformulation must also be supported by mandatory disclosure of digital evidence by data controllers to ensure procedural equality and prevent corporate impunity.

Law enforcement also needs to be reoriented from an administrative compliance-based approach to rights-based enforcement. Administrative sanctions alone are insufficient without restitution of victims' rights. Therefore, victim restitution must be explicitly integrated into criminal decisions for data crimes, so that punishment serves not only a repressive but also a restorative function. This model is consistent with the victim justice approach in international law and the practice of protecting cybercrime victims.⁷⁵

Another important reform is the standardization of meaningful data breach notifications, which should be timely, risk-based, and actionable by victims. Notifications should include information about potential impacts, mitigation measures, and victims' rights to redress. This practice has become standard practice in the GDPR regime and has been shown to increase victims' capacity to protect themselves from further harm.⁷⁶ Effective notifications should also be accompanied by a post-breach digital identity rehabilitation scheme, given the high risk of re-victimization and psychological distress resulting from the loss of control over digital identities.⁷⁷

From an institutional perspective, reformulation requires accelerating the establishment and strengthening of an independent Personal Data Protection Authority, with a mandate not only to oversee compliance but also to facilitate complaints, provide victim redress, and provide strategic law enforcement against systemic violations. Comparative studies have shown that the existence of an independent authority is a key element in the effectiveness of data protection

⁷⁴ Colin J. Bennett, and Charles D. Raab., Revisiting the governance of privacy: Contemporary policy instruments in global perspective, *Regulation & Governance*, Vol.14, no.3, 2020, page.456. See too, Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh., Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations, *IT Research Journal*, 2024.

⁷⁵ United Nations Office on Drugs and Crime., Good practices in protecting victims of cybercrime, *United Nations Office on Drugs and Crime*, 2020. See too, Umi Enggarsasi, Nur Khalimatus Sa'diyah, and Pratama Alifiandi Martio., Legal Safeguards for Victims of Data Dissemination Crimes and Cybercrime Protection, *Jurnal Hukum*, Vol.40, no.2, 2024, page.266.

⁷⁶ Chlotia Garrison, and Clovia Hamilton., A comparative analysis of the EU GDPR to the US's breach notifications, *Information & Communications Technology Law*, Vol.28, no.1, 2019.

⁷⁷ Christopher R. Sears, and Daniel R. Cunningham., Individual differences in psychological stress associated with data breach experiences, *Journal of Cybersecurity and Privacy*, Vol.4, no.3, 2024, page.614. See too, Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre De Montjoye., Estimating the success of re-identifications in incomplete datasets using generative models, *Nature communications*, Vol.10, no.1, 2019, page.3075.

regimes.⁷⁸ These authorities must also prioritize law enforcement against major and repeated violations to create a deterrent effect and prevent systemic data breaches.

Victim-oriented reforms also require the provision of specialized legal assistance for data breach victims, especially those with low legal and digital literacy. Without state support, victims' rights risk becoming a normative illusion. Furthermore, guarantees of non-recurrence must be integrated through mandatory audits, remedial orders, and remedial orders as part of legal decisions, so that victim protection extends beyond compensation to prevention.

Finally, this overall reformulation must be framed within a digital restorative justice approach, which recognizes the psychological, social, and collective impacts of personal data misuse. This approach enables a more humane recovery and aligns with the vision of data justice and Society 5.0, which positions technology as a means of human well-being, not a source of new vulnerabilities.⁷⁹

4. Conclusion

This research finds that the Personal Data Protection (PDP) legal framework in Indonesia still exhibits structural gaps in positioning victims as legal subjects entitled to real redress. First, normatively, the PDP Law does not explicitly define victims of personal data breaches as rights-bearing subjects, so the rights to restitution, compensation, and digital rehabilitation have not been systematically integrated into law enforcement mechanisms. This results in fragmented victim protection and reliance on other legal instruments that are not specific to data crimes.

Second, in terms of implementation, the law enforcement approach remains predominantly compliance-based, rather than rights-based enforcement. The findings indicate that despite the increase in large-scale data breach incidents, the state's response remains focused on administrative sanctions against data controllers, without ensuring the psychological, economic, and digital identity recovery of victims. The absence of a limited reversal of the burden of proof scheme and the minimal obligation to disclose digital evidence weaken victims' positions in the legal process. Third, it confirms that the absence of an independent PDP authority and the slow integration of international principles, particularly the UN Basic Principles on Remedy and Reparation, hinder the development of a restorative digital justice model. Victims have not received guarantees of non-repetition, meaningful notification, or sustainable post-incident rehabilitation.

⁷⁸ I. Gusti Ngurah Parikesit Widiatedja, and Neha Mishra., Establishing an independent data protection authority in Indonesia: a future-forward perspective, *International Review of Law, Computers & Technology*, Vol.37, no.3, 2023, page.344. See too, Firsta Rahadatul 'Aisy, Muhammad Azil Maskur, and A.M Adzkiya' Amiruddin., Establishing Indonesia's personal data protection agency: Comparative administrative sanctions enforcement from Ireland, Australia, and Singapore, *Journal of Indonesian Legal Studies*, Vol.10, no.1, 2025, page.452.

⁷⁹ Linnet Taylor., What is data justice? The case for connecting digital rights and freedoms globally, *Big Data & Society*, Vol.4, no.2, 2017, page.338. See too, Carolina Narvaez Rojas, Gustavo Adolfo Alomia Peñafiel, Diego Fernando Loaiza Buitrago, and Carlos Andrés Tavera Romero., Society 5.0: A Japanese concept for a superintelligent society, *Sustainability*, Vol.13, no.12, 2021, page.6570.

Theoretically, these findings reinforce the urgency of a paradigm shift from data protection as compliance to data protection as victim-centered justice, in line with the concepts of data justice and restorative digital justice. Practically, this research implies the need to reformulate the Personal Data Protection Law through the integration of restitution into criminal decisions, the establishment of victim recovery mechanisms, the acceleration of independent Personal Data Protection authorities, and harmonization with international human rights standards. Thus, personal data protection not only prevents violations but also fully restores victims' dignity and rights.

References

Books:

- Button, Mark, Dean Blackburn, Lisa Sugiura, David Shepherd, Richard Kapend, and Victoria Wang., Victims of cybercrime: Understanding the impact through accounts. In *Cybercrime in context: The human factor in victimization, offending, and policing*, Cham: Springer International Publishing, 2021;
- Bygrave, Lee Andrew., *Data privacy law: an international perspective*. Oxford, Oxford University Press, 2014;
- Doak, Jonathan., *Victims' rights, human rights and criminal justice: Reconceiving the role of third parties*. London, Bloomsbury Publishing, 2008;
- Evans, E. Christine., *The right to reparation in international law for victims of armed conflict*. No. 91. Cambridge: Cambridge University Press, 2012;
- Graham, Mark, and William H. Dutton., eds. *Society and the internet: How networks of information and communication are changing our lives*. Oxford, Oxford University Press, 2019;
- Hildebrandt, Mireille., *Law for computer scientists and other folk*. Oxford, Oxford University Press, 2020;
- Jain, Anil, Ruud Bolle, and Sharath Pankanti., Introduction to biometrics. In *Biometrics: personal identification in networked society*. Boston, MA: Springer US, 2011;
- Kuner, Christopher., *Transborder data flows and data privacy law*. Oxford, Oxford University Press, 2013;
- Mougayar, William., *The business blockchain: promise, practice, and application of the next Internet technology*. New Jersey, John Wiley & Sons, 2016;
- Solove, Daniel J., *The digital person: Technology and privacy in the information age*. New York, NYU Press, 2004;
- Susskind, Richard E., *Tomorrow's lawyers: An introduction to your future*. Oxford, Oxford University Press, 2023;

- Van Boven, Theo., Victims' Rights to a Remedy and Reparation: The United Nations Principles and Guidelines. In *Reparations for Victims of Genocide, War Crimes and Crimes against Humanity*. Leiden, Brill Nijhoff, 2020;
- Voigt, Paul, and Axel Von dem Bussche., The eu general data protection regulation (gdpr). *A practical guide, 1st ed.*, Cham, Springer International Publishing Vol.10, no.315, 2017;
- Zuboff, Shoshana., The age of surveillance capitalism. In *Social theory re-wired*. Oxfordshire, Routledge, 2023;

Journals:

- 'Aisy, Firsta Rahadatul, Muhammad Azil Maskur, and A.M Adzkiya' Amiruddin., Establishing Indonesia's personal data protection agency: Comparative administrative sanctions enforcement from Ireland, Australia, and Singapore. *Journal of Indonesian Legal Studies* Vol.10, no.1, 2025;
- Ausloos, Jef., The 'right to be forgotten'—worth remembering? *Computer law & security review* Vol.28, no.2, 2012; <https://doi.org/10.1016/j.clsr.2012.01.006>;
- Bachura, Eric, Rohit Valecha, Rui Chen, and H. Raghav Rao., The OPM data breach: An investigation of shared emotional reactions on Twitter. *MIS quarterly* Vol.46, no.2, 2022; <https://doi.org/10.25300/MISQ/2022/15596>
- Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh., Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. *IT Research Journal*, 2024; DOI:10.51594/csitrj.v5i3.859;
- Bennett, Colin J., and Charles D. Raab., Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance* Vol.14, no.3, 2020; <https://doi.org/10.1111/rego.12222>;
- Cavoukian, Ann., Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada* Vol.5, no.9, 2009;
- Cech, Florian, and Hilda Tellioglu., Impact of the digital transformation: an online real-time delphi study. *arXiv preprint arXiv:1904.11411* no.1, 2019; <https://doi.org/10.48550/arXiv.1904.11411>;
- Citron, Danielle Keats, and Daniel J. Solove., Privacy harms. *BUL Rev.* no.102, 2022;
- D'Acquisto, Giuseppe, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, and Athena Bourka., Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. *arXiv preprint arXiv:1512.06000* no.2, 2015; <https://doi.org/10.2824/641480>;
- De Donno, Michele, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone, and Manuel Mazzara., Cyber-storms come from clouds: Security of cloud computing in the IoT era. *Future Internet* Vol.11, no.6, 2019;

- <https://doi.org/10.3390/fi11060127>;
- DeMarco, Joseph V., US Federal Trade Commission hosts public forum on facial recognition technology. 2012; <https://doi.org/10.1016/j.clsr.2012.01.010>;
- Enggarsasi, Umi, Nur Khalimatus Sa'diyah, and Pratama Alifiandi Martio., Legal Safeguards for Victims of Data Dissemination Crimes and Cybercrime Protection. *Jurnal Hukum* Vol.40, no.2, 2024; <https://dx.doi.org/10.26532/jh.v40i2.39974>;
- Garrison, Chlotia, and Clovia Hamilton., A comparative analysis of the EU GDPR to the US's breach notifications. *Information & Communications Technology Law* Vol.28, no.1, 2019; <https://doi.org/10.1080/13600834.2019.1571473>;
- Gasser, Urs, and Virgilio AF Almeida., A layered model for AI governance. *IEEE Internet Computing* Vol.21, no.6, 2017;
- Gerber, Paula, Joanna Kyriakakis, and Katie O'Byrne., General Comment 16 on state obligations regarding the impact of the business sector on children's rights: what is its standing, meaning and effect?. *Melb. J. Int'l L.* no.14, 2013; DOI:10.1109/MIC.2017.4180835;
- Greenleaf, Graham., Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report* no.145, 2017;
- Greenleaf, Graham., Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. *Privacy Laws & Business International Report* no.169, 2021;
- Hasian, Diah Putri, and Annisa Fitria., Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome. *Arus Jurnal Sosial dan Humaniora* Vol.5, no.2, 2025; <https://doi.org/10.57250/ajsh.v5i2.1440>;
- Junaedi, Asep Mahbub., Urgensi perlindungan data pribadi dalam era digital: analisis Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan* Vol.5, no.2, 2025; <https://doi.org/10.51878/knowledge.v5i2.5269>;
- Kumalaratri, Giosita., Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia. *Jurnal Hukum* Vol.37, no.1, 2021;
- Latifah, Emmy, Anis H. Bajrektarevic, and Moch Najib Imanullah., The shifting of alternative dispute resolution: From Traditional form to the online dispute resolution. *Brawijaya Law Journal* Vol.6, no.1, 2019;
- Lesmana, Desta, Mochammad Afifuddin, and Agus Adriyanto., Challenges and cybersecurity threats in digital economic transformation. *International Journal of Humanities Education and Social Sciences (IJHESS)* Vol.2, no.6,

2023;

- Livingstone, Sonia, and Amanda Third., Children and young people's rights in the digital age: An emerging agenda. *New media & society* Vol.19, no.5, 2017; <https://doi.org/10.1177/1461444816686318> ;
- Livingstone, Sonia, and Ellen Helsper., Gradations in digital inclusion: Children, young people and the digital divide. *New media & society* Vol.9, no.4, 2007; <https://doi.org/10.1177/1461444807080335>;
- Lyon, David., Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society* Vol.1, no.2, 2014; <https://doi.org/10.1177/2053951714541861>;
- Martin, Kirsten, and Katie Shilton., Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology* Vol.67, no.8, 2016; <https://doi.org/10.1002/asi.23500>;
- Narvaez Rojas, Carolina, Gustavo Adolfo Alomia Peñafiel, Diego Fernando Loaiza Buitrago, and Carlos Andrés Tavera Romero., Society 5.0: A Japanese concept for a superintelligent society. *Sustainability* Vol.13, no.12, 2021; <https://doi.org/10.3390/su13126567>;
- Nugroho, Andriyanto Adhi, Atik Winanti, and Surahmad Surahmad., Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding* Vol.7, no.7, 2020;
- Panjaitan, Hulman, Junimart Girsang, Moermahadi Soerja Djanegara, and Md Hasnath Kabir Fahim., Strengthening Consumer Protection in Digital Transactions: A Legal Perspective on Click-Wrap Agreements Under the Consumer Protection Law. *Jurnal Hukum UNISSULA* Vol.41, no.3, 2025; <https://dx.doi.org/10.26532/jh.v41i3.47262>;
- Park, Yong Jin., Digital literacy and privacy behavior online. *Communication research* Vol.40, no.2, 2013; <https://doi.org/10.1177/0093650211418338>;
- Purba, Yedija Otniel, and Agus Mauluddin., Kejahatan siber dan kebijakan identitas kependudukan digital: Sebuah studi tentang potensi pencurian data online. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial* Vol.5, no.2, 2023; <https://doi.org/10.51486/jbo.v5i2.113>;
- Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre De Montjoye., Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications* Vol.10, no.1, 2019; <https://doi.org/10.1038/s41467-019-10933-3>;
- Rosadi, Sinta Dewi., Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal* Vol.5, no.1, 2018;
- Safinatunnajah, Awalia, Mahrus Ali, and Papontee Teeraphan., Compliance of the Subjective Terms of Detention in Criminal Procedure with International Covenant on Civil and Political Rights. *Lex Publica* Vol.9, no.2, 2022; <https://doi.org/10.58829/lp.9.2.2022.88-101>;
- Said, Zahidah Mohamad, and Mohamad Fadli Zolkipli., Internet of Things (IoT): A

- Study of Security Issues and Challenges. *Int. J. Recent Contributions Eng. Sci. IT* Vol.10, no.2, 2022; <https://doi.org/10.3991/ijes.v10i02.29301>;
- Sari, Yesi Nurmantiyas, Rizal Nugroho, and Al Khanif., Land acquisition for public interests: A review from the human rights context. *Indon. JLS* Vol.1 2020; 23;
- Sears, Christopher R., and Daniel R. Cunningham., Individual differences in psychological stress associated with data breach experiences. *Journal of Cybersecurity and Privacy* Vol.4, no.3, 2024; <https://doi.org/10.3390/jcp4030028>;
- Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah., Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review* Vol.10, no.1, 2025; DOI:10.20956/halrev.v10i1.5016;
- Sholehuddin, Nawal, Surianom Miskam, Farah Mohd Shahwahid, Tuan Nurhafiza Raja Abdul Aziz, and Naqibah Mansor., A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perbandingan Perbandingan Undang-undang Perlindungan Data Pribadi di Negara-negara ASEAN. *Journal of Muwafaqat* Vol.7, no.1, 2024; <https://doi.org/10.53840/muwafaqat.v7i1.166>;
- Spanca, Fiona, and Armend Salihu. "Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age." In *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*. New York, IEEE, 2024;
- Stefani, Eduardo, Ivanir Costa, Marcos Antonio Gaspar, Roberto de Souza Goes, Rogerio Carlos Monteiro, Breno Ribeiro Petrili, and Alexandre de Paula Pereira., Information Security Risk Framework for Digital Transformation Technologies. *Systems* Vol.13, no.1, 2025; <https://doi.org/10.3390/systems13010037>;
- Subashini, Subashini, and Veeraruna Kavitha., A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications* Vol.34, no.1, 2011; <https://doi.org/10.1016/j.jnca.2010.07.006>;
- Sukerta, Putu Aryan Darma, and Andri Sutrisno., Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks. *Constitutional Law Review* no.3, 2024; <https://doi.org/10.30863/clr.v3i2.5605>;
- Sun, Luyao., Overview of regulations on cross border data flow. *Academic Journal of Science and Technology* Vol.8, no.1, 2023;
- Sutomo, Deni Anggreani., The Impact of Digital Transformation on Economic Growth in Developing Countries: A Case Study of Indonesia. *Innovative: Journal Of Social Science Research* Vol.5, no.3, 2025;

<https://doi.org/10.31004/innovative.v5i3.19670>;

Taylor, Linnet., What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* Vol.4, no.2, 2017; <https://doi.org/10.1177/2053951717736335>;

Tene, Omer, and Jules Polonetsky., Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.* Vol.11, no.2, 2012;

Tufekci, Zeynep., Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ* no.13, 2015;

Van Boven, Theo., The United Nations basic principles and guidelines on the right to a remedy and reparation for victims of gross violations of international human rights law and serious violations of international humanitarian law. *United Nations Audiovisual Library of International Law* no. 7, 2010;

Waiganjo, Iyaloo N., and Linekela S. Nandjenda., Unveiling Insider Threats: Examining Vulnerabilities in an Organizational Structure: A Case Study of NamPost. *Open Access Library Journal* Vol.12, no.1, 2025;

Widiatedja, I. Gusti Ngurah Parikesit, and Neha Mishra., Establishing an independent data protection authority in Indonesia: a future-forward perspective. *International Review of Law, Computers & Technology* Vol.37, no.3, 2023; <https://doi.org/10.1080/13600869.2022.2155793>;

Report:

Bhatt, Charukeshi, and Anirudh Burman., Data Protection Regulation in the Global South. *Carnegie Endowment for International Peace*, February 21, 2024; <https://carnegieendowment.org/posts/2024/02/data-protection-regulation-in-the-global-south?lang=en>. Accessed October 2, 2025;

Organisation for Economic Co-operation and Development., *Digital transformation in the age of COVID-19: Building resilience and bridging divides*. OECD Policy Responses to Coronavirus COVID-19, 2020, <https://img.lalr.co/cms/2020/11/27173400/digital-economy-outlook-covid.pdf>. Accessed September 27, 2025;

Tisné, Martin., The Data Delusion: Protecting Individual Data Isn't Enough When the Harm Is Collective. Edited by Marietje Schaake. Luminare, July 2020. <https://luminaregroup.com/storage/1023/The-Data-Delusion---July-2020.pdf>. Accessed October 2, 2025;

UNESCO., Japan Pushing Ahead with Society 5.0 to Overcome Chronic Social Challenges, *UNESCO*, February 21, 2019. <https://www.unesco.org/en/articles/japan-pushing-ahead-society-50-overcome-chronic-social-challenges>, Accessed October 2, 2025;

United Nations Office on Drugs and Crime., *Good practices in protecting victims of cybercrime*. United Nations Office on Drugs and Crime, 2020. <https://www.unodc.org/>. Accessed October 2, 2025;

Waranggani, Arundati Swastika. Data BPJS Kesehatan Bocor, Risiko Keamanan

Data Pribadi Mengancam. *Cloud Computing Indonesia*. May 25, 2021. <https://event.cloudcomputing.id/berita/data-bpjs-kesehatan-bocor-ancam-masyarakat>. Accessed October 2, 2025;

Website:

Aditya Widya Putri., Data pribadi terserak, nasib sial masyarakat hadapi kebocoran data. *Katadata.co.id*. July 31, 2023. <https://katadata.co.id/indepth/telaah/64c725ca09e2e/data-pribadi-terserak-nasib-sial-masyarakat-hadapi-kebocoran-data>. Accessed October 2, 2025;

BBC Indonesia, BPJS Kesehatan: Data ratusan juta peserta diduga bocor - Otomatis yang dirugikan masyarakat, kata pakar, *BBC News Indonesia*, May 21, 2021, <https://www.bbc.com/indonesia/indonesia-57196905>. Accessed October 2, 2025;

Mediana., There have only been three criminal cases of personal data protection violations. *Kompas.id*. August 20, 2024. <https://www.kompas.id/artikel/en-baru-ada-tiga-kasus-pidana-pelanggaran-pelindungan-data-pribadi>. Accessed October 2, 2025;

Puspita Sari, Rita., RI masuk 10 besar kebocoran data, hampir 94,22 juta akun bocor. *CSIRT Indonesia*. November 29, 2024. <https://csirt.or.id/berita/ri-masuk-10-besar-kebocoran-data>. Accessed October 2, 2025;

Wijaya, Ahmad., Kebocoran data jadi ancaman serius merugikan individu dan perusahaan. *ANTARA News*. May 23, 2024. <https://www.antaranews.com/berita/4118397/kebocoran-data-jadi-ancaman-serius-merugikan-individu-dan-perusahaan>. Accessed October 2, 2025;

Proceedings:

Keswani, Vijay, and L. Elisa Celis., Algorithmic Fairness from the Perspective of Legal Anti-discrimination Principles. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, vol.7, 2024;

Nasution, Vivi Indra Amelia, Isna Yuliani, Tora Akadira, and Eha Saleha., Transforming Governance: Indonesia's Digital Leap. In *Proceedings of the 6th Open Society Conference (OSC 2024)*. vol. 894. Berlin, Springer Nature, 2024;

Nurse, Jason RC, Nikki Williams, Emily Collins, Niki Panteli, John Blythe, and Ben Koppelman., Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In *International Conference on Human-Computer Interaction*. Cham, Springer International Publishing, 2021;

Wong, Richmond Y., and Deirdre K. Mulligan., Bringing design to the privacy table: Broadening design in privacy by design through the lens of HCI. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, 2019.