Jurnal Hukum Siber
dan Regulasi Teknologi

SAH PUBLISHER

e-ISSN 3123-8114
Vol. 1, No. 2, May 2026

Cybercrime and Data Protection: A Comparative Analysis of Indonesian and International Regulations

Muhammad Ruslan Afandi[1]*
[1]Department of Law, Faculty of Social Sciences and Humanities, Universitas Harkat Negeri, Indonesia
Email: mruslanafandi@harkatnegeri.ac.id

Abstract. This article examines the development, structure, and remaining weaknesses of Indonesian cybercrime and personal data protection law in comparison with selected international regulatory standards. The urgency of the study arises from the rapid growth of digital services, cross-border electronic evidence, data breaches, online fraud, phishing, and AI-enabled cybercrime, while Indonesia's regulatory framework is still distributed across the Electronic Information and Transactions Law, the Personal Data Protection Law, electronic system regulations, and institutional cybersecurity mandates. Using a normative juridical method supported by systematic legal literature review and comparative legal analysis, the study evaluates Indonesian law against the GDPR, the Budapest Convention, the NIS 2 Directive, ASEAN cybersecurity cooperation instruments, and comparative models from Singapore and Australia. The findings show that Indonesia has moved beyond a legal vacuum, especially after Law Number 27 of 2022 and Law Number 1 of 2024, but still faces gaps in institutional independence, cyber incident reporting, cross-border cooperation, digital evidence procedures, risk-based obligations, and integrated supervision. The article argues that reform should prioritize harmonization among cybercrime, data protection, and cybersecurity governance instruments; establishment of a strong personal data protection authority; clearer incident-reporting duties; and structured international cooperation for electronic evidence and transnational enforcement. The novelty of the study lies in integrating cybercrime enforcement and data protection analysis into one regulatory-harmonization framework rather than treating them as separate legal regimes.

Keywords: cybercrime, data protection, Indonesian regulation, GDPR, Budapest Convention

INTRODUCTION

Cybercrime and personal data protection have become central issues in contemporary Indonesian law because almost every layer of economic, social, and governmental activity now depends on electronic systems. Digital transformation has expanded financial inclusion, electronic commerce, public administration, health services, and communication platforms, but it has also created new spaces for hacking, phishing, identity theft, ransomware, online fraud, doxing, illegal access, and misuse of personal data. Indonesia has responded through the Electronic Information and Transactions Law as amended by Law Number 1 of 2024, the Personal Data Protection Law, Government Regulation Number 71 of 2019, and the institutional mandate of BSSN [1]-[4]. These instruments show that Indonesia is no longer in a condition of legal vacuum. The more important legal question is whether the existing framework is coherent, enforceable, and sufficiently aligned with the transnational character of cybercrime and data flows.

The urgency of this issue is amplified by three developments. First, cybercrime increasingly depends on cross-border infrastructure: servers, cloud storage, payment channels, social-media accounts, and digital evidence may be located outside the forum state. Second, data protection violations are no longer merely private-law or administrative issues; data leaks may enable phishing, account takeover, financial fraud, and blackmail. Third, AI-enabled phishing, synthetic identity fraud, and automated social engineering make conventional cybercrime categories less adequate unless cybercrime enforcement is connected to data governance and platform accountability. Indonesian scholarship has recognized these challenges in studies on cybersecurity law, transnational online fraud, hacking, telematics law, and AI-based phishing [14]-[24]. However, many studies still analyze cybercrime, personal data protection, and cybersecurity governance

Received Feb 2026 / Revised May 2026 / Accepted May 2026
*Corresponding author.
Email addresses: mruslanafandi@harkatnegeri.ac.id (Afandi)

separately, so the relationship among criminal enforcement, administrative supervision, and data-subject rights remains underdeveloped.

The state of the art in international regulation points to a more integrated model. The GDPR is not only a privacy instrument; it operationalizes lawfulness, transparency, security of processing, accountability, data-subject rights, impact assessment, breach notification, and cross-border transfer control [5]. The NIS 2 Directive adds cybersecurity risk-management and incident-reporting obligations for essential and important entities [6]. The Budapest Convention provides the leading framework for substantive cybercrime offences, procedural powers, preservation of computer data, and international cooperation [7], while the Second Additional Protocol reflects the contemporary need for faster cooperation and disclosure of electronic evidence [8]. ASEAN and OECD instruments further emphasize readiness, policy coordination, digital-security risk management, and public-private cooperation [9], [10]. These instruments reveal a regulatory trend: effective cyber law combines criminalization, data protection, preventive cybersecurity obligations, institutional capacity, and cross-border cooperation.

Previous Indonesian studies provide important foundations but leave identifiable gaps. Fuady et al. [14] and Judijanto and Nugroho [17] emphasize the need to strengthen cybersecurity and cybercrime enforcement. Maesaroh [15] highlights the constitutional and state-resilience dimension of cybersecurity. Mulyana [16], Fikri [20], Abidah et al. [23], and Nurmansyah et al. [24] discuss transnational fraud, phishing, and AI-based crime. Kennedy [18] and Mardisontori [21] focus on telematics and the PDP Law, while Erikha and Saptomo [22] and Wicaksono and Yasin [25] address legal policy dilemmas and sectoral fragmentation. The gap is that these works rarely construct a single comparative matrix showing how Indonesian cybercrime enforcement and data protection should be harmonized with international standards. This article fills that gap by asking: (1) how has Indonesia's cybercrime and data protection framework developed from 2008 to 2026; and (2) how should Indonesian law be harmonized with international cybercrime and data protection standards?

METHODS

This study uses a normative juridical method combined with systematic legal literature review and comparative legal analysis. The normative component examines positive law, legal concepts, institutional mandates, and regulatory principles. The literature-review component maps journal articles and doctrinal writings on Indonesian cybercrime, cybersecurity, personal data protection, online fraud, phishing, and transnational enforcement [14]-[25]. The comparative component benchmarks Indonesian law against international and regional instruments, including the GDPR, NIS 2 Directive, Budapest Convention, ASEAN Cybersecurity Cooperation Strategy, OECD Recommendation, Singapore's Cybersecurity Act model, and Australia's Security of Critical Infrastructure Act [5]-[13].

Primary legal materials consist of Law Number 1 of 2024, Law Number 27 of 2022, Government Regulation Number 71 of 2019, and Presidential Regulation Number 28 of 2021 concerning BSSN [1]-[4]. International materials include the GDPR, the NIS 2 Directive, the Budapest Convention and its Second Additional Protocol, ASEAN cybersecurity cooperation instruments, OECD digital-security recommendations, UNODC cybercrime materials, and selected comparative laws [5]-[13]. Secondary legal materials consist of peer-reviewed journal articles and conference papers verified through DOI metadata where available.

The analysis was conducted in four stages. First, the study identified the legal norms governing cybercrime, personal data processing, electronic system operation, breach response, and institutional cybersecurity authority. Second, it mapped each norm against international benchmarks. Third, it assessed whether the Indonesian framework provides preventive, supervisory, enforcement, and cooperative mechanisms. Fourth, it formulated reform recommendations based on legal coherence, proportionality, institutional feasibility, and compatibility with Indonesia's civil-law tradition.

RESULTS AND DISCUSSION

The Development of Indonesian Cybercrime and Data Protection Regulation. Indonesia's cyber regulatory development began with the Electronic Information and Transactions Law, which introduced legal recognition of electronic information and transactions and became the principal basis for cybercrime enforcement. The second amendment through Law Number 1 of 2024 is significant because it attempts to

reduce interpretive controversies, clarify several offences, and adjust the ITE framework to contemporary digital communication [1]. Government Regulation Number 71 of 2019 complements this framework by regulating electronic system operators, electronic transactions, and obligations related to system operation [3]. The institutional dimension is supported by Presidential Regulation Number 28 of 2021, which gives BSSN responsibility in the field of cybersecurity and cryptography [4].

The enactment of Law Number 27 of 2022 on Personal Data Protection marks a structural shift. Before the PDP Law, personal data rules were scattered across sectoral regulations, creating uncertainty in consent, lawful processing, data-subject rights, sanctions, and supervision. The PDP Law recognizes personal data categories, regulates data-controller and processor obligations, provides data-subject rights, governs transfer of personal data, and introduces administrative and criminal sanctions [2]. This development directly affects cybercrime policy because identity theft, phishing, account takeover, and fraud often begin with unlawful acquisition or disclosure of personal data [16], [20], [23], [24].

Nevertheless, the Indonesian framework remains fragmented. Cybercrime offences are primarily located in the ITE framework and the Criminal Code; personal data obligations are in the PDP Law; electronic system operation is regulated through government regulations; and cybersecurity coordination is institutionally assigned to BSSN. Fragmentation does not automatically mean legal failure, but it creates coordination problems when a single incident involves illegal access, personal data breach, consumer fraud, platform negligence, cloud-based evidence, and cross-border investigation. Indonesian literature repeatedly identifies these obstacles, particularly limited enforcement capacity, uneven digital literacy, unclear institutional coordination, and insufficient cross-border mechanisms [14]-[19], [22], [25].

Table 1. Comparative Matrix of Indonesian and International Cyber Regulation

Indicator	Indonesia	International benchmark	Legal implication
Substantive cybercrime offences	ITE Law as amended and Criminal Code provisions regulate illegal access, manipulation, prohibited content, and related acts [1].	Budapest Convention uses a coherent catalogue of offences against confidentiality, integrity, availability, computer-related offences, and content-related offences [7].	Indonesia should keep offence definitions technology-neutral while adding clarity for AI-enabled phishing, credential theft, and automated fraud.
Personal data protection	PDP Law regulates data categories, data-subject rights, controller obligations, transfers, sanctions, and criminal prohibitions [2].	GDPR provides stronger operational detail on accountability, breach notification, data protection impact assessment, and independent supervision [5].	The most urgent issue is not recognition of privacy, but implementation through an independent supervisory authority and enforceable compliance duties.
Electronic system governance	GR 71/2019 regulates electronic system operators and electronic transactions [3].	NIS 2 imposes risk-management, incident-reporting, and sectoral cybersecurity obligations [6].	Indonesia needs clearer incident reporting thresholds and risk-based security duties for high-risk electronic system operators.
International cooperation	Cooperation exists through general mutual legal assistance and bilateral or regional mechanisms, but cyber-specific procedures remain limited.	Budapest Convention and its Second Additional Protocol provide expedited preservation, 24/7 cooperation, and electronic evidence tools [7], [8].	Cross-border evidence access should be strengthened while preserving due process and personal data safeguards.
Regional and policy coordination	BSSN coordinates cybersecurity functions under Presidential Regulation No. 28/2021 [4].	ASEAN and OECD emphasize cyber readiness, policy coordination, trust, capacity building, risk management, and international cooperation [9], [10].	Indonesia should translate regional commitments into binding operational duties, reporting channels, and coordination protocols.

Source: Author's analysis based on verified legal instruments and literature.

The comparison shows that Indonesia's main weakness is not the absence of rules but the absence of a fully integrated architecture. The GDPR and NIS 2 demonstrate the importance of combining data protection, cybersecurity risk management, and supervision [5], [6]. The Budapest framework shows that criminal law requires procedural tools and cooperation mechanisms in addition to substantive offences [7], [8]. ASEAN and OECD instruments reinforce that cyber resilience must be built through policy coordination, trust, and capacity development [9], [10]. Comparative experiences from Singapore and Australia further show that

high-risk infrastructure and essential services require special duties, not merely general cybercrime prohibitions [12], [13].

Table 2. Main Legal Gaps and Corrective Direction

Legal gap	Observed problem	Corrective direction
Institutional supervision	The PDP Law anticipates supervisory functions, but effective implementation depends on an authority that is independent, adequately resourced, and technically capable [2], [21].	Establish a strong personal data protection authority with investigative, corrective, administrative-sanction, and public-guidance powers.
Cyber incident reporting	Current rules do not yet create a fully harmonized incident-reporting system comparable to NIS 2 for essential and important entities [6].	Adopt tiered reporting based on severity, affected data, sector, public impact, and systemic risk.
Cross-border evidence	Cybercrime investigations often require preservation or disclosure of electronic evidence located overseas [7], [8], [11].	Develop cyber-specific mutual assistance protocols and consider alignment with Budapest Convention standards.
AI-enabled crime	AI-based phishing and automated social engineering blur the boundary between ordinary fraud, identity misuse, and data protection violations [23], [24].	Clarify liability for automated phishing infrastructure, credential harvesting, synthetic identity misuse, and negligent security practices.
Sectoral fragmentation	Cybercrime, PDP, electronic system operation, and cybersecurity governance are regulated through separate instruments [1]-[4].	Create a harmonization framework or implementing regulation that connects criminal enforcement, administrative supervision, and cybersecurity risk management.

Source: Author's analysis based on verified legal instruments and literature.

For Indonesia, harmonization should proceed through three legal moves. First, the PDP Law must be implemented through a credible supervisory authority. Without such an authority, data-subject rights risk becoming formal entitlements with limited practical effect. Second, cyber incident reporting should be standardized so that data breaches, system compromises, and cyber fraud involving personal data are not reported through disconnected channels. Third, cybercrime procedure should be modernized to support lawful evidence preservation and cross-border cooperation. These measures would also answer concerns raised by Indonesian researchers about enforcement capacity, regulatory fragmentation, and the limits of sectoral reform [14]-[25].

A further implication is that data protection and cybercrime should not be treated as separate policy silos. A phishing case may involve unlawful access, credential theft, misuse of personal data, consumer loss, platform security failure, and overseas electronic evidence in a single factual chain. If each issue is handled by a separate institution without interoperable procedures, enforcement becomes slow and inconsistent. A harmonized framework should therefore define institutional coordination, minimum security standards, notification timelines, evidentiary preservation duties, and cooperation with foreign authorities.

Table 3. Policy Recommendations for Regulatory Harmonization

Time frame	Recommendation	Rationale	Priority
Short term	Issue implementing regulations for the PDP Law and establish an operational data protection supervisory authority.	Rights and sanctions under the PDP Law require institutional enforcement, technical guidance, and complaint-handling mechanisms [2], [5], [21].	High
Short term	Create harmonized breach and cyber-incident reporting rules for electronic system operators.	A unified reporting system would reduce duplication and improve response coordination among BSSN, sectoral regulators, and data protection authorities [3], [4], [6].	High
Medium term	Align cybercrime procedure with Budapest standards on preservation, production, search, seizure, and international cooperation.	Transnational evidence is often decisive in online fraud, phishing, and identity theft investigations [7], [8], [16], [20].	High

Medium term	Adopt risk-based obligations for high-risk digital services, public-sector platforms, and critical electronic system operators.	Risk-management duties are consistent with NIS 2, OECD recommendations, Singapore's CII approach, and Australia's critical infrastructure model [6], [10], [12], [13].	Medium
Long term	Develop an integrated cyber law roadmap connecting cybercrime, data protection, cybersecurity governance, consumer protection, and digital evidence.	Fragmentation is repeatedly identified in Indonesian legal scholarship and weakens legal certainty and enforcement capacity [14], [15], [17]-[19], [22], [25].	High

Source: Author's analysis based on verified legal instruments and literature.

This article also corrects a common misconception in earlier drafts of cyber regulation analysis: the PDP Law is no longer merely a bill. Since 2022 it has become positive law, and the real legal problem is implementation rather than enactment [2]. Likewise, the ITE framework has been amended by Law Number 1 of 2024, so analysis should refer to the current amended framework rather than only to Law Number 11 of 2008 [1]. Legal scholarship and policy recommendations must therefore move from general calls for regulation toward more precise questions of institutional design, enforcement thresholds, cross-border procedure, and accountability.

CONCLUSION

Indonesia has developed a meaningful legal basis for cybercrime enforcement and personal data protection through the ITE Law as amended, the PDP Law, electronic system regulations, and BSSN's institutional mandate. However, the comparative analysis shows that the Indonesian framework still requires harmonization with international standards in three areas: integrated supervision, risk-based cybersecurity obligations, and cross-border cooperation for electronic evidence. The GDPR, NIS 2 Directive, Budapest Convention, ASEAN cybersecurity strategy, OECD recommendations, and comparative models from Singapore and Australia demonstrate that modern cyber regulation must combine criminal law, administrative supervision, preventive duties, institutional coordination, and international cooperation. The practical contribution of this study is a harmonization agenda for Indonesia: establish an effective personal data protection authority, adopt unified breach and incident reporting, clarify legal duties for high-risk electronic system operators, modernize cybercrime procedure for cross-border evidence, and connect cybercrime enforcement with personal data protection. These reforms would strengthen legal certainty, consumer and citizen protection, and national digital resilience.

REFERENCES

[1] Republic of Indonesia. (2024). Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions. Available: https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024

[2] Republic of Indonesia. (2022). Law Number 27 of 2022 on Personal Data Protection. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[3] Republic of Indonesia. (2019). Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions. Available: https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

[4] Republic of Indonesia. (2021). Presidential Regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency. Available: https://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021

[5] European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[6] European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[7] Council of Europe. (2001). Convention on Cybercrime (Budapest Convention, ETS No. 185). Available: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[8] Council of Europe. (2021). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Available: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

[9] ASEAN Secretariat. (2022). ASEAN Cybersecurity Cooperation Strategy 2021-2025. Available: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
[10] OECD. (2019). Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456. Available: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456
[11] UNODC. (2013). Comprehensive Study on Cybercrime. Available: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html
[12] Cyber Security Agency of Singapore. (2026). Cybersecurity Act. Available: https://www.csa.gov.sg/legislation/cybersecurity-act/
[13] Australian Government. (2026). Security of Critical Infrastructure Act 2018. Available: https://www.legislation.gov.au/Series/C2018A00029
[14] Fuady, A., Hasibuan, F. Y., & Kotto, Z. (2025). Strengthening cybersecurity and data protection legal framework in Indonesia: A normative analysis of current challenges and future directions. Law and Justice Research Journal. https://doi.org/10.70062/ljrj.v1i3.87
[15] Maesaroh, R. S. (2025). Tantangan keamanan siber dan implikasinya terhadap hukum kenegaraan: Tinjauan atas peran negara dalam menjamin ketahanan digital. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam. https://doi.org/10.14421/3n8bxw79
[16] Mulyana, Y. (2025). Cybercrime and transnational criminal law: Tackling online fraud and identity theft. Ipso Jure. https://doi.org/10.62872/zep90829
[17] Judijanto, L., & Nugroho, B. (2025). Regulasi keamanan siber dan penegakan hukum terhadap cybercrime di Indonesia. Sanskara Hukum dan HAM. https://doi.org/10.58812/shh.v3i03.544
[18] Kennedy, A. (2025). Tantangan implementasi dan perkembangan hukum telematika di Indonesia. Ethics and Law Journal: Business and Notary. https://doi.org/10.61292/eljbn.262
[19] Darmawan, C. K., Sebastian, E., Notokusumo, F. L., & Loprang, J. R. (2025). Urgensi penguatan regulasi pelindungan data dan keamanan siber di Indonesia terhadap ancaman hacking dalam sistem pemerintahan berbasis elektronik. Jurnal Suara Keadilan. https://doi.org/10.24176/sk.v26i1.14752
[20] Fikri, A. (2024). Kebijakan hukum dalam pemberantasan pelaku online romance fraud di ruang maya. JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial. https://doi.org/10.51486/jbo.v6i2.219
[21] Mardisontori. (2025). Legal review of personal data regulations in the Personal Data Protection Law. Proceedings of the First International Cyber Law Conference. https://doi.org/10.4108/eai.11-11-2023.2351324
[22] Erikha, A., & Saptomo, A. (2024). Dilemma of legal policy to address cybercrime in the digital era. Asian Journal of Social and Humanities, 3(3). https://doi.org/10.59888/ajosh.v3i3.452
[23] Abidah, S. Q., Faturrahman, M. R., Khoirunnisa, N., Wicaksono, S. S., & Wulandari, S. (2025). Criminal policy of Indonesian criminal law in combating the crime of phishing. SHS Web of Conferences, 221, 03006. https://doi.org/10.1051/shsconf/202522103006
[24] Nurmansyah, G., Wiranata, G. A. B., Fardiansyah, A., & Mladenov, S. V. (2024). Preventing AI-based phishing crimes across national borders through the reconstruction of personal data protection laws. Jurnal Hukum Novelty, 15(2). https://doi.org/10.26555/jhn.v15i2.27558
[25] Wicaksono, S. S., & Yasin, I. F. (2024). Criminal law reformulation through omnibus law as a solution to sectoral cyber protection. Al-Jinayah: Jurnal Hukum Pidana Islam, 10(2), 237-261. https://doi.org/10.15642/aj.2024.10.2.237-261