

LEGAL PROTECTION AGAINST DIGITAL VICTIMIZATION: ALIGNING INDONESIA'S NATIONAL SECURITY LAWS WITH GLOBAL PRIVACY STANDARDS

^{1*} Indah Sri Utari, ^{1,2} Muhammad Azil Maskur, ^{1,3} Ridwan Arifin, ⁴ Christina Noelia Umbría

¹Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

²Faculty of Law, Universitas Diponegoro, Semarang, Indonesia

³Faculty of Law, Universitat de Barcelona, Barcelona, Spain

⁴Sociedad Civil de Derecho y Políticas Públicas (SOCIPOL), Barcelona, Spain

*Corresponding author: indahsuji@mail.unnes.ac.id

Abstract

The rapid digital transformation has fundamentally reshaped the concept of national sovereignty, shifting security concerns from territorial boundaries toward the borderless domain of cyberspace. Indonesia's increasing dependence on digital infrastructure has generated significant opportunities for economic and social development while simultaneously exposing citizens and state institutions to emerging forms of digital victimization, including data breaches, ransomware attacks, cyber harassment, and unauthorized personal data exploitation. The 2024 ransomware attack on the National Data Center (Pusat Data Nasional/PDN) illustrates the structural vulnerabilities of Indonesia's cyber governance, revealing gaps between legal frameworks, institutional capacity, and operational resilience. This study aims to examine Indonesia's legal and institutional framework for addressing digital victimization by analyzing the alignment between Law No. 27 of 2022 on Personal Data Protection (PDP Law) and international data protection standards, particularly the European Union General Data Protection Regulation (GDPR). This research employs a doctrinal legal method with comparative and case study approaches. Secondary data consisting of legislation, international instruments, academic literature, and government reports are analyzed qualitatively through legal interpretation and content analysis. The findings reveal that although the PDP Law represents a significant advancement toward comprehensive data protection, substantial challenges remain regarding institutional independence, enforcement mechanisms, national security exemptions, and inter-agency coordination. Through the perspectives of Routine Activity Theory, Rational Choice Theory, and victimology, this study demonstrates that digital victimization results not only from technological weaknesses but also from insufficient guardianship and fragmented governance structures. This research proposes a harmonization model integrating stronger victim protection mechanisms, accountable cybersecurity governance, judicial oversight of state data access, and institutional reforms to strengthen Indonesia's digital resilience. The study argues that personal data protection should be positioned as a fundamental component of national security rather than merely an administrative obligation.

Keywords: *Digital Victimization; Personal Data Protection Law; Data Privacy; National Security Standard; Legal Harmonization.*

Received: 14 February 2026; Revised: 19 October 2026; Accepted: 20 October 2026; Available online: 30 October 2026; Published: 30 October 2026.

How to Cite: Utari, Indah Sri, Muhammad Azil Maskur, Ridwan Arifin, and Christina Noelia Umbría. "Legal Protection Against Digital Victimization: Aligning Indonesia's National Security Laws with Global Privacy Standards." *Diponegoro Law Review* 11, no. 2 (2026): 225–59. <https://doi.org/10.14710/dilrev.11.2.2026.225-259>.

Copyright © Diponegoro Law Review. Published by the Faculty of Law, Universitas Diponegoro. This is an open-access article under the CC-BY-NC-SA License. (<https://creativecommons.org/licenses/by-nc-sa/4.0/>)

1. Introduction

The contemporary era has fundamentally challenged the traditional Westphalian concept of sovereignty. Once defined strictly by physical borders and territorial integrity, national sovereignty is now contested within the intangible frontier of cyberspace.¹ As nations undergo rapid digital transformation, the “surface area” for digital victimization has expanded exponentially. This evolution transcends individual grievances, elevating cyber-vulnerability to a matter of paramount national security.² For Indonesia, as the world's fourth most populous nation and a critical hub for Southeast Asia's digital economy, this presents a paradox: while digitalization fuels unprecedented economic growth, it also exposes the state to sophisticated threats that operate beyond the reach of conventional law enforcement.³

This rapid expansion of digital technologies has transformed social, economic, and political life, yet it has concurrently birthed new vulnerabilities. Indonesia, like many emerging economies, faces escalating risks of digital victimization, including systemic data breaches, ransomware assaults, and cross-border cyber fraud.⁴ The gravity of these threats was starkly illustrated in June 2024, when a massive ransomware attack on the National Data Center (Pusat Data Nasional [PDN])⁵ disrupted essential immigration and education services. This incident exposed millions of civil servant and taxpayer records, highlighting the fragility of the national cyber defense ecosystem and raising urgent questions regarding the adequacy of existing governance mechanisms.

The scale of this challenge is further underscored by data from the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara [BSSN]), which recorded nearly one billion traffic anomalies in recent years. These range from automated ransomware probes to highly targeted

¹ Simona Țuțuianu, *Towards Global Justice: Sovereignty in an Interdependent World* (T.M.C. Asser Press The Hague, 2012), <https://doi.org/10.1007/978-90-6704-891-0>; Luke Glanville, “The Myth of ‘Traditional’ Sovereignty,” *International Studies Quarterly* 57, no. 1 (2013): 79–90, <https://doi.org/10.1111/isqu.12004>.

² Paul Cornish, ed., *The Oxford Handbook of Cyber Security* (Oxford Academic, 2021), <https://doi.org/10.1093/oxfordhb/9780198800682.001.0001>; Scott J. Shackelford, “The Law of Cyber Peace,” *Chicago Journal of International Law* 18, no. 1 (2017), <https://cjl.uchicago.edu/print-archive/law-cyber-peace>.

³ Dea Melati, “Implementation of Digital Governance in Improving Cyber Security in Indonesia,” *Journal of Law, Social Science and Humanities* 2, no. 2 (2025): 379–90, <https://myjournal.or.id/index.php/JLSSH/article/view/347>; Sarah Safira Aulianisa and Indirwan Indirwan, “Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia,” *Lex Scientia Law Review* 4, no. 1 (2020): 31–45, <https://doi.org/10.15294/lesrev.v4i1.38197>; Rudy Cahya Kurniawan, “Enhancing Cybercrime Response Capabilities through Integrated Digital Policing Systems,” *Jurnal Scientia Indonesia* 9, no. 2 (2025): 41–48, <https://doi.org/10.15294/scientia.v9i2.37964>.

⁴ Muhlis Hafel, “Digital Transformation in Politics and Governance in Indonesia: Opportunities and Challenges in the Era of Technological Disruption,” *Society* 11, no. 2 (2023): 742–57, <https://doi.org/10.33019/society.v11i2.577>; Thomas Paterson, “Indonesian Cyberspace Expansion: A Double-Edged Sword,” *Journal of Cyber Policy* 4, no. 2 (2019): 216–34, <https://doi.org/10.1080/23738871.2019.1627476>.

⁵ In June 2024, Indonesia suffered a major ransomware attack on its National Data Center infrastructure, specifically targeting the Temporary National Data Centre (Pusat Data Nasional Sementara, PDNS) operations in Surabaya. Hackers deployed a new variant of LockBit 3.0 ransomware called “Brain Cipher,” which encrypted data and disrupted services for over 200 central and regional government institutions. Key public systems, including immigration checks at airports, visa and passport services, investment licensing, and other digital government services, were crippled when the malware locked them and made them inaccessible. The attackers demanded a ransom of about \$8 million (≈ Rp 131 billion) for decryption, but the Indonesian government publicly refused to pay and focused on recovery and data migration to unaffected systems. The incident highlighted weaknesses in national cybersecurity and put pressure on authorities to strengthen protections for critical digital infrastructure. See Reuters, “Cyber Attack Compromised Indonesia Data Centre, Ransom Sought,” *Reuters*, June 24, 2024, <https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/>.

Advanced Persistent Threats (APTs). These high-profile breaches involving state-owned enterprises and sensitive government databases are not merely isolated technical failures; they are symptoms of a systemic gap in the nation's cyber defense architecture.⁶ Consequently, the protection of personal data must be viewed through the lens of national resilience rather than as a secondary administrative requirement.

On the global stage, Indonesia's internal struggles reflect a broader "Cyber Cold War."⁷ As global powers weaponize data and utilize cyber espionage as a primary tool of statecraft, developing nations often find themselves caught in the crossfire of geopolitical digital maneuvers. The enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law) marked a significant legislative milestone, theoretically aligning Indonesia's domestic framework with international standards, including the EU's General Data Protection Regulation (GDPR). However, the transition from legislative intent to operational resilience remains fraught with hurdles, including limited cybersecurity literacy and the rapid pace of technological innovation outstripping regulatory cycles.⁸

Legal protection against digital victimization in Indonesia has become an increasingly important issue due to the rapid expansion of digital communication and social media platforms. Various cases demonstrate how individuals can become victims of online harassment, cyberbullying, privacy violations, and misuse of digital laws. One prominent example is the case of Baiq Nuril, a teacher who recorded evidence of sexual harassment but was later prosecuted under the EIT Law, sparking national controversy regarding victim protection and freedom of expression.⁹ Another significant case involved Bjorka, a hacker responsible for leaking millions of Indonesian citizens' personal data, highlighting weaknesses in cybersecurity and accelerating the implementation of the PDP Law.¹⁰ In addition, numerous victims of revenge porn and cyberbullying, particularly women and students, have suffered psychological harm after private photos or humiliating content were distributed online without consent. These cases illustrate the

⁶ Caecilia Mediana, "Internet Traffic Anomaly Averages 1.25 Billion per Year," *Kompas.id*, August 11, 2025, <https://www.kompas.id/artikel/en-bssn-rata-rata-tahunan-anomali-trafik-internet-mencapai-125-miliar>.

⁷ The term "Cyber Cold War" refers to ongoing, low-intensity digital conflict between major powers, marked by espionage, cyberattacks, and influence operations rather than open military confrontation. It draws comparison to the 20th-century Cold War, but instead of nuclear arms races, today's competition centers on hacking capabilities, artificial intelligence, critical infrastructure, and information warfare. Countries such as the United States, China, and Russia are frequently cited as key actors. Activities include ransomware campaigns, intellectual property theft, election interference, cyber-espionage, and attacks on power grids or government networks. Unlike traditional warfare, attribution is often difficult, and operations are designed to remain below the threshold of armed conflict. The concept emphasizes persistent rivalry in cyberspace, where states compete for strategic advantage, technological dominance, and geopolitical influence without direct, large-scale military war. See Cheerala Rohith and Ranbir Singh Batth, "Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and Its Repercussion," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (IEEE, 2019), 640–45, <https://doi.org/10.1109/ICCIKE47802.2019.9004236>; Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law* 17, no. 2 (2012): 187–209, <https://doi.org/10.1093/jcsl/krs017>; Hans-Joachim Heintze and Pierre Thielbörger, eds., *From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years*, 2016, <https://link.springer.com/book/10.1007/978-3-319-19087-7>.

⁸ Muchamad Taufiq and Ananda Salsabila Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR," *International Journal of Business, Law, and Education* 6, no. 2 (2025): 1260–68, <https://doi.org/10.56442/ijble.v6i2.1178>.

⁹ Muhammad Zaidan Syafiqy Akhmad and Ridwan Arifin, "Baiq Nuril Case and Discourse on Freedom of Expression: Analysis of the Decision of the Supreme Court of the Republic of Indonesia Number 574k/Pid.Sus/2018 Regarding the Dissemination of Electronic Information Having Content Violating Morals," *Indonesia Media Law Review* 1, no. 2 (2022): 123–44, <https://journal.unnes.ac.id/journals/imrev/article/view/21735>.

¹⁰ Tole Sutikno and Deris Stiawan, "Cyberattacks and Data Breaches in Indonesia by Bjorka: Hacker or Data Collector?," *Bulletin of Electrical Engineering and Informatics (BEEI)* 11, no. 6 (2022), <https://beei.org/index.php/EEI/article/view/4854>.

urgent need for stronger legal protection, digital literacy, and effective law enforcement to ensure public safety in Indonesia's digital space.

Recent scholarship has increasingly highlighted the emergent challenges of digital victimization in Indonesia, particularly among vulnerable groups such as children, students, and marginalized populations. Putra¹¹ emphasizes the absence of specific legislation addressing cyberbullying, noting that existing laws on juvenile crimes and online offenses fail to capture the nuanced harms caused by digital harassment. High exposure to violent or abusive content online has been correlated with both increased victimization and the emergence of new perpetrators, underscoring the interplay between digital environments and social behaviors. Similarly, Puluhalawa and Husain¹² identify the phenomenon of body shaming through social media as a digital crime exacerbated by gaps in legal substance and weak enforcement mechanisms, demonstrating that victims often endure psychological distress, social stigma, and secondary victimization due to systemic regulatory inadequacies. These studies collectively suggest that Indonesia's fragmented legal framework contributes directly to both the scale and impact of digital victimization, leaving victims under-protected despite escalating online harms.

The literature further demonstrates that Indonesia's regulatory environment struggles to reconcile digital rights with enforcement capacity and institutional coordination. Mashdurohatun et al.¹³ analyze digital defamation under Law No. 11 of 2008 *jis*. Law No. 19 of 2016 and Law No. 1 of 2024 on Electronic Information and Transactions (hereinafter referred to as EIT Law) highlight regulatory inadequacies, weak institutional synergy, and public unawareness as structural factors undermining both victim protection and freedom of expression. Utomo¹⁴ extends this critique to broader human rights protection, noting that sector-specific legislation, insufficient enforcement, and limited digital literacy exacerbate vulnerabilities in online spaces. Margiansyah¹⁵ and Hermawan¹⁶ contextualize these legal deficiencies within socio-political dynamics, showing how digital platforms have been leveraged for political repression and oligarchic competition, which in turn creates additional risks of victimization in cyberspace. Together, these studies demonstrate that digital harm in Indonesia is not merely technical but deeply intertwined with socio-legal and political structures.

Emerging scholarship highlights the importance of participatory and victim-centered solutions. Sari and Silalahi¹⁷ propose digital participatory archives as a mechanism for advocacy and empowerment, enabling vulnerable groups to document their experiences, assert their cultural identity, and engage in digital justice initiatives. This perspective aligns with modern victimology, emphasizing victims as active stakeholders whose protection and agency are essential to systemic resilience. Across these studies, a clear pattern emerges: digital

¹¹ Eka Nugraha Putra, "Law's Silence on Cyberbullying to Children in Indonesia," *Brawijaya Law Journal* 11, no. 1 (2024): 135–63, <https://doi.org/10.21776/ub.blj.2024.011.01.07>.

¹² Mohamad Rusdiyanto U. Puluhalawa and Riski Husain, "Body Shaming Through Social Media As a Digital Crime In The Era of Disruption," *Jambura Law Review* 3, no. 1 (2021): 112–23, <https://doi.org/10.33756/jlr.v3i1.7200>.

¹³ Anis Mashdurohatun et al., "Combating Digital Defamation: Regulations, Challenges and Protecting Reputation," *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (2025): 486–514, <https://journal.yapici.or.id/index.php/JSDERI/article/view/147>.

¹⁴ Setiyo Utomo, "The Digital Age and Human Rights Protection in Indonesia: Legal Framework, Challenges, and Reform Directions," *Yustisia* 14, no. 2 (2025): 225–41, <https://doi.org/10.20961/yustisia.v14i2.85404>.

¹⁵ Defbry Margiansyah, "Digitalizing Authoritarianism in Indonesia: Exploring the Intersection of Civic Activism, Digital Repression, and Democratic Erosion," in *Indonesian Perspectives on Democracy* (Singapore: Springer, 2025), 183–209, https://doi.org/10.1007/978-981-96-3137-7_11.

¹⁶ Ary Hermawan, "Intra-Oligarchic Struggles and the Rise of Digital Attacks on Civil Society in Indonesia," *Journal of Contemporary Asia* 56, no. 3 (2026): 407–29, <https://doi.org/10.1080/00472336.2025.2505918>.

¹⁷ T.Y. Sari and K.P. Silalahi, "Digital Participatory Archive for Justice: An Inclusive Future for Vulnerable Groups," in *Religion, Education, Science and Technology towards a More Inclusive and Sustainable Future*, ed. Maila D.H. Rahiem (Routledge, 2024), <https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9781003322054-34/digital-participatory-archive-justice-inclusive-future-vulnerable-groups-sari-silalahi>.

victimization in Indonesia is structurally mediated by gaps in legal frameworks, enforcement capacity, and socio-political dynamics, suggesting the urgent need for comprehensive, interdisciplinary approaches that integrate legal reform, institutional coordination, and citizen-centered interventions.

The primary limitation of earlier scholarship lies in the inability to bridge the gap between digital victimization, broader national security concerns, and international data protection “adequacy” standards. There is a lack of interdisciplinary analysis connecting the human dimension of being a “digital victim” to the structural failures of state institutions. This research seeks to address these gaps by rigorously analyzing Indonesia’s regulatory framework, institutional coordination, and strategic initiatives in cyber defense, particularly in the wake of the 2024 PDN crisis.

The objective of this study is to examine specific weaknesses in Indonesia’s current legal framework regarding digital victimization, particularly in cases involving data breaches, cyber harassment, and unauthorized distribution of personal information. This study also aims to evaluate the effectiveness of existing regulations, including the EIT Law and the PDP Law, in protecting victims and ensuring legal accountability. Furthermore, the research proposes measurable regulatory harmonization through clearer victim-protection mechanisms, stronger institutional coordination, and more consistent law-enforcement practices. The novelty of this study lies in its interdisciplinary approach, integrating normative legal analysis with victimology and criminology to assess both the legal impact and the social consequences experienced by victims. Additionally, this paper argues that for Indonesia to achieve digital resilience, it must move toward a governance model that treats data privacy as a pillar of national security rather than a hindrance to it. The following sections will detail the research methodology, analyze the PDP Law’s alignment with global standards, and provide policy recommendations to strengthen Indonesia’s cyber defense architecture. This analysis is expected to contribute to the global discourse on digital constitutionalism, offering a blueprint for how developing nations can navigate the complexities of sovereignty in a borderless digital world.

2. Method

This study employs a doctrinal legal research method, characterized by an analytical approach to statutory provisions, legal doctrines, and underlying legal principles. The research is framed through a comparative approach, systematically evaluating Indonesia’s Law No. 27 of 2022 on Personal Data Protection (PDP Law) against global benchmarks, specifically the European Union’s General Data Protection Regulation (GDPR)¹⁸. To contextualize the legal analysis in light of current digital threats, the study also employs a case study approach, examining the 2024 ransomware attack on the National Data Center (PDN). This multifaceted lens enables a rigorous assessment of how domestic security imperatives, often codified in the EIT Law, intersect with international data privacy adequacy standards. This study employs normative legal research using secondary data, including Indonesian laws, government regulations, international instruments, academic journals, and official reports from the National Cyber and Crypto Agency (BSSN). The data are analyzed qualitatively through legal interpretation and content analysis to identify weaknesses in existing regulations and evaluate legal protection mechanisms for victims of digital victimization in Indonesia.

3. Results and Discussion

3.1. The Legal Anatomy of Indonesia’s PDP Law vs. Global Standards (GDPR)

Indonesia’s regulatory and institutional architectures for cyber defense currently reside at a critical evolutionary juncture. The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a seminal milestone in consolidating a historically fragmented landscape of data privacy regulations. This statute establishes a comprehensive normative framework for the collection, processing, and retention of personal data, mandating that data controllers appoint

¹⁸ European Union, “General Data Protection Regulation (GDPR)-Regulation (EU) 2016/679 of the European Parliament and of the Council,” 2016, <https://gdpr.eu.org/full/full.pdf>.

Data Protection Officers (DPOs) and deploy robust technical safeguards. However, the transition from legislative intent to operational enforcement remains asymmetrical. As Yuniarti¹⁹ observes the efficacy of the PDP Law is significantly hampered by constrained institutional capacity and the persistence of overlapping mandates among competing state agencies, which creates a “regulatory gray area” in the event of cross-sectoral data breaches.

The state’s strategic trajectory toward enhancing cyber resilience is further articulated in the 2025 Cyber Security and Resilience Bill (*Rancangan Undang-Undang Keamanan dan Ketahanan Siber*, hereinafter as RUU KKS). This draft legislation seeks to fundamentally recalibrate the authority of the National Cyber and Crypto Agency (BSSN), empowering it with expansive jurisdictions over crisis management, the regulation of Artificial Intelligence (AI), and the stringent oversight of digital service providers. Nevertheless, this expansion of power has sparked intense academic and policy debate regarding institutional friction. Sulubara, Tasril, and Nurkhalisah²⁰ argue that the bill risks exacerbating inter-agency rivalries rather than fostering a consolidated governance model, particularly concerning the boundaries of investigative powers and digital content intervention. Such structural tensions underscore the profound difficulty of reconciling the Westphalian pursuit of national digital sovereignty with the practical requirements of transparent, effective cyberspace governance.

At the institutional level, the National Cyber and Crypto Agency (BSSN) has sought to provide a centralized strategic trajectory through BSSN Regulation No. 5 of 2024 regarding the National Cybersecurity Action Plan (2024–2028). This roadmap prioritizes the fortification of Critical Information Infrastructure (CII), the streamlining of incident response, and the enhancement of digital literacy. However, the operational success of this mandate is contingent upon seamless inter-agency synergy and the equitable distribution of technical resources. As Aji, Somantri, and Rofii²¹ argue, the realization of cyber sovereignty in Indonesia necessitates a fundamental revitalization of the BSSN to ensure coherent leadership and authoritative coordination across disparate ministries. In the absence of such institutional reform, Indonesia’s posture remains inherently reactive, a vulnerability that invites persistent exploitation by sophisticated digital actors.

When viewed through a comparative lens, Indonesia’s regulatory framework exhibits significant lag relative to global best practices, most notably the European Union’s General Data Protection Regulation (GDPR). The GDPR’s success lies in its ability to harmonize standards across diverse jurisdictions while simultaneously ensuring institutional accountability and the inviolability of individual rights. In contrast, Indonesia’s fragmented legal environment creates enforcement vacuums that erode public trust. Solikhah²² observes that even with the ratification of the PDP Law, the Indonesian regime lacks the proactive enforcement mechanisms, such as independent oversight and pre-emptive audits that characterize the European model. This discrepancy suggests that legislative adoption is insufficient without the corresponding institutional maturity required for global adequacy status.

The catastrophic ransomware assault on the National Data Center (PDN) in Surabaya in June 2024 represents more than a mere technical failure; it serves as a definitive empirical case study of the systemic fragilities inherent in Indonesia’s nascent digital governance. This incident revealed a profound synchronization deficit between the Ministry of Communication and

¹⁹ Siti Yuniarti, “Protection of Indonesia’s Personal Data After Ratification of Personal Data Protection Act,” *Progressive Law Review* 4, no. 2 (2022): 54–68, <https://doi.org/10.36448/plr.v4i02.85>.

²⁰ Seri Mughni Sulubara, Viridya Tasril, and Nurkhalisah Nurkhalisah, “Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia’S Defense,” *De Lega Lata: Jurnal Ilmu Hukum* 10, no. 2 (2025): 287–97, <https://jurnal.umsu.ac.id/index.php/delegalata/article/view/25786>.

²¹ Muhammad Prakoso Aji, Gumilar Rusliwa Somantri, and Muhammad Syaroni Rofii, “The Strategic Role of the National Cyber and Crypto Agency (BSSN) in Maintaining State Sovereignty in Cyberspace,” *Journal of Law, Politic and Humanities* 5, no. 5 (2025): 3916–3924, <https://doi.org/10.38035/jlph.v5i5.1973>.

²² Mar’atus Solikhah, “Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework,” *Indonesian Cyber Law Review* 2, no. 1 (2025): 39–50, <https://iclr.polteksci.ac.id/index.php/sci/article/view/15>.

Informatics (Kementerian Komunikasi dan Informatika [Kominfo]) as the facility provider, the National Cyber and Crypto Agency (BSSN) as the security overseer, and the Indonesian National Police (Kepolisian Negara Republik Indonesia [Polri]) as the investigative arm (see Table 3). The lack of a predefined, legally binding hierarchy for crisis intervention resulted in protracted recovery delays and the exposure of sensitive data belonging to millions of citizens. This institutional paralysis underscores the “silo mentality”²³ that persists despite the enactment of the PDP Law, demonstrating that legislative mandates are ineffective without operational interoperability.

Applying Routine Activity Theory (RAT) to the PDN breach provides a rigorous framework for understanding this victimization (see Table 2). Under this criminological lens, the breach occurred at the convergence of three critical elements: a motivated offender, a highly suitable target, and the absence of a capable guardian. The offenders in this case used the sophisticated LockBit 3.0 ransomware and identified the PDN as a high-value, suitable target due to the extreme centralization of state data. Crucially, the absence of a capable guardian was not merely a lack of firewalls, but a lack of legal and institutional guardianship. The failure to implement mandatory backups and the absence of a digital sovereign authority with the power to enforce security compliance left the target essentially undefended against a known threat vector.

Furthermore, the crisis highlighted a significant legal vacuum regarding public sector accountability. While Article 46 of the PDP Law mandates that in the event of a failure to protect personal data, the Data Controller must provide written notification to the Data Subject and the Agency, the PDN incident revealed that the government struggled to fulfill its role as a *Controller* while simultaneously acting as the *Regulator*. This dual role created a conflict of interest that hindered transparent communication and delayed efforts to mitigate digital victimization among the affected public. The sound of the law in Article 46 requires notification within 3 x 24 hours. Yet the ambiguity of which institution bore ultimate responsibility for the PDN's integrity meant accountability was diffused rather than enforced.

²³ Silo mentality refers to a situation in which departments or units within an organization operate in isolation, limiting communication, collaboration, and information sharing. The term derives from agricultural silos, which store grain separately, symbolizing how teams become vertically insulated from one another. In management literature, silo mentality is linked to fragmented decision-making, duplication of work, and reduced organizational learning. Scholars such as Peter Senge emphasize that organizational effectiveness depends on systems thinking, where interconnected parts work toward shared goals rather than isolated targets. Similarly, Chris Argyris highlights how defensive routines and poor communication can inhibit collective problem-solving. In public sector and cybersecurity contexts, silo mentality can be particularly harmful, as complex threats require coordinated responses across agencies. When information is withheld or not integrated, vulnerabilities increase, and crisis responses slow down. Therefore, overcoming silo mentality through cross-functional collaboration and shared accountability is critical for institutional resilience and strategic effectiveness. In this context, the UU PDP was enacted to strengthen personal data protection and institutional accountability across the public and private sectors. However, effective enforcement requires strong coordination between ministries, regulators, cybersecurity agencies, and state-owned enterprises. If these actors operate in silos, failing to share risk assessments, audit findings, or breach reports, compliance becomes fragmented and reactive rather than preventive. This institutional fragmentation was evident during the 2024 ransomware attack, when disruptions affected hundreds of public services. The crisis exposed weaknesses in inter-agency coordination, incident response integration, and centralized oversight. A silo mentality may delay threat intelligence sharing and obscure accountability for cybersecurity standards. See Peter Senge, “Classic Work: The Leader’s New Work: Building Learning Organizations,” in *Knowledge Management: Classic and Contemporary Works*, ed. Daryl Morey, Mark T. Maybury, and Bhavani Thuraisingham (The MIT Press, 2000), <https://doi.org/10.7551/mitpress/4075.003.0008>; Tegar Islami Putra et al., “Challenges in Ensuring Personal Data Protection For Society in The Era of Society 5.0: Indonesia’s Case Study,” *Unnes Law Journal* 10, no. 2 (2024): 223–54, <https://journal.unnes.ac.id/journals/ulj/article/view/8928>; Firsta Rahadatul ‘Aisy, Muhammad Azil Maskur, and A.M Adzkiya’ Amiruddin, “Establishing Indonesia’s Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore,” *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431–82, <https://doi.org/10.15294/jils.v10i1.13755>; Supeno Supeno, Rosmidah Rosmidah, and Syed Mohd Uzair Iqbal, “Personal Data Protection in Review of Legal Theories and Principles,” *Journal of Law and Legal Reform* 6, no. 3 (2025): 1349–1376, <https://doi.org/10.15294/jllr.v6i3.10252>.

The socio-legal implications of the PDN attack extend to the erosion of the *social contract* in the digital age. When citizens are compelled by law to submit their biometric and personal data to state databases (such as *SatuSehat* or immigration systems), the state assumes an absolute fiduciary duty to protect that data.²⁴ The 2024 breach demonstrated that the current institutional framework is insufficient to uphold this duty. The crisis, therefore, catalyzes the "securitization" of data privacy, shifting the discourse from a technical IT issue to a matter of national survival. This necessitates a fundamental reimagining of the BSSN's role, not merely as a consultant, but as a *Supreme Guardian* with the statutory authority to override ministerial autonomy in the interest of national cyber defense.

In a descriptive-analytic sense, the PDN incident exposed the myth of centralization as a security panacea. While the government's move toward a National Data Center was intended to streamline governance and enhance control (in line with Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems), it paradoxically created a single point of failure. The research suggests that Indonesia's drive for Digital Sovereignty through data centralization has outpaced its development of institutional resilience. Without a harmonized crisis management protocol codified in a specific legal instrument that delineates the rules of engagement among Kominfo, BSSN, and Polri, the PDN remains a lucrative target for both state and non-state actors in the global cyber arena.

Furthermore, the current landscape of Indonesia's digital governance is defined by a paradigmatic transition from a *permissive-administrative* regime to a *sovereign-punitive* framework, where the protection of the individual is increasingly inextricably linked to national resilience. Historically, digital activities were governed by a patchwork of regulations centered on the Electronic Information and Transactions (EIT) Law, which prioritized the legality of electronic commerce over the data subject's inherent rights.²⁵ However, the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) has fundamentally recalibrated this trajectory, introducing a *lex specialis* that seeks to harmonize domestic standards with the EU GDPR.²⁶ This legislative cornerstone shifts the focus toward the ontological protection of the data subject,

²⁴ The PDN ransomware attack carries significant socio-legal consequences by weakening the digital social contract between citizens and the state. Indonesians are legally required to submit personal and biometric data to centralized systems such as *SatuSehat* and immigration databases, leaving them with no meaningful option to withhold participation. In return, the state assumes a fiduciary duty to safeguard that data through strong cybersecurity governance and oversight. When such systems are compromised, the failure extends beyond technical disruption, it erodes public trust, questions institutional accountability, and challenges the legitimacy of Indonesia's broader digital transformation agenda and data protection commitments. See Shafa Suhaila et al., "Pertanggungjawaban Negara Dalam Kebocoran Data Pada Platform E-Government: Analisis Hukum Administrasi Atas Kasus Satu Sehat Dan DPMPSTSP Online," *Jurnal Ilmiah Penelitian Mahasiswa* 4, no. 2 (2026): 12–21, <https://ejurnal.kampusakademik.my.id/index.php/jipm/article/view/2166>; Andreas Abimanyu Prasetya et al., "Legal Enforcement on the Misuse of Health Data in the SATUSEHAT Mobile Application: Patient Privacy Protection," *Immortalis Journal of Interdisciplinary Studies* 2, no. 1 (2026): 1–8, <https://immortalispub.com/IJIS/article/view/59>.

²⁵ Bambang Sugeng Ariadi Subagyo et al., "Can Indonesia's Laws Keep Up? Protecting Consumer Rights in Digital Transactions," *Journal of Law and Legal Reform* 5, no. 3 (2024): 869–90, <https://doi.org/10.15294/jllr.v5i3.4202>.

²⁶ Muhammad Akbar Eka Pradana and Horadin Saragih, "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya," *Innovative: Journal Of Social Science Research* 4, no. 4 (2024): 3412–3425, <https://j-innovative.org/index.php/Innovative/article/view/13476>; Tegar Islami Putra, Nurul Fibrianti, and Rizky Andeza Prasetya, "Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe)," *Journal of Private and Commercial Law* 9, no. 1 (2025): 72–109, <https://doi.org/10.15294/jpcl.v9i1.9370>; Supeno, Rosmidah, and Iqbal, "Personal Data Protection in Review of Legal Theories and Principles"; Arnanda Yusliwidaka, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana, "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?," *Pandecta Research Law Journal* 19, no. 2 (2024): 453–82, <https://doi.org/10.15294/pandecta.v19i2.13279>.

establishing a comprehensive regime of rights and obligations that did not previously exist in the Indonesian legal hierarchy.

The core of this protective framework is articulated in Article 8 of the PDP Law, which provides the foundational right to erasure. The article explicitly states that: *"The Data Subject shall be entitled to terminate processing, delete, and/or destroy their Personal Data."* This provision represents a radical departure from previous norms, yet its descriptive reality is complicated by the procedural limitations inherent in Indonesian administrative law. While the sound of the law grants total control to the individual, the analysis reveals that the implementation of this right, particularly in relation to state-owned databases, remains hindered by a lack of technical guidelines and the absence of a fully independent supervisory authority. This suggests that while Indonesia has adopted the language of global privacy standards, the power dynamics remain weighted toward the state as the primary data controller.

The most profound normative friction, and perhaps the greatest challenge to the paper's focus on digital victimization, is identified in the *securitization loophole* found in Article 15, paragraph (1), point (a) of the PDP Law. This specific provision stipulates that: *"The rights of the Data Subject as referred to in Articles 8, 9, 10, 11, and 13 shall be exempted for: (a) National defense and security."* In a descriptive-analytic sense, this article creates a legal paradox; it essentially deactivates the individual's shield against victimization the moment the state invokes a security imperative. Because the law does not provide a narrow, technical definition of national security in the digital realm, this provision grants executive agencies broad discretion. This analysis argues that such an expansive exemption risk transforms a tool of protection into an instrument of state surveillance, potentially facilitating the very digital victimization the law was designed to prevent.

Furthermore, the research highlights a strategic shift toward institutional accountability through the mandate for Data Protection Officers (DPOs). Article 53 of the PDP Law mandates that: *"Data Controllers and Data Processors shall appoint a Personal Data Protection Officer if... the core activities of the Data Controller consist of processing operations which require regular and systematic monitoring of Data Subjects on a large scale."*²⁷ This provision is theoretically aligned with the concept of the capable guardian in Routine Activity Theory. However, an analysis of the 2024 National Data Center (PDN) crisis reveals a catastrophic compliance gap. While the law requires a DPO to safeguard data, the absence of such oversight in public-sector institutions during the ransomware attack demonstrated that the mandates of Article 53 have yet to be effectively internalized within the government's administrative culture.

The deterrent aspect of the Indonesian framework is notably more punitive than its European counterparts, emphasizing criminal over administrative liability. This is encapsulated in Article 67, paragraph (2), which states: *"Any Person who intentionally and unlawfully creates false Personal Data or uses false Personal Data with the intention to benefit themselves or another person that may cause loss to other persons shall be sentenced to imprisonment for a maximum period of 6 (six) years."* By focusing on the intent to benefit and causing loss, the Indonesian legislature frames data protection as a criminal matter of public order rather than a mere regulatory compliance issue. This descriptive reality underscores a heavy-handed approach to digital victimization that seeks to deter offenders through the threat of incarceration. This strategy reflects Indonesia's unique legal tradition but may fail to address the systemic technical vulnerabilities of digital infrastructure.²⁸

²⁷ Sidi Wiraguna, "Strengthening the Functional Autonomy of Data Protection Officers Under Indonesia's PDP Law 2022: A Critical Legal and Institutional Review," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 4, no. 3 (2025): 1–8, <https://jurnal.penerbitwidina.com/index.php/JPS/article/view/2317>; Brahmantyo Suryo Satwiko, "Privacy and Data Protection: Indonesian Legal Framework," *Corporate and Trade Law Review (CTLR)* 1, no. 2 (2021): 98–118, <https://doi.org/10.21632/ctrlr.1.2.98-118>.

²⁸ Putra et al., "Challenges in Ensuring Personal Data Protection For Society in The Era of Society 5.0: Indonesia's Case Study"; Tegar Islami Putra, Nurul Fibrianti, and Adinda Zeranica Putri Fakhis, "Implementation of CNIL's Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection," *The Indonesian Journal of International Clinical Legal Education* 7, no. 2 (2025): 203–34, <https://doi.org/10.15294/iccle.v7i2.21049>; Ratih Damayanti, Duhita Driyah Suprpti, and Rohmat

The legislative mechanism is being used as a strategic tool for Digital Sovereignty, as evidenced by the interplay among the PDP Law, Presidential Regulation No. 47 of 2023 on the National Cyber Security Strategy, and Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure. These regulations provide the legal basis for protecting Critical Information Infrastructure (CII) and justify data localization. However, the analysis suggests that this drive for sovereignty, while intended to shield the nation from international digital victimization, can paradoxically increase domestic vulnerability. By centralizing sensitive data within the national borders to satisfy the sound of sovereign control, the state creates high-value targets for sophisticated actors.²⁹ This suggests that Indonesia's regulatory shift is a complex effort to leverage global privacy norms to consolidate control, creating a digital ecosystem that is both a protective fortress and a singular point of systemic risk.

Furthermore, in this context, within the Indonesian legal framework, digital victimization is only indirectly addressed under Law No. 11 of 2008 on Electronic Information and Transactions, as lastly amended by Law No. 1 of 2024 (the EIT Law). Several provisions criminalize cyber-enabled conduct that frequently results in digital victimization. For example, Article 30 prohibits unauthorized access to electronic systems, while Article 31 criminalizes unlawful interception or wiretapping of electronic information and electronic documents. Article 32 prohibits the unauthorized alteration, transfer, destruction, concealment, or disclosure of electronic information and electronic documents. In contrast, Article 35 prohibits the manipulation, creation, alteration, deletion, or destruction of electronic information intended to make such information appear authentic. These offences are reinforced by the corresponding criminal sanctions contained in Articles 46, 47, 48, and 51. Collectively, these provisions provide a legal basis for prosecuting cyber offenders responsible for hacking, unlawful surveillance, identity theft, data manipulation, and other forms of cybercrime that frequently cause digital harm to individuals.

Despite these criminal provisions, the EIT Law remains primarily offender-oriented and does not explicitly recognize digital victimization as a distinct legal concept. The law focuses on identifying prohibited conduct and imposing criminal liability without comprehensively regulating the legal rights of victims whose personal data, digital identity, or electronic communications have been compromised. For instance, although unlawful interception under Article 31 and unauthorized access under Article 30 may directly violate an individual's privacy, the law does not establish corresponding rights to notification, compensation, rehabilitation, or data restoration for affected persons. Similarly, victims of doxing, identity theft, cyberstalking, or large-scale personal data misuse often depend on a combination of the EIT Law, the Personal Data Protection Law, and the Indonesian Criminal Code to seek legal protection, creating fragmentation and uncertainty regarding available remedies.

This regulatory gap becomes increasingly significant when digital victimization arises from cybersecurity operations or national security measures that involve the processing of personal data. While the EIT Law provides the legal foundation for safeguarding electronic systems and combating cybercrime, it lacks explicit safeguards to balance national security objectives with individual digital rights. Consequently, future amendments should introduce specific provisions that recognize digital victimization as a protected legal interest, define victims' procedural and substantive rights, and ensure effective coordination with the Personal Data Protection Law and the State Intelligence Law. Such reforms would enable the EIT Law to evolve from a predominantly punitive instrument into a comprehensive legal framework that simultaneously strengthens cybersecurity, protects national security, and guarantees effective legal remedies for victims of digital harm. In the global context, data privacy is currently anchored by the EU's General Data Protection Regulation (GDPR), which serves as the gold standard for digital

Rohmat, "Judicial Precedents on Privacy Rights: Court Rulings in the Digital Era," *Indonesian Court and Justice Review* 1, no. 4 (2024), <https://journal.perhaki.org/index.php/court/article/view/60>; Hendrikus Adiputra, Jingga Putri, and Ravion Iskandar Valeon, "Digital Health, Data Sovereignty, and Justice: Legal Challenges of Telemedicine Expansion in Post-Pandemic Indonesia," *Indonesian Health Justice Review* 2, no. 4 (2025), <https://journal.perhaki.org/index.php/health/article/view/383>.

²⁹ Eunike Putri and Fadhel Arjuna Adinda, "Artificial Intelligence, Digital Rights, and Human Dignity in Indonesia's Tech Regulation," *Contemporary Issues on Indonesian Human Rights Law and Policy* 2, no. 1 (2025), <https://journal.perhaki.org/index.php/humanrights/article/view/358>.

constitutionalism and the primary benchmark for Indonesia's Law No. 27 of 2022 (UU PDP) (see Table 1). This legislative evolution in Indonesia represents a profound shift from a fragmented, sectoral approach to a unified, omnibus framework aimed at fostering international trust. By adopting the GDPR's conceptual vocabulary, such as the distinction between data controllers and processors, Indonesia aims to achieve adequacy status to facilitate seamless trans-border data flows. However, a thorough legal analysis reveals that while the UU PDP mimics the GDPR's structural form, its operational essence is shaped by Indonesia's unique civil law tradition and specific national security imperatives. This creates a regulatory environment that is theoretically aligned with global norms but, in practice, distinct in its enforcement philosophy and institutional hierarchy.

One of the most significant points of convergence lies in the codification of data subject rights, where Articles 5 to 15 of the UU PDP closely mirror the rights enshrined in Chapter III of the GDPR. For instance, the Indonesian rights to erasure (Article 8) and to data portability (Article 13) are direct ideological descendants of GDPR Articles 17 and 20, respectively. These provisions represent a move toward informational self-determination, granting Indonesian citizens unprecedented control over their digital personas. Nevertheless, the descriptive analysis suggests that the UU PDP lacks the procedural granularity found in the GDPR's Recitals, which provide extensive interpretative guidance on how these rights should be exercised. In the absence of such detailed guidance, the exercise of these rights in Indonesia remains contingent upon future implementing regulations, creating a period of legal uncertainty that may hinder the immediate protection of victims of digital victimization.

The principle of *Lawful Basis for Processing* serves as another critical intersection, where Article 20 of the UU PDP adopts the GDPR's multi-pronged approach to data legitimacy. Both regimes require that processing be based on explicit consent, contract performance, legal obligations, or legitimate interests. However, the Indonesian interpretation of legitimate interest remains narrower than the GDPR's balancing test found in Article 6(1)(f), which stated that: "*necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*". In the EU, legitimate interest is a flexible tool for innovation, whereas in the Indonesian context, the emphasis remains heavily weighted toward explicit consent and state-defined public interests.³⁰ This suggests that while Indonesia has adopted the GDPR's language, the application of these bases may be more restrictive, potentially limiting the agility of digital enterprises while simultaneously granting the state broader latitude under the guise of public service and administrative necessity.

A fundamental divergence appears in the institutional design of the supervisory authority, a cornerstone of the GDPR's success. Under GDPR Article 52, the supervisory authority must act with complete independence, remaining free from external influence, whether direct or indirect. In contrast, the UU PDP, specifically through its transitional provisions, indicates that the Indonesian Personal Data Protection Agency will be established by and responsible to the President. Analytically, this positioning within the executive branch creates a potential conflict of interest, particularly when the state itself acts as a massive data controller through its electronic government systems (Sistem Pemerintahan Berbasis Elektronik, hereinafter referred to as SPBE). Without the *Functional Independence*³¹ mandated by the GDPR, the Indonesian agency may struggle to audit government institutions impartially, a weakness that was starkly exposed

³⁰ Jan Philipp Albrecht, "How the GDPR Will Change the World," *European Data Protection Law Review* 2, no. 3 (2016): 287–89, <https://doi.org/10.21552/EDPL/2016/3/4>.

³¹ In GDPR, functional independence refers to the autonomy of Data Protection Authorities (DPAs) to perform their duties without external influence, ensuring impartial enforcement of data protection laws. DPAs must make decisions on investigations, sanctions, and guidance independently, while maintaining administrative and financial control over their operations. This independence prevents conflicts of interest, particularly when regulating powerful public or private entities, and safeguards individuals' fundamental rights. By operating autonomously, DPAs can enforce GDPR consistently, protect personal data effectively, and maintain public trust, ensuring that political, organizational, or financial pressures do not compromise compliance and accountability.

during the 2024 National Data Center (PDN) crisis, where the lines between regulator and operator became dangerously blurred.

The Securitization of Privacy represents another area of critical divergence, specifically regarding the exemptions for national security. While the GDPR (Article 23) allows for restrictions on data rights for the sake of national security, such measures must be necessary and proportionate in a democratic society and subject to judicial oversight. Conversely, Article 15 of the UU PDP provides a broad exemption for national defense and security without the explicit requirement for a proportionality test or independent judicial review. This creates a descriptive reality where the state can deactivate privacy protections with minimal friction, a move that contradicts the GDPR's emphasis on the inviolability of fundamental rights. For Indonesia to achieve true alignment, it must refine this exemption to ensure that national security is not a generic justification for bypassing the PDP Law's protective mandates, thereby preventing state-led digital victimization.

Furthermore, the sanctioning regimes of the two frameworks reveal differing philosophies regarding deterrence. The GDPR is famous for its administrative fines of up to €20 million or 4% of total worldwide annual turnover, a mechanism designed to make data protection a boardroom priority.³² While Article 57 of the UU PDP introduces administrative fines of up to 2% of annual income, the Indonesian framework places a unique and heavy emphasis on criminal liability.³³ Articles 67 to 70 of the UU PDP prescribe imprisonment for various data offenses, reflecting a punitive approach that is absent from the GDPR's primary text. This analysis argues that while criminalization may deter individual motivated offenders, it does not necessarily foster the culture of compliance that the GDPR's administrative model achieves. To mitigate digital victimization effectively, Indonesia must balance its criminal sanctions with the rigorous administrative auditing processes characterized by the GDPR's Accountability Principle.

The concept of *Privacy by Design and by Default* (GDPR Article 25)³⁴ is theoretically integrated into the Indonesian framework through the general obligations of data controllers. However, the descriptive analysis of the 2024 PDN breach suggests that these principles have not yet permeated the operational layer of Indonesian public administration. The GDPR requires that data protection be integrated into the development of all digital systems from the outset. In Indonesia, the drive for digital sovereignty has often prioritized data centralization over risk decentralization. This results in the creation of high-value targets for ransomware actors, where the lack of GDPR-standard technical guardianship (such as encryption and automated backups) transforms sovereign data hubs into singular points of failure. The transition to a GDPR-aligned state requires not only legal compliance but also technical hardening of the national digital infrastructure to match the law's normative promises.

The alignment between the UU PDP and the GDPR is a work of *Regulatory Hybridization*.³⁵ Indonesia has successfully adopted the global standard's normative vocabulary to protect its

³² İbrahim Barış Sayar, "The Administrative Fines Regime of the General Data Protection Regulation and Its Impact," *Kişisel Verileri Koruma Dergisi* 3, no. 1 (2021): 1–16, <https://izlik.org/JA87PT29LY>.

³³ Kuku Dwi Kurniawan et al., "Criminal Sanctions and Personal Data Protection in Indonesia," *Lex Publica* 11, no. 2 (2024): 221–47, <https://doi.org/10.58829/lp.11.2.2024.255>.

³⁴ Lee A. Bygrave, "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements," *Oslo Law Review* 4, no. 2 (2017): 105–120, <https://doi.org/10.18261/issn.2387-3299-2017-02-03>; Fabio Bravo, "Data Management Tools and Privacy by Design and by Default," in *Privacy and Data Protection in Software Services*, ed. R. Senigaglia, C. Irti, and A. Bernes (Singapore: Springer, 2022), 85–95, https://link.springer.com/chapter/10.1007/978-981-16-3049-1_8.

³⁵ Regulatory Hybridization in Indonesia's UU PDP represents a strategic synthesis where the government integrated the rigorous, globally recognized standards of the EU's GDPR with Indonesia's specific constitutional values and existing legal infrastructure. Rather than adopting a foreign framework in its entirety, Indonesia "hybridized" the law by adopting Western concepts, such as the classification of data controllers and processors, while embedding them within a local enforcement system that includes heavy criminal sanctions and a supervisory authority that remains under the executive branch's oversight. This approach allows Indonesia to participate in the global digital economy by offering "adequate" data protection levels that satisfy international partners, while simultaneously maintaining national sovereignty and aligning with the country's unique administrative traditions and the principle of *Pancasila*.

citizens and participate in the digital economy, yet it maintains a state-centric approach to enforcement and security. The success of this hybrid model depends on whether the state can establish a *Capable Guardian* that is institutionally independent and legally empowered to protect data subjects against both private and state-sponsored victimization.³⁶ By refining the independence of its supervisory agency and strictly defining the limits of security exemptions, Indonesia can move from a state of *Symbolic Convergence* to *Operational Adequacy*, ensuring that the UU PDP serves as a transformative shield for the nation's digital future while remaining a credible partner in the global data protection regime.

Table 1.
Gold Standard of GDPR and Its Connection to UU PDP Indonesia

Regulatory Aspect	EU GDPR (Standard)	Indonesia UU PDP (No. 27/2022)	Academic Analysis
Supervisory Authority	Fully Independent: Autonomous from government influence (Art. 52).	Executive-Led: Established by and responsible to the President.	Divergence raises concerns regarding "Functional Independence" in state data breaches.
Sanction Philosophy	Administrative: Heavy fines up to 4% of global turnover.	Hybrid: Administrative fines (2%) + Criminal Imprisonment (Art. 67-70).	Indonesia emphasizes punitive deterrence (criminal) over corporate compliance (administrative).
National Security	Restricted: Must be necessary, proportionate, and legally specific.	Broad Exemption: General exemption for "National Defense" (Art. 15).	Creates a "Securitization Loophole" that may bypass individual privacy shields.
Breach Notification	Mandatory within 72 hours.	Mandatory within 3 x 24 hours (Art. 46).	High Alignment: Temporal standards for "Capable Guardianship" are synchronized.

Source: Various sources, edited by the authors

This table identifies the degree of normative alignment between the global "*gold standard*" and Indonesia's 2022 legislation. It highlights where Indonesia has successfully converged and where institutional "*lag*" remains.

³⁶ Judith Emmanuel, Windiahsari Windiahsari, and Hee-Joon Kim, "Indonesia's Foreign Policy: Navigating Relations Between the U.S., China, and ASEAN," *Indonesia Discourse* 1, no. 2 (2024): 285–312, <https://journal.unnes.ac.id/journals/indi/article/view/22759>; Andi Tenri Sapada and Mohammad Arif, "Use of Artificial Intelligence in General Elections: Comparison of Indonesian and German Regulations," *Contemporary Issues on Indonesian Social Justice and Legal Reform* 1, no. 1 (2025): 21–40, <https://journals.arteslibres.org/index.php/law/article/view/2>; Joshua Lee, Zhang Mei, and Kunal Mehta, "Digital Authoritarianism and the Erosion of Civil Liberties: A Comparative Legal Study of Surveillance Laws in China, India, and the United States," *Journal of Transformative Legal and Social Studies* 1, no. 1 (2025): 97–120, <https://journals.arteslibres.org/index.php/social/article/view/15>.

Table 2.
Theoretical Framework on Applying Criminology to Digital Victimization

Element of RAT	Application to 2024 PDN Breach	Impact on Digital Victimization
Motivated Offender	Transnational Ransomware Actors (e.g., LockBit 3.0).	Operates beyond the jurisdictional reach of domestic Indonesian law enforcement.
Suitable Target	Centralized National Data Center (PDN) containing millions of civil servant records.	Centralization (Digital Sovereignty) created a "Single Point of Failure" and a high-value target.
Absence of Capable Guardian	Failure in institutional stewardship; lack of mandatory encrypted backups.	The "Legal Guardian" (UU PDP) was in place, but the "Technical Guardian" (BSSN/Kominfo) lacked operational synergy.

Source: Various sources, edited by the authors

This table applies Routine Activity Theory (RAT) to the 2024 National Data Center (PDN) crisis to explain why legal frameworks alone were insufficient to prevent victimization.

Table 3.
The Three Pillars of Indonesia’s Cyber Defense

Institutional Pillar	Primary Role	Legal Basis	Strategic Weakness
BSSN (National Cyber Agency)	Centralized Operational Lead & Crisis Management.	PR No. 47/2023	Limited statutory authority to compel other ministries to follow security mandates.
Kominfo (Ministry of Comm & Info)	Facility Provider & Regulatory Support.	EIT Law (No. 1/2024)	Overlapping mandates with BSSN often lead to "Synchronization Deficits" during crises.
Satsiber TNI (Military Cyber Unit)	Defense of the "Fifth Domain" of Warfare.	TNI Doctrine	Tension between military surveillance needs and civilian privacy rights (UU PDP).

Source: Various sources, edited by the authors

The provided tables (Table 1, Table 2, and Table 3) reveal a profound structural tension between Indonesia’s legislative aspirations and its operational reality, effectively defining the current state of Digital Victimization in the country. Table 1 demonstrates that while the UU PDP has successfully adopted the normative *grammar* of the GDPR, such as temporal standards for breach notification and data subject rights, a critical divergence persists in the institutional positioning of the supervisory authority and the broadness of national security exemptions. This Securitization Loophole is further deconstructed in Table 2 through the lens of Routine Activity Theory, which posits that the 2024 PDN crisis was a direct result of the convergence of motivated transnational offenders and a highly centralized, suitable target. The failure, in this context, was not a lack of law, but the absence of a capable guardian possessing the technical and institutional autonomy to enforce protection over state-owned assets.

To bridge this *Policy-Practice Gap*, Table 3 identifies the need to harmonize the disparate roles of the BSSN, Kominfo, and the Indonesian National Military (Tentara Nasional Indonesia [TNI]) into a cohesive national defense architecture. The current institutional synthesis suffers

from *Synchronization Deficits*, where the administrative autonomy of facility providers and the strategic imperatives of military doctrine often undermine the BSSN's role as the centralized operational lead. Analytically, these tables suggest that Indonesia's path toward global adequacy status requires a fundamental shift from a punitive, state-centric model of deterrence toward an independent, accountability-based framework. By establishing a truly autonomous data protection and cybersecurity watchdog, Indonesia would be better positioned to strengthen accountability, improve inter-agency coordination, and ensure consistent enforcement of digital rights protections. Such an institution could function independently from political and sectoral interests, enabling more effective oversight of data controllers, rapid responses to cyber incidents, and stronger remedies for victims of digital victimization. This institutional reform is particularly important as Indonesia increasingly faces threats within the "*Fifth Domain*" of warfare, cyberspace, where attacks on digital infrastructure, personal data, and public systems can destabilize governance without the use of conventional military force. In this context, protecting citizens' privacy is no longer solely a matter of individual rights, but also a strategic component of national resilience and sovereignty.

The urgency of this reform is further reinforced by the principles articulated in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, which provides the most comprehensive scholarly interpretation of how existing international law applies to cyberspace. Although the Manual is not legally binding, it is widely recognized as an authoritative reference for states in formulating national cyber governance frameworks. The Manual affirms that cyber operations targeting critical infrastructure, government information systems, or personal data may infringe state sovereignty and, depending on their scale and effects, constitute internationally wrongful acts or even trigger the application of the law governing the use of force. It further elaborates the principle of due diligence, requiring states to take reasonable measures to prevent their territory or cyber infrastructure from being used for cyber operations that cause serious harm to other states (Rules 6–8). Equally important, the Manual emphasizes that state responses to cyber threats must comply with the principles of necessity and proportionality, while respecting applicable international human rights obligations, including the rights to privacy and freedom of expression. These principles are particularly relevant to Indonesia, where national security legislation currently provides broad governmental authority to collect and process digital information without comprehensive statutory safeguards governing judicial authorization, oversight, data retention, or remedies for unlawful surveillance. Accordingly, harmonizing Indonesia's national security framework with the normative guidance of the Tallinn Manual requires incorporating clear legal standards that simultaneously strengthen the State's capacity to address cyber threats and ensure the effective protection of individuals against arbitrary or disproportionate interference with their digital rights.³⁷

In this case, Indonesia's fragmented cybersecurity governance and inconsistent implementation of the PDP Law reveal substantial gaps when measured against these international standards. Large-scale data breaches, ransomware attacks, and unauthorized dissemination of personal information demonstrate that Indonesia's digital ecosystem remains vulnerable to both criminal exploitation and strategic cyber threats. The absence of a fully independent supervisory authority further weakens legal enforcement and limits effective protection for victims. By adopting principles reflected in the Tallinn Manual, particularly the obligation to secure critical digital infrastructure and protect civilian data, Indonesia could develop a more coherent and resilient cyber governance model. Such harmonization would not only enhance domestic legal certainty and public trust but also reinforce Indonesia's position within the broader international effort to safeguard sovereignty and human rights in the digital era.

3.2. Digital Victimization and National Security: Problems and Challenges

Digital victimization represents a growing and complex challenge to Indonesia's national security, reflecting the convergence of technological, legal, and institutional vulnerabilities. In the

³⁷ Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), <https://www.onlinelibrary.iuhl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>.

context of rapid digitization of public services, citizens are required to submit highly sensitive personal and biometric data to government systems, such as *SatuSehat* for healthcare and immigration databases. The UU PDP 2022, Article 5, explicitly mandates that “Every Electronic System Provider must ensure the protection of the personal data processed”, legally imposing a duty on institutions to safeguard this data. Despite this clear statutory requirement, enforcement remains inconsistent, and many agencies operate without standardized protocols or sufficient technical capacity. Scholars such as Yar³⁸ argue that cybercrime arises from both the technological opportunity structure and social vulnerabilities, emphasizing that institutional gaps create conditions conducive to criminal exploitation.³⁹ From a criminological perspective, Cohen and Felson’s routine activity theory⁴⁰ explains how motivated offenders exploit systems lacking capable guardianship, making public digital infrastructure an attractive target. The 2024 ransomware attack on Indonesia’s National Data Center demonstrates how statutory obligations can fail in practice, exposing citizens to both direct harms, such as service disruption, and indirect harm, such as loss of trust in governance. This underscores that digital victimization is not merely a technical or individual issue but a systemic problem that intertwines legal compliance, institutional readiness, and societal consequences.

Digital victimization extends beyond conventional cybercrime by encompassing both individual and collective harms, including psychological distress, disruption of services, and societal erosion of trust. Victimology scholars, particularly Karmen,⁴¹ they argue that harm can manifest even without physical contact, making digital crimes uniquely insidious because they combine technical breaches with social and emotional consequences. Legally, the UU PDP 2022, Article 6, requires that “Electronic System Providers must process personal data lawfully, fairly, and limited to a clear purpose”, establishing a normative framework to protect citizens. However, in practice, many government agencies lack clear procedures for ensuring lawful processing, leaving citizens vulnerable to data misuse and unauthorized access. Clarke’s situational crime prevention theory⁴² provides a theoretical lens, arguing that reducing opportunity structures and strengthening guardianship are central to preventing crime. In the Indonesian context, the absence of integrated monitoring systems, combined with fragmented responsibilities among ministries, has created a permissive environment in which digital victimization can occur systematically. Citizens, therefore, experience a dual form of harm: they are victims of cybercrime and simultaneously victims of institutional failures that prevent the enforcement of legal protections. This dual victimization highlights the socio-legal complexity of Indonesia’s digital ecosystem, where the law exists but operational and cultural gaps exacerbate vulnerabilities, making digital victimization both pervasive and difficult to mitigate.

The intersection of digital victimization and national security reveals a critical dimension of vulnerability in Indonesia’s state apparatus. Disruptions in government digital infrastructure, particularly in health, immigration, and administrative systems, pose strategic risks by undermining essential services and public confidence. Article 15 of UU PDP 2022 explicitly

³⁸ Majid Yar, “Toward a Cultural Criminology of the Internet,” in *Technocrime and Criminological Theory*, ed. Kevin Steinmetz and Matt R. Nobles (Routledge, 2017), <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315117249-8/toward-cultural-criminology-internet-majid-yar>.

³⁹ Daffa Irfan Mahendra, “Polarization, Hate Speech, and Democracy: Social Media Discourse During Indonesia’s 2019 Elections,” *Indonesian Discourse on Communication, Democracy, and Political Movements* 1, no. 2 (2024), <https://journal.perhaki.org/index.php/indepolcom/article/view/618>.

⁴⁰ Lawrence E. Cohen and Marcus Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach,” *American Sociological Review* 44, no. 4 (1979): 588–608, <https://doi.org/10.2307/2094589>.

⁴¹ Andrew Karmen, “The Controversy over Shared Responsibility: Is Victim-Blaming Ever Justified?,” in *To Be a Victim*, ed. D. Sank and D.I. Caplan (Boston: Springer, 1991), 395–408, https://doi.org/10.1007/978-1-4899-5974-4_24.

⁴² Ronald V. Clarke, “Situational Crime Prevention,” *Crime and Justice* 19 (1995): 91–150, <https://www.journals.uchicago.edu/doi/abs/10.1086/449230>; R. V. G. Clarke, “‘Situational’ Crime Prevention: Theory and Practice,” in *Crime Opportunity Theories* (Routledge, 2011), <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315095301-21/situational-crime-prevention-theory-practice-clarke>.

obliges agencies to implement technical and administrative safeguards: “Every Electronic System Provider must implement technical and administrative measures to protect personal data from loss, theft, or unauthorized access”. Yet, the gap between statutory requirements and operational enforcement remains significant. Nye⁴³ frames cyber threats as “*soft power coercion*,” in which attacks can destabilize institutions without the use of kinetic force, exemplifying how digital victimization can escalate into national security threats. Routine activity theory suggests that the lack of capable guardianship creates opportunities for attackers, who exploit both technological weaknesses and institutional gaps. Victimology perspectives extend this analysis, emphasizing that citizens collectively experience harm when public systems fail, eroding social trust and the perceived legitimacy of the state. In Indonesia, the uneven application of protective measures has left legal provisions intended to secure infrastructure aspirational in practice. Consequently, digital victimization is both a socio-legal and a national security problem, in which systemic weaknesses, legal non-compliance, and insufficient enforcement converge to amplify the consequences of cyberattacks.

The June 2024 ransomware attack on Indonesia’s National Data Center exemplifies the systemic challenges of digital victimization. Over 200 government institutions, including health, immigration, and administrative services, were severely disrupted. Article 17 of UU PDP 2022 requires that “Personal data breaches must be reported to the Data Protection Authority and the data subject without undue delay”, yet reporting was inconsistent, highlighting gaps in implementation. Victimologically, citizens experienced harm not only in service disruption but also psychologically, as the breach undermined trust in the state’s capacity to protect data. Criminologically, the attack demonstrates how motivated offenders exploit systemic weaknesses and organizational fragmentation, aligning with Clarke’s situational crime prevention theory, which posits that crimes are more likely where guardianship is weak. Yar⁴⁴ notes that digital victimization often results from both opportunity structures and governance failures, emphasizing that attacks are rarely purely technical in nature. This incident underscores the dual nature of Indonesia’s challenge: even with statutory protection under UU PDP, operational gaps and institutional deficiencies leave citizens and institutions vulnerable to complex, cascading harms spanning legal, social, and strategic dimensions.

The ransomware attack revealed extensive systemic vulnerabilities in the delivery of public services. Disruption of *SatuSehat* delayed access to healthcare, while immigration and licensing systems became temporarily nonfunctional (see Table 4). Article 15 of UU PDP 2022 requires protective measures, including periodic risk assessments, yet most agencies had limited capacity to implement these provisions effectively. Criminological analysis suggests that this gap between law and practice increases the opportunity for cybercrime, as weak guardianship and fragmented responsibilities leave digital assets exposed. Victimology perspectives highlight that harm extends beyond direct service denial: citizens experience collective vulnerability, fear, and diminished confidence in governance. Scholars like Grabosky⁴⁵ argue that regulatory frameworks without practical operationalization are insufficient to reduce risk. The Indonesian case demonstrates that even robust statutory language cannot guarantee protection when institutions lack the capability, culture, and coordination to operationalize these obligations, resulting in amplified digital victimization and societal disruption.

⁴³ Joseph S. Nye, “Normative Restraints on Cyber Conflict,” 2017, https://www.sipa.columbia.edu/sites/default/files/2022-11/Nye_Normative_Restraints_on_Cyber_Conflict_0502.pdf.

⁴⁴ Yar, “Toward a Cultural Criminology of the Internet”; Sherry Hamby et al., “Digital Poly-Victimization: The Increasing Importance of Online Crime and Harassment to the Burden of Victimization,” in *Polyvictimization: Adverse Impacts in Childhood and Across the Lifespan*, ed. Julian D. Ford and Brianna C. Delker (London: Routledge, 2019), 112–128, <https://www.routledge.com/Polyvictimization-Adverse-Impacts-in-Childhood-and-Across-the-Lifespan/Ford-Delker/p/book/9780367729509>; Rachel L. McNealey and Adam Ghazi-Tehrani, “Risky Digital Behavior or Risky Digital Places? Victimization Risk Perception and Evaluation on the Internet,” *Journal of Crime and Justice* 47, no. 4 (2024): 530–44, <https://doi.org/10.1080/0735648X.2023.2244927>.

⁴⁵ Peter N Grabosky, “Virtual Criminality: Old Wine in New Bottles?,” *Social & Legal Studies* 10, no. 2 (2001), <https://doi.org/10.1177/a017405>.

Trust is a central dimension of both governance and victimology. In Indonesia, inconsistent enforcement of UU PDP provisions has eroded public confidence in government institutions. Article 5 obliges electronic system providers to ensure the protection of personal data, yet the absence of uniform implementation and transparency in reporting breaches undermines this statutory mandate. Victimology emphasizes that the harm of cyber incidents includes social and psychological dimensions, particularly when citizens perceive the state as incapable or negligent. Levi⁴⁶ notes that institutional legitimacy depends on the consistent application of law, which is essential for compliance and societal stability. In Indonesia, operational gaps create a perception that legal obligations are symbolic rather than enforceable, exacerbating the impact of digital victimization. Citizens are thereby subjected to a dual form of harm: the technical disruption of services and the erosion of the social contract, reflecting the interdependence among legal enforcement, organizational capacity, and societal trust.

Technical weaknesses, such as outdated infrastructure, insufficient cybersecurity protocols, and inadequate monitoring systems, compound Indonesia's vulnerability. Article 15 of UU PDP mandates that institutions implement both technical and administrative safeguards, but fragmented responsibilities and resource limitations hinder practical compliance.⁴⁷ Clarke's situational crime prevention theory suggests that reducing opportunity structures and strengthening guardianship are central to crime mitigation.⁴⁸ Victimology emphasizes that individuals and collectives are harmed when systemic vulnerabilities exist, as cyberattacks exploit gaps in protection and coordination. Indonesia's recurring cybersecurity incidents reveal that even strong statutory language cannot prevent digital victimization when implementation capacity is limited, highlighting the centrality of operational readiness as a complement to legal frameworks.

Silo mentality among agencies exacerbates the challenges of implementing UU PDP provisions. Poor inter-agency communication, a lack of unified protocols, and limited data sharing impede timely threat detection and response.⁴⁹ Criminological theory identifies organizational fragmentation as a structural facilitator of crime, where weaknesses in coordination allow offenders to exploit vulnerabilities. Victimologically, this amplifies harm because citizens and institutions simultaneously become victims when systemic failures prevent effective mitigation. Articles 15 and 17 of UU PDP require coordinated protection and breach reporting, yet operational silos prevent agencies from fulfilling these obligations effectively. The silo mentality, therefore, represents both a procedural and strategic challenge, illustrating the complex interplay between statutory obligations, organizational culture, and systemic digital vulnerability.

Despite the comprehensive framework of UU PDP 2022, particularly Articles 5 through 17, significant gaps persist in legal implementation, exposing citizens to systemic digital victimization. Article 5 mandates the protection of personal data, while Article 6 requires lawful, fair, and purpose-limited processing. Article 15 obliges providers to implement technical and administrative safeguards, and Article 17 requires reporting of breaches without undue delay. However, in practice, government agencies often lack the capacity, standardized procedures, and technical infrastructure to comply effectively with these obligations. Grabosky⁵⁰ emphasizes that laws alone are insufficient to prevent crime if organizational and operational integration is weak. From a criminological perspective, routine activity theory explains that motivated offenders exploit these

⁴⁶ Margaret Levi, "The Who, What, and Why of Performance-Based Legitimacy," *Journal of Intervention and Statebuilding* 12, no. 4 (2018): 603–10, <https://doi.org/10.1080/17502977.2018.1520955>.

⁴⁷ Agus Bhakti et al., "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia," *Journal of Human Security* 20, no. 1 (2024): 109–17, <https://jhumansecurity.com/menuscript/index.php/jhe/article/view/210/152>; Muhammad Azza Ulin Nuha et al., "Reformulation of the Vulnerability Management Cycle for Enhancing Indonesia's Critical Information Infrastructure Protection: An International Comparative Study," *The Indonesian Journal of Computer Science* 14, no. 1 (2025): 322–37, <https://doi.org/10.33022/ijcs.v14i1.4609>.

⁴⁸ Clarke, "Situational Crime Prevention."

⁴⁹ Tedo Hindami Guna, Suparno Suparno, and Indra Kertati, "Breaking down Barriers: Overcoming Silo Mentality in Bureaucratic Reform," *Journal of Sustainability, Society, and Eco-Welfare* 2, no. 1 (2024): 16–28, <https://doi.org/10.61511/jssew.v2i1.2024.884>; Solikhah, "Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework."

⁵⁰ Grabosky, "Virtual Criminality: Old Wine in New Bottles?"

gaps in which legal compliance exists nominally but guardianship is weak; the system becomes an attractive target. Victimology highlights that citizens bear both direct and indirect harm: direct harm through unauthorized data access or service disruption, and indirect harm through anxiety, mistrust, and societal insecurity. Thus, the gap between statutory law and its operationalization is not merely administrative; it is a systemic enabler of digital victimization, underscoring the critical need for enforcement mechanisms that bridge the divide between legal provisions and real-world institutional capacity.⁵¹

The UU PDP 2022 explicitly establishes the state's fiduciary duty over citizens' personal data. Articles 15–17 collectively frame the government as a guardian responsible for implementing technical protections, administratively monitoring systems, and promptly reporting breaches. Article 17, for instance, requires reporting of breaches “without undue delay”, reflecting the urgency of transparency and accountability. Victimology underscores that when the state fails to uphold these duties, citizens experience systemic victimization: their trust, psychological security, and expectation of institutional protection are undermined. Karmen⁵² argue that this form of indirect harm is central to understanding victimization in the digital age. From a criminological standpoint, the combination of weak enforcement and fragmented institutional responsibility aligns with situational crime theory, which posits that inadequate guardianship increases the likelihood of crime. In Indonesia, the erosion of the social contract manifests in reduced citizens' confidence in governance and a reluctance to participate in state-mandated data systems fully. This duality of harm, both technical and social, demonstrates that digital victimization transcends the individual, extending to collective societal risk, and highlights that legal provisions alone cannot secure trust without effective, consistent, and transparent implementation.

Digital victimization in Indonesia has evolved into a serious socio-legal and national security issue, particularly as government institutions increasingly rely on digital systems to manage public services and personal data. Critical sectors such as healthcare, immigration, banking, and public administration remain vulnerable to cyberattacks, data leaks, and unauthorized access. Several

⁵¹ In further, the regulatory hybridization of UU PDP faces a grueling test in cases of Gender-Based Violence (GBV), where the gap between law and enforcement facilitates systemic victimization. While the law recognizes data rights, the lack of an independent oversight body creates a “protection vacuum” for victims of non-consensual intimate image sharing or digital stalking. The hybrid model's reliance on executive-linked agencies often prioritizes state stability over victim-centric recovery, leaving citizens to navigate a labyrinth of bureaucracy. This operational disconnect transforms administrative delays into secondary trauma, where institutional incapacity acts as a catalyst for prolonged societal mistrust and digital insecurity. For broader discussion, also see Sebastián Alejandro Morales and Andrés Castillo, “The Case of Gender Violence in Mexico: Does the Judicial System Ensure Substantive Justice for Victims? = El Caso de La Violencia de Género En México: ¿Garantiza El Sistema Judicial La Justicia Sustantiva Para Las Víctimas?,” *Crítica de La Justicia Sustantiva* 1, no. 2 (2025): 205–32, <https://publications.socipol.org/index.php/cjs/article/view/25>; Mateo Julián Ortega Ramírez, “Smart Cities, Smart Exclusion: The Digital Divide in Marginalized Neighborhoods,” *Revista de Justicia Social En La Sociedad Urbana* 1, no. 2 (2025): 181–214, <https://publications.socipol.org/index.php/rjs/article/view/29>; César Paredes Montoya and Isabel Aguirre Lozano, “Digital Disobedience: The Impact of Social Media on Collective Actions and Rebellions = Desobediencia Digital: El Impacto de Las Redes Sociales En Las Acciones Colectivas y Rebeliones,” *Revista de Desobediencia Comunitaria* 1, no. 2 (2025), <https://publications.socipol.org/index.php/rdc/article/view/34>; Wang Zhihao et al., “Digital Rights and Freedoms: The Fight for a Free Internet in Authoritarian Regimes,” *Revista de Derechos Humanos Contemporáneos* 1, no. 2 (2025): 347–76, <https://publications.socipol.org/index.php/rdh/article/view/40>.

⁵² Karmen, “The Controversy over Shared Responsibility: Is Victim-Blaming Ever Justified?” Furthermore, in this context, it is emphasized that while the law successfully adopts high-level international standards (GDPR), its operational reality is hindered by a “hybrid” enforcement structure that remains tied to the executive branch rather than being fully independent. According to Situational Crime Theory, this lack of a “capable guardian” not only fails to stop data crimes; it also creates the environment for them to occur. For a victim of digital violence, the harm isn't just the leaked data (direct harm); it is the anxiety and mistrust (indirect harm) caused by an administrative system that is legally present but functionally unable to provide immediate protection. Thus, the law becomes a “systemic enabler” of victimization because the gap between the written statute and real-world institutional capability remains unbridged.

incidents involving the exposure of citizens' personal information have demonstrated weaknesses in institutional cybersecurity and uneven implementation of the PDP Law. These vulnerabilities not only threaten the confidentiality and integrity of data but also undermine public trust in state institutions and digital governance. In this context, cyber threats should be understood not merely as technical disruptions but as systemic risks with social, legal, and strategic implications.

The growing scale of data breaches in Indonesia also raises important concerns about privacy protection and the recognition of the "*right to be forgotten*." This principle, partially accommodated under the EIT Law, grants individuals the right to request the deletion of irrelevant or harmful digital information that undermines their dignity and privacy.⁵³ However, in practice, the implementation of this right remains inconsistent due to unclear procedural mechanisms, overlapping institutional authority, and limited public awareness. Victims of digital harassment, revenge porn, defamation, and unauthorized dissemination of personal information often continue to suffer long-term psychological and social consequences because harmful content remains permanently accessible online.⁵⁴ As a result, digital victimization extends beyond the initial cyber incident and becomes a continuing violation of personal rights in cyberspace.

From a victimology and criminology perspective, both individuals and state institutions can be viewed as co-victims of cybercrime and weak data governance. Routine activity theory explains that cyber offenders are more likely to exploit systems lacking adequate protection, particularly within fragmented institutional structures. At the same time, ineffective enforcement of data protection obligations and the limited realization of the right to be forgotten contribute to prolonged victimization and legal uncertainty. Therefore, strengthening Indonesia's cyber defense architecture requires not only technical safeguards but also clearer legal harmonization, stronger institutional coordination, and victim-centered policies that ensure accountability, protect privacy, and enforce digital rights effectively.

When compared with countries that have centralized cybersecurity authorities and independent oversight, Indonesia demonstrates statutory ambition but operational weakness. Wall⁵⁵ argues that effective cybercrime prevention requires integration of legal frameworks, technical capacity, and organizational coordination. While UU PDP 2022 provides robust legal obligations through Articles 5–17, fragmented enforcement, lack of monitoring, and limited technical capacity hinder compliance. Victimology reinforces the idea that collective harm is magnified when regulatory and operational mechanisms are insufficient, as the broader citizenry bears the indirect consequences of systemic failures. This comparative perspective underscores that legal provisions without functional institutional architecture are inadequate. Indonesia's challenges demonstrate that bridging the law-implementation gap requires investment in capacity building, inter-agency collaboration, and independent supervision. Failure to address these issues perpetuates the cycle of digital victimization, undermining both citizen welfare and national security.

To address systemic problems, Indonesia must focus on strengthening the enforcement of UU PDP Articles 5–17, ensuring that agencies implement consistent technical and administrative safeguards, maintain proper monitoring, and comply with breach-reporting requirements. Clarke's situational crime prevention theory⁵⁶ emphasizes reducing opportunity structures and enhancing capable guardianship to prevent crime. Victimology emphasizes safeguarding both individual and collective rights, recognizing that citizens' trust and psychological security are integral to societal resilience. Policies must therefore combine legal enforcement, operational capacity, inter-agency coordination, and technical resilience. Without integrating these dimensions, statutory protection

⁵³ Putri Zaltina and Lidwina Inge Nurtjahyo, "Right to Be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases," *The Indonesian Journal of Socio-Legal Studies* 3, no. 2 (2024), <https://doi.org/10.54828/ijsls.2024v3n2.4>.

⁵⁴ Uni Tsulasi Putri, Irna Nurhayati, and Taufiq El Rahman, "Legal Challenges of the Application of the Right to Be Forgotten in Blockchain in Indonesia and the European Union," *Jambura Law Review* 7, no. 2 (2025): 633–63, <https://doi.org/10.33756/jlr.v7i2.30514>.

⁵⁵ David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (New York: John Wiley & Sons, 2024).

⁵⁶ Clarke, "Situational Crime Prevention."

remains aspirational rather than functional, leaving citizens and institutions vulnerable to increasingly sophisticated digital threats.

Human factors are critical determinants of both vulnerability and resilience in digital systems. Training government personnel, conducting awareness programs, and developing clear operational protocols are essential for translating statutory requirements into practice. UU PDP Articles 15 and 17 provide the legal foundation for these measures, mandating protective action and prompt reporting of breaches. However, gaps in enforcement and limited technical expertise hinder effective compliance. Criminological theory highlights that human error and weak procedural culture increase susceptibility to crime, while victimology stresses that inadequate protection amplifies harm to citizens, both individually and collectively. In Indonesia, addressing capacity-building gaps is as critical as strengthening technical infrastructure, as failure to integrate human, legal, and technological dimensions perpetuates digital victimization and erodes public confidence in state institutions.

Indonesia faces multifaceted challenges in addressing digital victimization, marked by gaps between statutory provisions and their practical implementation. Articles 5–17 of UU PDP 2022 provide a robust legal framework, yet inconsistent enforcement, silo mentality, limited technical capacity, and fragmented governance leave citizens and institutions exposed. Victimology highlights both individual and collective harms, including psychological distress, social vulnerability, and loss of trust, while criminological theories explain how systemic gaps create opportunities for offenders. The June 2024 ransomware attack exemplifies how operational and legal shortcomings converge to amplify societal risk. Addressing these challenges requires a holistic approach that aligns statutory obligations with operational capacity, strengthens inter-agency coordination, invests in human and technical resources, and embeds cybersecurity as a strategic national priority to protect citizens, uphold the social contract, and secure national infrastructure against evolving digital threats.

Table 4.
Digital Victimization and National Security: Indonesia in a Global Context

Aspect / Indicator	Indonesia (2024 Data)	Global Comparison (Selected Cases)	Implications for National Security
Major Incident	Ransomware attack on the National Data Centre (Pusat Data Nasional – Pusat Data Nasional Sementara 2, Surabaya) in June 2024. Services disrupted: immigration, education, and civil service. Attackers: Brain Cipher (LockBit 3.0 variant). Ransom demand: USD 8 million.	Colonial Pipeline ransomware attack (United States, 2021) disrupted fuel supply; WannaCry (2017) affected 150+ countries.	Demonstrates the vulnerability of critical infrastructure and the disruption of essential state functions.
Volume of Cyber Anomalies	The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara) reported 330 million anomalous traffic events in 2024. Top threats: ransomware, phishing, and botnets. Mirai Botnet alone: 81 million anomalies.	Global ransomware damage is projected to reach USD 265 billion annually by 2031 (Cybersecurity Ventures).	Scale of attacks shows systemic exposure; Indonesia mirrors global escalation but with weaker resilience.
Institutional Response	The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara) coordinates cyber defense. Still, a fragmented regulatory environment with overlapping mandates (Ministry of Communication and	Countries like the United States and the European Union have centralized Computer Emergency Response Teams (CERTs) and harmonized data	Fragmentation weakens Indonesia's ability to respond quickly and align with global standards.

Aspect / Indicator	Indonesia (2024 Data)	Global Comparison (Selected Cases)	Implications for National Security
	Informatics, Indonesian National Police, National Cyber and Crypto Agency) limits crisis coordination during the National Data Centre attack.	protection laws (e.g., the GDPR).	
Data Protection Framework	Draft Cyber Security and Resilience Bill (2025) under discussion; Personal Data Protection Law (2022) enacted, but implementation remains uneven.	The European Union's GDPR (2018) sets a global benchmark; ASEAN countries are adopting harmonized frameworks.	Regulatory gaps hinder Indonesia's compliance with global norms and weaken trust in digital governance.
Victimology Perspective	Millions of civil servant and taxpayer records exposed; public trust eroded; limited victim support mechanisms.	Global trend: victim-centered approaches emerging (e.g., European Union's emphasis on data subject rights).	Highlights need to integrate victimology and criminology into cyber defense strategies.

Source: Various sources, edited by the authors

Taken together, the preceding analysis reveals that digital victimization in Indonesia is not merely a function of technical vulnerabilities but is deeply embedded within legal, institutional, and socio-political structures. The interplay between statutory obligations, fragmented implementation, and evolving cyber threats illustrates a systemic challenge in which citizens and state infrastructure are simultaneously exposed to risk. Understanding these vulnerabilities requires a holistic perspective that situates domestic experiences within broader global cybersecurity trends, where transnational actors, ransomware syndicates, and evolving attack vectors shape the threat landscape. Building on this understanding, the next section critically examines the regulatory and institutional frameworks underpinning Indonesia's cyber defense, interrogating their operational efficacy, structural limitations, and compliance with international standards. By examining both formal legal provisions and practical enforcement mechanisms, this discussion illuminates how Indonesia navigates the tension between normative cybersecurity ideals and the practical realities of safeguarding critical infrastructure and citizen data in an increasingly interconnected digital environment.

3.3. Victimology and Criminology Perspectives in Cybersecurity Discourse

The application of criminology to cybersecurity allows for a systematic understanding of offender behavior, opportunity structures, and systemic vulnerabilities that facilitate digital crime. Routine Activity Theory⁵⁷ is particularly instructive. It posits that crime occurs when three elements converge: motivated offenders, suitable targets, and the absence of capable guardianship. In Indonesia, digital systems such as *SatuSehat*, e-government platforms, and educational networks represent highly suitable targets due to the concentration of sensitive personal and institutional data. Motivated offenders range from individual opportunists to organized transnational cybercriminals exploiting economic incentives, weak legal enforcement, and globalized digital infrastructure. The absence of capable guardianship, manifested in fragmented institutional coordination, silo mentality across ministries, and inconsistent enforcement of UU PDP 2022, Articles 5, 15, and 17, creates an environment conducive to cybercrime. This convergence explains the prevalence of ransomware attacks, data breaches, and illegal fintech operations, illustrating how routine activity theory transcends physical crime to apply directly to digital victimization.

⁵⁷ Cohen and Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach."

Beyond Routine Activity Theory, which frames crime as arising from the convergence of motivated offenders, suitable targets, and the absence of capable guardians, Rational Choice Theory offers a complementary, more nuanced understanding of offender behavior in cyberspace. Rational Choice Theory⁵⁸ assumes that offenders are deliberate, calculating actors who weigh potential risks and rewards before committing a crime. This perspective treats crime not as random or impulsive but as a series of strategic decisions made within an environment of opportunities and constraints. In Indonesia, the ransomware attack on the National Data Center exemplifies this logic: attackers deliberately targeted a system storing sensitive citizen data, calculating that enforcement mechanisms were fragmented, institutional monitoring was weak, and immediate penalties were unlikely to materialize. From a criminological standpoint, this demonstrates that digital victimization arises not from isolated mistakes or technological malfunctions alone but from systemic vulnerabilities, including inconsistent implementation of UU PDP 2022, particularly Articles 5, 15, and 17, which mandate protection of personal data, technical safeguards, and breach reporting. The attackers' decision-making reflects the rational evaluation of opportunity structures within Indonesia's cyber infrastructure, showing that weak oversight and delayed institutional response amplify both the probability and impact of cybercrime.

Routine Activity Theory complements Rational Choice by highlighting the structural conditions that make crimes possible. In cyberspace, suitable targets include large databases, critical infrastructure, or digital systems containing high-value personal, financial, or institutional data. Motivated offenders can range from opportunistic individuals to highly organized transnational criminal groups. The absence of capable guardianship is particularly evident in Indonesia, where siloed agencies, limited inter-institutional coordination, and uneven enforcement of existing laws create gaps in surveillance, incident response, and risk mitigation. The National Data Center attack illustrates this convergence: high-value digital assets existed alongside weak protective oversight, allowing rational offenders to exploit institutional gaps with minimal resistance. Routine Activity Theory thus emphasizes that digital victimization is not only the result of individual vulnerability but also the product of structural and organizational weaknesses in governance and cybersecurity management.

Meanwhile, Strain Theory, as emphasized by Merton⁵⁹ adds a socio-economic dimension, explaining how structural pressures can influence offender behavior. Strain Theory posits that when individuals are unable to achieve socially accepted goals (e.g., economic stability or social mobility) through legitimate means, they may adopt alternative or illicit pathways. In the Indonesian context, low digital literacy, high connectivity, and limited formal employment opportunities can create pressures that incentivize opportunistic cybercrime. Illegal online lending operations, phishing schemes, and ransomware attacks by less-organized offenders can thus be understood as adaptive responses to socio-economic strain rather than purely technological exploitation. Strain Theory highlights that cybercrime is embedded within broader social structures: digital victimization is not only a technical or legal problem but also a societal one, reflecting inequalities, education gaps, and uneven access to institutional protection.

Integrating these three criminological perspectives provides a comprehensive lens for analyzing digital victimization. Rational Choice Theory explains the deliberate, calculated behaviors of offenders who exploit systemic weaknesses; Routine Activity Theory emphasizes how structural opportunities, such as weak guardianship, high-value targets, and decentralized

⁵⁸ Ronald V. Clarke and Derek B. Cornish, "Rational Choice and Routine Activities," in *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*, ed. Raymond Paternoster and Ronet Bachman (Roxbury Publishing Company, 2001), 23–42; Travis Hirschi, "On the Compatibility of Rational Choice and Social Control Theories of Crime," in *The Reasoning Criminal* (Routledge, 2014), <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315134482-7/compatibility-rational-choice-social-control-theories-crime-travis-hirschi>.

⁵⁹ Robert K. Merton, *Social Theory and Social Structure* (Sydney: Simon and Schuster, 1968); Robert Agnew, "Revitalizing Merton: General Strain Theory," in *The Origins of American Criminology*, ed. Francis T. Cullen et al. (London: Routledge, 2017), 137–58, <https://www.routledge.com/The-Origins-of-American-Criminology-Advances-in-Criminological-Theory/Cullen-Jonson-Myer-Adler/p/book/9781138516557>.

systems, enable crime; and Strain Theory contextualizes cybercrime within socio-economic pressures that motivate opportunistic offending. The victims of these crimes, including citizens, institutions, and critical infrastructure, experience multifaceted harm: financial loss, psychological stress, erosion of trust in state institutions, and broader social disruption. From a victimological standpoint, this underscores that cyber victims are not passive; they are stakeholders whose protection is central to maintaining public trust and national digital resilience.

By linking these theories to the Indonesian context, several policy implications emerge. Strengthening institutional guardianship through better coordination between agencies, improving digital literacy, and enforcing data protection under UU PDP 2022 Articles 5, 15, and 17 can reduce the opportunities available to rational offenders. Additionally, socio-economic interventions, such as digital education, legal employment pathways in IT, and public awareness campaigns, can mitigate the strain factors that incentivize opportunistic cybercrime. Together, these measures operationalize criminological insights into a human-centered cybersecurity strategy, demonstrating that effective digital defense requires integrating technological, legal, and social dimensions.

Furthermore, in the same context as this study, victimology provides a critical lens for understanding cybercrime, moving beyond the perception of victims as passive recipients of harm. By analyzing specific victimology theories, we can see that digital victimization manifests across psychological, social, and economic dimensions, often extending well beyond immediate financial or data loss. Condry's framework of secondary victimization⁶⁰ highlights how institutional failures, insufficient protections, and societal neglect can exacerbate harm, increasing psychological distress and social stigma for victims. In Indonesia, illegal online lending platforms exemplify this dynamic: beyond financial losses, victims endure harassment, reputational damage, and ongoing anxiety. These compounded effects illustrate that the harm is not merely material; it involves complex social and emotional dimensions that require careful recognition and intervention by both the state and relevant institutions.

Further, transactional victimology theory⁶¹ conceptualizes victimization as an ongoing interaction between offender, victim, and broader social context. In Indonesia, ransomware attacks on universities and schools demonstrate how such attacks can disrupt entire institutional ecosystems. Students face interrupted academic progression, faculty lose access to research data, and administrative systems collapse, creating cascading social and economic consequences. The theory underscores that victims are not isolated; their experiences are deeply interdependent with the institutional structures that are supposed to safeguard them. This framework highlights the need for proactive institutional measures, emphasizing the victim as an active stakeholder in both prevention and remediation.

These victimology perspectives demonstrate that effective cybersecurity policy must centralize victim protection as a core element of national resilience. In the Indonesian context, this includes aligning policy with UU PDP 2022, particularly Articles 5, 15, and 17, which mandate personal data protection, technical safeguards, and breach reporting. Victims' rights, trust, and well-being are intertwined with state legitimacy and social stability, making the protection of citizens a strategic imperative for national security. By foregrounding victim experiences, policymakers can design a human-centered cyber defense that addresses both systemic vulnerabilities exploited by offenders and the social consequences of digital victimization, ensuring that cyber governance is not merely reactive but anticipatory, equitable, and socially accountable.

Integrating victimology and criminology provides a multidimensional perspective that connects offender behavior, institutional vulnerabilities, and harm to citizens. Situational crime

⁶⁰ Rachel Condry, "Secondary Victims and Secondary Victimization," in *International Handbook of Victimology* (Routledge, 2010), <https://www.taylorfrancis.com/chapters/edit/10.1201/EBK1420085471-16/secondary-victims-secondary-victimization-rachel-condry>.

⁶¹ Ezzat A. Fattah and Vincent F. Sacco, "Age as a Victimological Variable," in *Crime and Victimization of the Elderly* (New York: Springer, 1989), 148–166, https://link.springer.com/chapter/10.1007/978-1-4613-8888-3_7.

prevention theory⁶² offers actionable insights: strengthening access controls, improving system monitoring, and implementing real-time incident response reduces opportunity structures exploited by offenders. When combined with victimological insight, such strategies are refined to prioritize protection of the most vulnerable populations, including those with low digital literacy, high exposure to online financial services, or dependence on public digital infrastructure. Legal instruments, particularly UU PDP 2022, operationalize these principles by mandating both preventive measures (Articles 5 and 15) and reactive obligations (Article 17) for breach reporting, aligning theoretical insights with enforceable policy measures.

Additionally, criminology illuminates the adaptive strategies of offenders in response to regulatory environments. As enforcement remains uneven, offenders evolve methods to circumvent controls, exploit legal ambiguities, and manipulate human error, a phenomenon aligned with the concept of “criminal innovation” in digital spaces. Victimology emphasizes that such adaptive behavior increases exposure to harm, particularly for populations least able to respond effectively. For example, in illegal online lending, perpetrators continuously refine phishing, impersonation, and social engineering tactics, while institutional enforcement remains reactive, illustrating the interplay between offender rationality and systemic weaknesses.

3.4. Harmonization Model of Indonesia's National Security and Privacy Protection Framework

The preceding analysis demonstrates that Indonesia's legal framework has not yet achieved an optimal balance between national security interests and the protection of individuals against digital victimization.⁶³ This study therefore proposes a harmonization model that balances Indonesia's sovereign security interests with robust consumer protection, which should be translated into concrete legal norms through targeted amendments to existing legislation rather than the enactment of an entirely new statute. This approach is consistent with Indonesia's legislative framework because the principal laws governing personal data protection, electronic information, and national security already provide the institutional foundation upon which additional safeguards can be built. Accordingly, the proposed reform adopts a *ius constituendum* perspective by recommending amendments to the Personal Data Protection Law, the State Intelligence Law, and the Electronic Information and Transactions Law, complemented by implementing Government and Presidential Regulations. Together, these reforms establish a coherent legal framework that integrates national security objectives with internationally recognized privacy and human rights standards.

The first and most significant reform should be incorporated into Law No. 27 of 2022 on Personal Data Protection (PDP Law). Although the PDP Law recognizes the protection of personal data as a fundamental right, it does not comprehensively regulate state access to personal data for national security purposes or provide explicit protection against digital victimization arising from government surveillance or unauthorized data processing.⁶⁴ The proposed amendment, therefore, introduces a new provision establishing the principle that any personal data processing conducted for national security purposes must comply with the principles of legality, necessity, proportionality, accountability, and respect for human rights. These principles, widely reflected in international privacy frameworks, ensure that national security exceptions remain narrowly tailored and do not become blanket justifications for excessive state intrusion. The amendment should further clarify that restrictions on privacy rights

⁶² Clarke, “Situational Crime Prevention.”

⁶³ Dahlia Putri Amanda, Damar Sinatrio Putra, and Siti Mahira Ahmad Mubarak, “Digital Identity Theft and Criminal Protection of Personal Data in Indonesia,” *Indonesian Journal of Digital Crime and Criminal Justice* 2, no. 1 (2026): 107–46, <https://journal.criminallawinstitute.org/JDCCJ/article/view/24>; Bunga Maulidina Lestari and Ahmad Fauzi, “The Role of Victims of NCT Concert Ticket Fraud Via Social Media: A Cyber Victimology Perspective,” *Indonesia Justice Spectrum* 1, no. 1 (2026): 119–46, <https://journal.criminallawinstitute.org/IJS/article/view/10>.

⁶⁴ Indah Sri Utari, Ridwan Arifin, and Sergi Fernandez Alejandro, “Gender-Based Violence and the Implementation of the Sexual Violence Crime Law in Indonesia,” *The Indonesian Journal of Feminist Legal Studies* 1, no. 1 (2026): 1–32, <https://inleads.id/publications/index.php/IJFLS/article/view/1>.

may only be imposed under express statutory authority and only to the extent necessary to protect legitimate national security interests.

A second proposed amendment to the PDP Law should regulate government access to personal data by defining the circumstances under which intelligence and law enforcement agencies may obtain personal information. Access should be limited to clearly defined objectives, including the prevention of terrorism, the investigation of serious cybercrime, the protection of national defense, and the response to imminent threats to public safety.⁶⁵ To prevent arbitrary surveillance, the law should require prior judicial authorization for access, except in narrowly defined emergencies where immediate action is necessary. Even in emergency cases, the responsible agency should be required to obtain judicial review within a prescribed period, such as seventy-two hours, thereby preserving both operational flexibility and judicial oversight. This provision reflects the internationally accepted principle that state surveillance must be subject to independent authorization and effective legal accountability.

The amended PDP Law should also explicitly recognize digital victimization as a legally protected harm. Existing legislation primarily regulates unlawful data processing in terms of data controllers' obligations, but provides limited recognition of the individual harms resulting from digital exploitation. A new provision should therefore define digital victimization to include unauthorized disclosure of personal data, unlawful surveillance, identity theft, cyber harassment facilitated through personal data misuse, and harmful algorithmic profiling. By codifying these forms of victimization, the law would provide greater legal certainty regarding the rights of affected individuals while acknowledging that digital harms extend beyond purely economic losses to encompass psychological, reputational, and social injuries.

To complement these substantive rights, the PDP Law should establish comprehensive remedies for victims of unlawful personal data processing. Individuals whose data have been unlawfully processed by public authorities or private entities should be entitled to compensation for material and non-material damages, deletion of unlawfully obtained data, cessation of illegal processing activities, and rehabilitation where reputational or psychological harm has occurred.⁶⁶ Providing explicit legal remedies strengthens consumer protection while reinforcing institutional accountability by ensuring that violations carry meaningful legal consequences.

The proposed harmonization model also requires amendments to Law No. 17 of 2011 on State Intelligence. The current legal framework grants intelligence agencies broad investigative powers without sufficiently detailed procedural safeguards governing the collection and retention of personal data.⁶⁷ A revised statutory framework should require intelligence agencies to obtain judicial authorization before conducting interceptions or collecting personal data relating to Indonesian citizens, except in strictly defined emergencies. Such judicial authorization would not impede legitimate intelligence operations but would instead strengthen their constitutional legitimacy by ensuring that surveillance activities are subject to independent legal review.

In addition, the State Intelligence Law should establish an independent supervisory mechanism to review the legality, necessity, proportionality, and accountability of intelligence data

⁶⁵ Yasmin Cantika et al., "The Role of International Law in Addressing State-Sponsored Cyber Operations," *Indonesian Journal of Digital Crime and Criminal Justice* 1, no. 2 (2025): 347–76, <https://journal.criminallawinstitute.org/JDCCJ/article/view/30>; Ardhitama Sucahyanto, "Digital Society and the Transformation of Community-Based Dispute Resolution in Indonesia," *The Indonesian Journal of Sociolegal Development* 1, no. 1 (2026): 57–78, <https://inleads.id/publications/index.php/IJSLD/article/view/14>; Muhammad Abdurrahman, "Digital Surveillance, State Power, and Civil Liberties in Contemporary Indonesia," *The Indonesian Journal of Critical Legal Studies* 1, no. 1 (2026): 57–88, <https://inleads.id/publications/index.php/IJCLS/article/view/19>.

⁶⁶ Suraji Suraji and Ipop Abdi Prabowo, "Harmonizing Privacy Rights Protection in Electronic Transaction with Roscoe Pound's Legal Principle," *Indonesian Journal of Advocacy and Legal Services* 7, no. 1 (2025): 71–94, <https://doi.org/10.15294/ijals.v7i1.22331>.

⁶⁷ Supeno, Rosmidah, and Iqbal, "Personal Data Protection in Review of Legal Theories and Principles"; Junaidi Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil, "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory," *Journal of Law and Legal Reform* 5, no. 2 (2024): 587–612, <https://journal.unnes.ac.id/journals/jllr/article/view/3437>.

collection activities. Independent oversight has become an essential feature of democratic national security governance because it promotes transparency while protecting sensitive operational information. The supervisory body should have the authority to audit intelligence practices, review complaints regarding unlawful surveillance, and submit periodic reports to the legislature on compliance with statutory safeguards. Such institutional oversight enhances public confidence without compromising national security objectives. Another essential amendment concerns the retention and destruction of personal data collected for national security purposes. Intelligence agencies should be legally required to retain personal data only for the minimum period necessary to achieve the lawful objective for which the data were collected. Once that objective has been fulfilled, the information should be securely destroyed unless continued retention is expressly required by law or authorized by judicial order. This principle reflects internationally recognized standards of data minimization and storage limitation, reducing the risk of unnecessary government accumulation of personal information while preserving operational effectiveness.

Beyond statutory amendments, the harmonization model should be supported by a new Government Regulation specifically governing personal data processing for national security purposes. This implementing regulation would provide detailed operational procedures that cannot be comprehensively addressed within the primary legislation. The regulation should define categories of national security data; establish standardized procedures for requesting and approving government access to personal information; specify documentation requirements demonstrating legal necessity and proportionality; regulate judicial authorization procedures; determine retention periods; prescribe independent auditing mechanisms; and establish transparency reporting obligations. It should also create clear administrative procedures through which victims of unlawful data processing may seek remedies without undermining legitimate national security operations.

In addition, a Presidential Regulation should be adopted to strengthen institutional coordination between agencies responsible for cybersecurity, intelligence, law enforcement, and personal data protection. The regulation should establish national standards for privacy impact assessments, cybersecurity audits, inter-agency information sharing, digital victim assistance mechanisms, and annual public transparency reports concerning government data access practices. Rather than creating new substantive rights, the Presidential Regulation would facilitate consistent implementation of statutory obligations while improving administrative coordination among the institutions responsible for balancing national security with the protection of individual rights.

Table 5.
Proposal for Legal Harmonization for Privacy Protection in Indonesia

Regulatory Instrument	Proposed Reform	Key Articles
Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Amendment	Digital victimization, government access safeguards, national security exceptions, remedies
Law No. 11 of 2008, as amended by Law No. 1 of 2024 (Electronic Information and Transactions/EIT Law)	Limited amendment	Protection against unlawful digital surveillance and cyber-harassment
Law No. 17 of 2011 on State Intelligence	Amendment	Judicial authorization, proportionality, oversight, accountability
Government Regulation (PP) on National Security Data Processing (<i>new</i>)	Implementing regulation	Operational procedures for lawful access to personal data
Presidential Regulation (Perpres) on Cybersecurity and Digital Rights Protection (<i>new</i>)	Coordination regulation	Institutional coordination and oversight mechanisms

Source: Various sources, compiled and analyzed by the Authors

Taken together, these proposed legislative reforms constitute a comprehensive harmonization model that aligns Indonesia's national security framework with global privacy standards while preserving the State's sovereign responsibility to protect national security. The model is structured around three mutually reinforcing pillars: lawful national security measures, robust procedural safeguards grounded in legality, necessity, proportionality, and accountability, and effective consumer protection through legally enforceable rights and remedies for victims of digital harm. By embedding these principles within Indonesia's existing legal framework, the proposed reforms offer a balanced and coherent normative model that can address the growing challenges of digital victimization without undermining legitimate national security functions.

4. Conclusion

This study concluded that digital victimization in Indonesia is a tangible and multifaceted phenomenon that impacts citizens, institutions, and national security alike. Rapid digitalization, high connectivity, and global data flows have created structural vulnerabilities that extend beyond technical failures, exposing both individuals and state systems to financial, social, and psychological harm. Cases such as ransomware attacks on public institutions and illegal fintech operations illustrate how digital victimization is systemic, reflecting not only technological gaps but also socio-legal and institutional weaknesses. The research highlights that effective cybersecurity must address the interplay between offender behavior, systemic vulnerabilities, and victim experiences, emphasizing a human-centered, socio-legal approach rather than a purely technical or regulatory response.

From a scholarly perspective, this analysis contributes to integrating criminology and victimology theories into cybersecurity discourse, advancing understanding of digital victimization as both a social and a security issue. By applying Routine Activity, Rational Choice, and Strain Theories alongside modern victimology frameworks, the study elucidates how offender strategies, institutional deficiencies, and victim vulnerabilities intersect to create cascading harms. It also situates Indonesia within the broader global cyber landscape, showing how national legal instruments, such as UU PDP 2022, and institutional mechanisms can be operationalized to bridge the gap between theoretical frameworks and practical governance. This interdisciplinary approach reinforces the argument that cybersecurity must be conceived as a holistic system that balances technological defenses, legal compliance, and citizen protection.

Looking ahead, future research should explore the dynamic interactions among emerging technologies, regulatory enforcement, and citizen resilience, particularly in contexts of AI-driven cybercrime, transnational attacks, and evolving data ecosystems. Empirical studies on the effectiveness of institutional coordination, public awareness campaigns, and the operationalization of the PDP Law would provide actionable insights for policy design. Additionally, comparative studies with other developing nations can help identify best practices for integrating victim-centered approaches into national cyber defense strategies. By foregrounding both offender behavior and victim protection, future scholarship can guide Indonesia toward a cyber-resilient state that safeguards citizens while asserting sovereignty in the increasingly contested global digital commons.

Acknowledgement

The authors would like to express sincere gratitude to Universitas Negeri Semarang for their support and resources throughout the preparation of this manuscript. Special thanks are extended to Sergi Fernandez Alejandro from Sociedad Civil de Derecho y Políticas Públicas (SOCIPOL), Spain, for his invaluable assistance in the final-stage review and meticulous proofreading of the text. The authors also acknowledge the use of artificial intelligence tools in refining sentence structure and language, which helped enhance the manuscript's clarity and coherence. The insights and support provided by these institutions and individuals have been instrumental in completing this work.

Funding Information

None

Conflicts of Interest Statement

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

References

- 'Aisy, Firsta Rahadatul, Muhammad Azil Maskur, and A.M Adzkiya' Amiruddin. "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore." *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431–82. <https://doi.org/10.15294/jils.v10i1.13755>.
- Abdurrahman, Muhammad. "Digital Surveillance, State Power, and Civil Liberties in Contemporary Indonesia." *The Indonesian Journal of Critical Legal Studies* 1, no. 1 (2026): 57–88. <https://inleads.id/publications/index.php/IJCLS/article/view/19>.
- Adiputra, Hendrikus, Jingga Putri, and Ravion Iskandar Valeon. "Digital Health, Data Sovereignty, and Justice: Legal Challenges of Telemedicine Expansion in Post-Pandemic Indonesia." *Indonesian Health Justice Review* 2, no. 4 (2025). <https://journal.perhaki.org/index.php/health/article/view/383>.
- Agnew, Robert. "Revitalizing Merton: General Strain Theory." In *The Origins of American Criminology*, edited by Francis T. Cullen, Cheryl Lero Jonson, Andrew J. Myer, and Freda Adler, 137–58. London: Routledge, 2017. <https://www.routledge.com/The-Origins-of-American-Criminology-Advances-in-Criminological-Theory/Cullen-Jonson-Myer-Adler/p/book/9781138516557>.
- Aji, Muhammad Prakoso, Gumilar Rusliwa Somantri, and Muhammad Syaroni Rofii. "The Strategic Role of the National Cyber and Crypto Agency (BSSN) in Maintaining State Sovereignty in Cyberspace." *Journal of Law, Politic and Humanities* 5, no. 5 (2025): 3916–3924. <https://doi.org/10.38035/jlph.v5i5.1973>.
- Akhmad, Muhammad Zaidan Syafiqy, and Ridwan Arifin. "Baiq Nuril Case and Discourse on Freedom of Expression: Analysis of the Decision of the Supreme Court of the Republic of Indonesia Number 574k/Pid.Sus/2018 Regarding the Dissemination of Electronic Information Having Content Violating Morals." *Indonesia Media Law Review* 1, no. 2 (2022): 123–44. <https://journal.unnes.ac.id/journals/imrev/article/view/21735>.
- Albrecht, Jan Philipp. "How the GDPR Will Change the World." *European Data Protection Law Review* 2, no. 3 (2016): 287–89. <https://doi.org/10.21552/EDPL/2016/3/4>.
- Amanda, Dahlia Putri, Damar Sinatrio Putra, and Siti Mahira Ahmad Mubarak. "Digital Identity Theft and Criminal Protection of Personal Data in Indonesia." *Indonesian Journal of Digital Crime and Criminal Justice* 2, no. 1 (2026): 107–46. <https://journal.criminallawinstitute.org/JDCCJ/article/view/24>.
- Aulianisa, Sarah Safira, and Indirwan Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia." *Lex Scientia Law Review* 4, no. 1 (2020): 31–45. <https://doi.org/10.15294/lesrev.v4i1.38197>.
- Bhakti, Agus, Arfin Sudirman, R. Widya Setiabudi Sumadinata, and Arry Bainus. "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia." *Journal of Human Security* 20, no. 1 (2024): 109–17. <https://jhumansecurity.com/menuscript/index.php/jhe/article/view/210/152>.
- Bravo, Fabio. "Data Management Tools and Privacy by Design and by Default." In *Privacy and Data Protection in Software Services*, edited by R. Senigaglia, C. Irti, and A. Bernes, 85–95. Singapore: Springer, 2022. https://link.springer.com/chapter/10.1007/978-981-16-3049-1_8.

- Bygrave, Lee A. "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements." *Oslo Law Review* 4, no. 2 (2017): 105–120. <https://doi.org/10.18261/issn.2387-3299-2017-02-03>.
- Cantika, Yasmin, Sergi Fernandez Alejandro, Valerio Sebastian, Christina Noelia Umbría, Izan Mateo Cassandro, and Ridwan Arifin. "The Role of International Law in Addressing State-Sponsored Cyber Operations." *Indonesian Journal of Digital Crime and Criminal Justice* 1, no. 2 (2025): 347–76. <https://journal.criminallawinstitute.org/JDCCJ/article/view/30>.
- Clarke, R. V. G. "'Situational' Crime Prevention: Theory and Practice." In *Crime Opportunity Theories*. Routledge, 2011. <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315095301-21/situational-crime-prevention-theory-practice-clarke>.
- Clarke, Ronald V. "Situational Crime Prevention." *Crime and Justice* 19 (1995): 91–150. <https://www.journals.uchicago.edu/doi/abs/10.1086/449230>.
- Clarke, Ronald V., and Derek B. Cornish. "Rational Choice and Routine Activities." In *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*, edited by Raymond Paternoster and Ronet Bachman, 23–42. Roxbury Publishing Company, 2001.
- Cohen, Lawrence E., and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4 (1979): 588–608. <https://doi.org/10.2307/2094589>.
- Condry, Rachel. "Secondary Victims and Secondary Victimization." In *International Handbook of Victimology*. Routledge, 2010. <https://www.taylorfrancis.com/chapters/edit/10.1201/EBK1420085471-16/secondary-victims-secondary-victimization-rachel-condry>.
- Cornish, Paul, ed. *The Oxford Handbook of Cyber Security*. Oxford Academic, 2021. <https://doi.org/10.1093/oxfordhb/9780198800682.001.0001>.
- Damayanti, Ratih, Duhita Driyah Suprpti, and Rohmat Rohmat. "Judicial Precedents on Privacy Rights: Court Rulings in the Digital Era." *Indonesian Court and Justice Review* 1, no. 4 (2024). <https://journal.perhaki.org/index.php/court/article/view/60>.
- Emmanuel, Judith, Windiahsari Windiahsari, and Hee-Joon Kim. "Indonesia's Foreign Policy: Navigating Relations Between the U.S., China, and ASEAN." *Indonesia Discourse* 1, no. 2 (2024): 285–312. <https://journal.unnes.ac.id/journals/indi/article/view/22759>.
- European Union. "General Data Protection Regulation (GDPR)-Regulation (EU) 2016/679 of the European Parliament and of the Council," 2016. <https://gdpr.eu.org/full/full.pdf>.
- Fattah, Ezzat A., and Vincent F. Sacco. "Age as a Victimological Variable." In *Crime and Victimization of the Elderly*, 148–166. New York: Springer, 1989. https://link.springer.com/chapter/10.1007/978-1-4613-8888-3_7.
- Glanville, Luke. "The Myth of 'Traditional' Sovereignty." *International Studies Quarterly* 57, no. 1 (2013): 79–90. <https://doi.org/10.1111/isqu.12004>.
- Grabosky, Peter N. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2 (2001). <https://doi.org/10.1177/a017405>.
- Guna, Tedo Hindami, Suparno Suparno, and Indra Kertati. "Breaking down Barriers: Overcoming Silo Mentality in Bureaucratic Reform." *Journal of Sustainability, Society, and Eco-Welfare* 2, no. 1 (2024): 16–28. <https://doi.org/10.61511/jssew.v2i1.2024.884>.
- Hafel, Muhlis. "Digital Transformation in Politics and Governance in Indonesia: Opportunities and Challenges in the Era of Technological Disruption." *Society* 11, no. 2 (2023): 742–57. <https://doi.org/10.33019/society.v11i2.577>.
- Hamby, Sherry, Zach Blount, Alli Smith, Lisa Jones, Kimberly Mitchell, and Elizabeth Taylor.

- “Digital Poly-Victimization: The Increasing Importance of Online Crime and Harassment to the Burden of Victimization.” In *Polyvictimization: Adverse Impacts in Childhood and Across the Lifespan*, edited by Julian D. Ford and Brianna C. Delker, 112–128. London: Routledge, 2019. <https://www.routledge.com/Polyvictimization-Adverse-Impacts-in-Childhood-and-Across-the-Lifespan/Ford-Delker/p/book/9780367729509>.
- Heintze, Hans-Joachim, and Pierre Thielbörger, eds. *From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years*, 2016. <https://link.springer.com/book/10.1007/978-3-319-19087-7>.
- Hermawan, Ary. “Intra-Oligarchic Struggles and the Rise of Digital Attacks on Civil Society in Indonesia.” *Journal of Contemporary Asia* 56, no. 3 (2026): 407–29. <https://doi.org/10.1080/00472336.2025.2505918>.
- Hirschi, Travis. “On the Compatibility of Rational Choice and Social Control Theories of Crime.” In *The Reasoning Criminal*. Routledge, 2014. <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315134482-7/compatibility-rational-choice-social-control-theories-crime-travis-hirschi>.
- Junaidi, Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil. “Legal Reform of Artificial Intelligence’s Liability to Personal Data Perspectives of Progressive Legal Theory.” *Journal of Law and Legal Reform* 5, no. 2 (2024): 587–612. <https://journal.unnes.ac.id/journals/jllr/article/view/3437>.
- Karmen, Andrew. “The Controversy over Shared Responsibility: Is Victim-Blaming Ever Justified?” In *To Be a Victim*, edited by D. Sank and D.I. Caplan, 395–408. Boston: Springer, 1991. https://doi.org/10.1007/978-1-4899-5974-4_24.
- Kurniawan, Kuku Dwi, Deassy J. A. Hehanussa, Rahmat Setiawan, Indah Susilowati, Sopian Sopian, and Desmarani Helfisar. “Criminal Sanctions and Personal Data Protection in Indonesia.” *Lex Publica* 11, no. 2 (2024): 221–47. <https://doi.org/10.58829/lp.11.2.2024.255>.
- Kurniawan, Rudy Cahya. “Enhancing Cybercrime Response Capabilities through Integrated Digital Policing Systems.” *Jurnal Scientia Indonesia* 9, no. 2 (2025): 41–48. <https://doi.org/10.15294/scientia.v9i2.37964>.
- Lee, Joshua, Zhang Mei, and Kunal Mehta. “Digital Authoritarianism and the Erosion of Civil Liberties: A Comparative Legal Study of Surveillance Laws in China, India, and the United States.” *Journal of Transformative Legal and Social Studies* 1, no. 1 (2025): 97–120. <https://journals.arteslibres.org/index.php/social/article/view/15>.
- Lestari, Bunga Maulidina, and Ahmad Fauzi. “The Role of Victims of NCT Concert Ticket Fraud Via Social Media: A Cyber Victimology Perspective.” *Indonesia Justice Spectrum* 1, no. 1 (2026): 119–46. <https://journal.criminallawinstitute.org/IJS/article/view/10>.
- Levi, Margaret. “The Who, What, and Why of Performance-Based Legitimacy.” *Journal of Intervention and Statebuilding* 12, no. 4 (2018): 603–10. <https://doi.org/10.1080/17502977.2018.1520955>.
- Mahendra, Daffa Irfan. “Polarization, Hate Speech, and Democracy: Social Media Discourse During Indonesia’s 2019 Elections.” *Indonesian Discourse on Communication, Democracy, and Political Movements* 1, no. 2 (2024). <https://journal.perhaki.org/index.php/indepolcom/article/view/618>.
- Margiansyah, Defbry. “Digitalizing Authoritarianism in Indonesia: Exploring the Intersection of Civic Activism, Digital Repression, and Democratic Erosion.” In *Indonesian Perspectives on Democracy*, 183–209. Singapore: Springer, 2025. https://doi.org/10.1007/978-981-96-3137-7_11.
- Mashdurohatun, Anis, Bambang Sugihartono, Nurul Masrifah, Arief Indra Kusuma Adhi, and Henning Glaser. “Combating Digital Defamation: Regulations, Challenges and Protecting

- Reputation.” *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (2025): 486–514. <https://journal.yapici.or.id/index.php/JSDERI/article/view/147>.
- McNealey, Rachel L., and Adam Ghazi-Tehrani. “Risky Digital Behavior or Risky Digital Places? Victimization Risk Perception and Evaluation on the Internet.” *Journal of Crime and Justice* 47, no. 4 (2024): 530–44. <https://doi.org/10.1080/0735648X.2023.2244927>.
- Mediana, Caecilia. “Internet Traffic Anomaly Averages 1.25 Billion per Year.” *Kompas.Id*, August 11, 2025. <https://www.kompas.id/artikel/en-bssn-rata-rata-tahunan-anomali-trafik-internet-mencapai-125-miliar>.
- Melati, Dea. “Implementation of Digital Governance in Improving Cyber Security in Indonesia.” *Journal of Law, Social Science and Humanities* 2, no. 2 (2025): 379–90. <https://myjournal.or.id/index.php/JLSSH/article/view/347>.
- Merton, Robert K. *Social Theory and Social Structure*. Sydney: Simon and Schuster, 1968.
- Montoya, César Paredes, and Isabel Aguirre Lozano. “Digital Disobedience: The Impact of Social Media on Collective Actions and Rebellions = Desobediencia Digital: El Impacto de Las Redes Sociales En Las Acciones Colectivas y Rebeliones.” *Revista de Desobediencia Comunitaria* 1, no. 2 (2025). <https://publications.socipol.org/index.php/rdc/article/view/34>.
- Morales, Sebastián Alejandro, and Andrés Castillo. “The Case of Gender Violence in Mexico: Does the Judicial System Ensure Substantive Justice for Victims? = El Caso de La Violencia de Género En México: ¿Garantiza El Sistema Judicial La Justicia Sustantiva Para Las Víctimas?” *Crítica de La Justicia Sustantiva* 1, no. 2 (2025): 205–32. <https://publications.socipol.org/index.php/cjs/article/view/25>.
- Nuha, Muhammad Azza Ulin, Muhammad Salman, Nur Annisa Kadarwati Febriyani, and Eka Hero Ramadhani. “Reformulation of the Vulnerability Management Cycle for Enhancing Indonesia’s Critical Information Infrastructure Protection: An International Comparative Study.” *The Indonesian Journal of Computer Science* 14, no. 1 (2025): 322–37. <https://doi.org/10.33022/ijcs.v14i1.4609>.
- Nye, Joseph S. “Normative Restraints on Cyber Conflict,” 2017. https://www.sipa.columbia.edu/sites/default/files/2022-11/Nye_Normative_Restraints_on_Cyber_Conflict_0502.pdf.
- O’Connell, Mary Ellen. “Cyber Security without Cyber War.” *Journal of Conflict and Security Law* 17, no. 2 (2012): 187–209. <https://doi.org/10.1093/jcsl/krs017>.
- Paterson, Thomas. “Indonesian Cyberspace Expansion: A Double-Edged Sword.” *Journal of Cyber Policy* 4, no. 2 (2019): 216–34. <https://doi.org/10.1080/23738871.2019.1627476>.
- Pradana, Muhammad Akbar Eka, and Horadin Saragih. “Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya.” *Innovative: Journal Of Social Science Research* 4, no. 4 (2024): 3412–3425. <https://j-innovative.org/index.php/Innovative/article/view/13476>.
- Prasetya, Andreas Abimanyu, Elvito Primanda Wibowo, Hendryco Bintang Burju Sianipar, and Vita Surya Pratiwi. “Legal Enforcement on the Misuse of Health Data in the SATUSEHAT Mobile Application: Patient Privacy Protection.” *Immortalis Journal of Interdisciplinary Studies* 2, no. 1 (2026): 1–8. <https://immortalispub.com/IJIS/article/view/59>.
- Puluhulawa, Mohamad Rusdiyanto U., and Riski Husain. “Body Shaming Through Social Media As a Digital Crime In The Era of Disruption.” *Jambura Law Review* 3, no. 1 (2021): 112–23. <https://doi.org/10.33756/jlr.v3i1.7200>.
- Putra, Eka Nugraha. “Law’s Silence on Cyberbullying to Children in Indonesia.” *Brawijaya Law Journal* 11, no. 1 (2024): 135–63. <https://doi.org/10.21776/ub.blj.2024.011.01.07>.
- Putra, Tegar Islami, Nurul Fibrianti, and Adinda Zeranica Putri Fakhis. “Implementation of CNIL’s Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection.” *The*

- Indonesian Journal of International Clinical Legal Education* 7, no. 2 (2025): 203–34.
<https://doi.org/10.15294/iccle.v7i2.21049>.
- Putra, Tegar Islami, Nurul Fibrianti, and Rizky Andeza Prasetya. “Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe).” *Journal of Private and Commercial Law* 9, no. 1 (2025): 72–109.
<https://doi.org/10.15294/jpcl.v9i1.9370>.
- Putra, Tegar Islami, Waspih Waspih, Indriana Firdaus, Fitria Damayanti, and Bintang Rafli Ananta. “Challenges in Ensuring Personal Data Protection For Society in The Era of Society 5.0: Indonesia’s Case Study.” *Unnes Law Journal* 10, no. 2 (2024): 223–54.
<https://journal.unnes.ac.id/journals/ulj/article/view/8928>.
- Putri, Eunike, and Fadhel Arjuna Adinda. “Artificial Intelligence, Digital Rights, and Human Dignity in Indonesia’s Tech Regulation.” *Contemporary Issues on Indonesian Human Rights Law and Policy* 2, no. 1 (2025).
<https://journal.perhaki.org/index.php/humanrights/article/view/358>.
- Putri, Uni Tsulasi, Irna Nurhayati, and Taufiq El Rahman. “Legal Challenges of the Application of the Right to Be Forgotten in Blockchain in Indonesia and the European Union.” *Jambura Law Review* 7, no. 2 (2025): 633–63. <https://doi.org/10.33756/jlr.v7i2.30514>.
- Ramírez, Mateo Julián Ortega. “Smart Cities, Smart Exclusion: The Digital Divide in Marginalized Neighborhoods.” *Revista de Justicia Social En La Sociedad Urbana* 1, no. 2 (2025): 181–214. <https://publications.socipol.org/index.php/rjs/article/view/29>.
- Reuters. “Cyber Attack Compromised Indonesia Data Centre, Ransom Sought.” *Reuters*, June 24, 2024. <https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/>.
- Rohith, Cheerala, and Ranbir Singh Batth. “Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and Its Repercussion.” In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 640–45. IEEE, 2019.
<https://doi.org/10.1109/ICCIKE47802.2019.9004236>.
- Sapada, Andi Tenri, and Mohammad Arif. “Use of Artificial Intelligence in General Elections: Comparison of Indonesian and German Regulations.” *Contemporary Issues on Indonesian Social Justice and Legal Reform* 1, no. 1 (2025): 21–40.
<https://journals.arteslibres.org/index.php/law/article/view/2>.
- Sari, T.Y., and K.P. Silalahi. “Digital Participatory Archive for Justice: An Inclusive Future for Vulnerable Groups.” In *Religion, Education, Science and Technology towards a More Inclusive and Sustainable Future*, edited by Maila D.H. Rahiem. Routledge, 2024.
<https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9781003322054-34/digital-participatory-archive-justice-inclusive-future-vulnerable-groups-sari-silalahi>.
- Satwiko, Brahmantyo Suryo. “Privacy and Data Protection: Indonesian Legal Framework.” *Corporate and Trade Law Review (CTLR)* 1, no. 2 (2021): 98–118.
<https://doi.org/10.21632/ctlr.1.2.98-118>.
- Sayar, İbrahim Barış. “The Administrative Fines Regime of the General Data Protection Regulation and Its Impact.” *Kişisel Verileri Koruma Dergisi* 3, no. 1 (2021): 1–16.
<https://izlik.org/JA87PT29LY>.
- Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. <https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>.
- Senge, Peter. “Classic Work: The Leader’s New Work: Building Learning Organizations.” In *Knowledge Management: Classic and Contemporary Works*, edited by Daryl Morey, Mark T. Maybury, and Bhavani Thuraisingham. The MIT Press, 2000.
<https://doi.org/10.7551/mitpress/4075.003.0008>.

- Shackelford, Scott J. "The Law of Cyber Peace." *Chicago Journal of International Law* 18, no. 1 (2017). <https://cjl.uchicago.edu/print-archive/law-cyber-peace>.
- Solikhah, Mar'atus. "Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework." *Indonesian Cyber Law Review* 2, no. 1 (2025): 39–50. <https://iclr.polteksci.ac.id/index.php/sci/article/view/15>.
- Subagyo, Bambang Sugeng Ariadi, Mochamad Kevin Romadhona, Zahry Vandawati Chumaida, Bambang Suheryadi, and Noureldin Samy Elkhassab. "Can Indonesia's Laws Keep Up? Protecting Consumer Rights in Digital Transactions." *Journal of Law and Legal Reform* 5, no. 3 (2024): 869–90. <https://doi.org/10.15294/jllr.v5i3.4202>.
- Sucahyanto, Ardhitama. "Digital Society and the Transformation of Community-Based Dispute Resolution in Indonesia." *The Indonesian Journal of Sociolegal Development* 1, no. 1 (2026): 57–78. <https://inleads.id/publications/index.php/IJSLD/article/view/14>.
- Suhaila, Shafa, Mutiara Andini, Oriza Satifa Wahyuni, M. Daris Alfi Putra Nurhadi, and Muhammad Sahriadi Lubis. "Pertanggungjawaban Negara Dalam Kebocoran Data Pada Platform E-Government: Analisis Hukum Administrasi Atas Kasus Satu Sehat Dan DPMPSTP Online." *Jurnal Ilmiah Penelitian Mahasiswa* 4, no. 2 (2026): 12–21. <https://ejurnal.kampusakademik.my.id/index.php/jipm/article/view/2166>.
- Sulubara, Seri Mughni, Viridya Tasril, and Nurkhalisah Nurkhalisah. "Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia'S Defense." *De Lega Lata: Jurnal Ilmu Hukum* 10, no. 2 (2025): 287–97. <https://jurnal.umsu.ac.id/index.php/delegalata/article/view/25786>.
- Supeno, Supeno, Rosmidah Rosmidah, and Syed Mohd Uzair Iqbal. "Personal Data Protection in Review of Legal Theories and Principles." *Journal of Law and Legal Reform* 6, no. 3 (2025): 1349–1376. <https://doi.org/10.15294/jllr.v6i3.10252>.
- Suraji, Suraji, and Ipop Abdi Prabowo. "Harmonizing Privacy Rights Protection in Electronic Transaction with Roscoe Pound's Legal Principle." *Indonesian Journal of Advocacy and Legal Services* 7, no. 1 (2025): 71–94. <https://doi.org/10.15294/ijals.v7i1.22331>.
- Sutikno, Tole, and Deris Stiawan. "Cyberattacks and Data Breaches in Indonesia by Bjorka: Hacker or Data Collector?" *Bulletin of Electrical Engineering and Informatics (BEEI)* 11, no. 6 (2022). <https://beei.org/index.php/EEI/article/view/4854>.
- Taufiq, Muchamad, and Ananda Salsabila Kenyo. "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR." *International Journal of Business, Law, and Education* 6, no. 2 (2025): 1260–68. <https://doi.org/10.56442/ijble.v6i2.1178>.
- Tutuianu, Simona. *Towards Global Justice: Sovereignty in an Interdependent World*. T.M.C. Asser Press The Hague, 2012. <https://doi.org/10.1007/978-90-6704-891-0>.
- Utari, Indah Sri, Ridwan Arifin, and Sergi Fernandez Alejandro. "Gender-Based Violence and the Implementation of the Sexual Violence Crime Law in Indonesia." *The Indonesian Journal of Feminist Legal Studies* 1, no. 1 (2026): 1–32. <https://inleads.id/publications/index.php/IJFLS/article/view/1>.
- Utomo, Setiyo. "The Digital Age and Human Rights Protection in Indonesia: Legal Framework, Challenges, and Reform Directions." *Yustisia* 14, no. 2 (2025): 225–41. <https://doi.org/10.20961/yustisia.v14i2.85404>.
- Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. New York: John Wiley & Sons, 2024.
- Wiraguna, Sidi. "Strengthening the Functional Autonomy of Data Protection Officers Under Indonesia's PDP Law 2022: A Critical Legal and Institutional Review." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 4, no. 3 (2025): 1–8.

<https://jurnal.penerbitwidina.com/index.php/JPS/article/view/2317>.

- Yar, Majid. "Toward a Cultural Criminology of the Internet." In *Technocrime and Criminological Theory*, edited by Kevin Steinmetz and Matt R. Nobles. Routledge, 2017.
<https://www.taylorfrancis.com/chapters/edit/10.4324/9781315117249-8/toward-cultural-criminology-internet-majid-yar>.
- Yuniarti, Siti. "Protection of Indonesia's Personal Data After Ratification of Personal Data Protection Act." *Progressive Law Review* 4, no. 2 (2022): 54–68.
<https://doi.org/10.36448/plr.v4i02.85>.
- Yusliwidaka, Arnanda, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana. "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?" *Pandecta Research Law Journal* 19, no. 2 (2024): 453–82.
<https://doi.org/10.15294/pandecta.v19i2.13279>.
- Zaltina, Putri, and Lidwina Inge Nurtjahyo. "Right to Be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases." *The Indonesian Journal of Socio-Legal Studies* 3, no. 2 (2024). <https://doi.org/10.54828/ijsls.2024v3n2.4>.
- Zhihao, Wang, Zhang Liyan, Mikhail Andreyevich Sokolov, and Omar Khaled Hussein. "Digital Rights and Freedoms: The Fight for a Free Internet in Authoritarian Regimes." *Revista de Derechos Humanos Contemporáneos* 1, no. 2 (2025): 347–76.
<https://publications.socipol.org/index.php/rdh/article/view/40>.