Law and Justice research journal

E-ISSN: 3089-6819

Research Article

Strengthening Cybersecurity and Data Protection Legal Framework in Indonesia: A Normative Analysis of Current Challenges and Future Directions

Ahmad Fuady*, Fauzie Yusuf Hasibuan, Zulkarnaen Kotto

Doctoral Law Program Universitas Jayabaya, Jakarta, Jl. Pulomas Selatan Kav. No. 23 4, RT. 4/RW. 9, Kayu Putih, Pulo Gadung District, East Jakarta City, Special Capital Region of Jakarta 13210, Indonesia.
* Corresponding Author : fuady9898@gmail.com

Abstract: Indonesia's digital transformation has accelerated dramatically, creating unprecedented opportunities alongside significant cybersecurity challenges. This article examines the current state (das sein) and normative expectations (das sollen) of Indonesia's cybersecurity and data protection legal framework through a comprehensive normative legal analysis. The study reveals critical gaps in existing legislation, particularly the Information and Electronic Transactions Law (UU ITE). It evaluates the potential impact of emerging regulatory frameworks, including the Draft Law on Personal Data Protection (RUU PDP). Using normative legal research methodology, this analysis draws from statutory regulations, policy documents, and comparative legal studies to assess Indonesia's legal preparedness for evolving cyber threats. The findings indicate that while foundational legal instruments exist, significant normative reforms are required to address sophisticated cybercrime, protect individual privacy rights, and maintain national digital security. The research concludes with actionable recommendations for legislative enhancement, institutional strengthening, and public-private collaboration to establish a robust, adaptive cybersecurity legal regime that meets international standards while addressing Indonesia's unique socio-legal context.

Keywords: Cybersecurity Law; Data Protection; Digital Transformation; Indonesia; Legal Reform; Normative Legal Analysis.

1. Introduction

Indonesia's rapid digital transformation has fundamentally altered the nation's socio-economic landscape, positioning the archipelago as Southeast Asia's largest digital economy with over 277 million people and internet penetration exceeding 77% of the population. The digital economy's contribution to Indonesia's GDP has reached approximately $70 billion annually, demonstrating the critical importance of cyberspace to national prosperity and security. However, this unprecedented digitalization has exposed the nation to sophisticated cyber threats that challenge the adequacy of existing legal frameworks and institutional capacity for cybersecurity governance.

The current state of cybersecurity law in Indonesia (das sein) reveals a complex but inadequate legal architecture primarily anchored by the Information and Electronic Transactions Law (UU ITE) No. 11 of 2008, as amended by Law No. 19 of 2016. While providing basic provisions for electronic transactions and cybercrime penalties, this foundational legislation demonstrates significant limitations in addressing the sophistication and scale of contemporary cyber threats. The law's cybercrime provisions remain focused on traditional digital offenses such as defamation, illegal gambling, and pornography distribution, failing to adequately address advanced persistent threats, state-sponsored cyber attacks, ransomware, and the complex security challenges posed by emerging technologies including artificial intelligence, blockchain, and Internet of Things (IoT) ecosystems.

Recent cybersecurity incidents have highlighted the vulnerabilities inherent in Indonesia's current legal and institutional framework. The National Cyber and Crypto Agency

Received: June 26, 2025
Revised: July 12, 2025
Accepted: July 28, 2025
Published: July 31, 2025
Curr. Ver.: July 31, 2025

(BSSN) documented a 156% increase in cyber attacks in 2023 compared to the previous year, with particularly concerning trends in ransomware attacks targeting critical infrastructure, large-scale personal data breaches affecting millions of Indonesian citizens, and sophisticated phishing campaigns exploiting regulatory gaps. These incidents have caused substantial economic losses, undermined public trust in digital services, and exposed weaknesses in inter-agency coordination and international cooperation mechanisms.

Institutional fragmentation further complicates the regulatory landscape, with multiple government agencies possessing overlapping cybersecurity mandates but lacking clear coordination protocols. The Ministry of Communication and Information Technology (Kominfo), the National Cyber and Crypto Agency (BSSN), the Indonesian National Police (Polri), and sector-specific regulators each maintain separate cybersecurity responsibilities, creating potential conflicts, enforcement gaps, and inefficiencies in threat response capabilities. This fragmented approach particularly hampers Indonesia's ability to respond effectively to transnational cyber threats and participate meaningfully in international cybersecurity cooperation initiatives.

The inadequacy of current legal instruments becomes particularly evident when examining their capacity to address emerging technological challenges. The UU ITE's static provisions fail to accommodate the dynamic nature of cyber threats and technological innovation, lacking adaptive mechanisms that could enable regulatory evolution without requiring lengthy legislative processes. Moreover, while including imprisonment and monetary fines, the law's penalty structure lacks proportionality for different cyber offenses and may provide insufficient deterrence for sophisticated attackers, particularly those operating from jurisdictions beyond Indonesian law enforcement's reach.

Normatively (das sollen), Indonesia aspires to establish a comprehensive, adaptive, and internationally aligned legal system that deters cybercrime while protecting individual privacy rights, fostering technological innovation, and maintaining public confidence in digital services. The country's cybersecurity vision, as articulated in the National Cybersecurity Strategy 2017-2030, emphasizes the creation of a "secure, safe, and trustworthy cyberspace" that supports sustainable economic growth, protects national sovereignty, and ensures the fundamental rights of citizens in the digital realm. This normative framework envisions Indonesia as a leader in regional cybersecurity cooperation and a responsible participant in global digital governance initiatives.

The normative legal framework should encompass several critical elements to achieve these aspirations. First, robust data protection regulations aligned with international best practices, particularly the European Union's General Data Protection Regulation (GDPR) standards, establish clear rights for data subjects and comprehensive obligations for data controllers and processors. Second, comprehensive cybercrime prevention and enforcement mechanisms that address both traditional and emerging forms of cyber threats, including provisions for critical infrastructure protection, incident response coordination, and international cooperation. Third, clear and balanced guidelines for cross-border data transfers that protect national security interests while enabling participation in global digital value chains. Fourth, adaptive regulatory frameworks incorporating sunset clauses, regular review mechanisms, and delegated authority for technical updates that can evolve with technological advancement without requiring comprehensive legislative revision.

The proposed Draft Law on Personal Data Protection (RUU PDP) represents a significant step toward achieving these normative goals, incorporating key principles from international best practices including consent mechanisms, data portability rights, and the right to be forgotten. However, the draft legislation faces implementation challenges and contains regulatory gaps, particularly regarding cross-border data transfer mechanisms, enforcement authority delegation, and coordination with existing cybersecurity institutions. The law's success will depend not only on its legislative enactment but also on the development of implementing regulations, institutional capacity building, and public awareness initiatives.

The urgency of comprehensive legal reform stems from multiple converging factors that threaten Indonesia's digital sovereignty and economic security. The COVID-19 pandemic has accelerated digital adoption across all sectors of society, creating new vulnerabilities while exposing existing weaknesses in regulatory frameworks and enforcement capabilities. High-profile cybersecurity incidents, including the 2022 government data breach affecting 1.3 million citizens, the 2023 ransomware attack on critical infrastructure, and ongoing threats to financial sector institutions, demonstrate the immediate and escalating nature of cyber risks facing Indonesian society.

Indonesia's strategic position as Southeast Asia's largest digital economy makes it an increasingly attractive target for cybercriminals, state-sponsored actors, and transnational organized crime groups seeking to exploit regulatory gaps and enforcement limitations. The country's participation in international trade agreements, regional economic partnerships, and global digital governance initiatives requires compliance with evolving international standards for cybersecurity and data protection, making legal reform not merely a domestic security imperative but an essential component of Indonesia's international economic competitiveness and diplomatic credibility. The failure to establish adequate legal frameworks risks immediate security vulnerabilities, long-term economic isolation, and reduced participation in the global digital economy.

2. Research Methodology

This study employs a normative legal research methodology that systematically analyzes legal norms, principles, and their practical applications within Indonesia's cybersecurity and data protection legal framework. As defined by Peter Mahmud Marzuki, the normative approach emphasizes examining legal sources to identify, analyze, and evaluate the adequacy of existing legal instruments in addressing contemporary challenges. This methodology is particularly appropriate for cybersecurity law research as it examines both positive law (lex lata) and ideal law (lex ferenda), providing a comprehensive understanding of current legal realities and normative aspirations for reform.

The research design follows a doctrinal legal analysis approach, examining statutory regulations, regulatory frameworks, and policy documents to assess their effectiveness in addressing cybersecurity and data protection challenges. This approach, as Terry Hutchinson and Nigel Duncan outlined, involves systematically examining legal sources to identify legal principles, analyze their application, and evaluate their adequacy in addressing contemporary legal problems. The study particularly emphasizes the conceptual framework of das sein (what is) and das sollen (what ought to be), borrowed from Hans Kelsen's pure theory of law, to analyze the gap between current legal reality and normative expectations for Indonesia's cybersecurity legal regime.

Primary legal sources examined in this study include the Indonesian Constitution of 1945, particularly provisions related to information rights and state obligations for public security; the Information and Electronic Transactions Law (UU ITE) No. 11 of 2008 and its amendment Law No. 19 of 2016; the Law on Personal Data Protection No. 27 of 2022 (UU PDP); relevant government regulations and ministerial decrees implementing cybersecurity provisions; and international treaties and conventions ratified by Indonesia, including those related to cybercrime prevention and international cooperation. The analysis also incorporates policy documents such as the National Cybersecurity Strategy, sector-specific cybersecurity guidelines, and institutional frameworks established by various government agencies with cybersecurity mandates.

Secondary sources utilized in this research encompass authoritative academic textbooks on cybersecurity law and data protection, peer-reviewed journal articles published in Indonesian and international law journals focusing on cybersecurity governance, comparative legal studies examining cybersecurity frameworks in ASEAN countries and other relevant jurisdictions, and policy analysis reports from international organizations including the United Nations, OECD, and regional bodies such as ASEAN.[14] The study also incorporates empirical data from government agencies, particularly the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Information Technology (Kominfo), to understand the practical implementation challenges of existing legal frameworks.

The analytical framework employed in this study utilizes legal interpretation methodologies, including grammatical interpretation to examine the literal meaning of legal texts, systematic interpretation to understand legal provisions within their broader regulatory context, historical interpretation to analyze the legislative intent and evolution of cybersecurity laws, and teleological interpretation to evaluate whether existing laws achieve their intended purposes. The study also employs comparative legal analysis, examining cybersecurity frameworks from Singapore, Malaysia, and other relevant jurisdictions to identify best practices and lessons learned that could inform Indonesia's legal reform efforts.

Conceptual analysis is a vital part of the research methodology, especially in assessing whether existing legal concepts sufficiently address emerging technological challenges. This involves analysing legal definitions related to cybercrime, data protection, and cybersecurity governance; reviewing the legal principles that underpin current regulatory approaches; and

evaluating the coherence and consistency of legal frameworks across different sectors and agencies.

The study also investigates the relationship between national cybersecurity law and international legal obligations, analysing how domestic legal reforms can strengthen Indonesia's involvement in international cybersecurity cooperation while preserving national sovereignty and legal independence.

The research process involves multiple stages of analysis, beginning with comprehensive documentation and categorization of relevant legal sources, followed by systematic analysis of legal provisions to identify gaps, inconsistencies, and inadequacies in addressing contemporary cybersecurity challenges. The study then conducts a comparative analysis with international best practices to identify potential reform options. It concludes with normative analysis to develop recommendations for legal reform that balance security imperatives, individual rights protection, and economic development objectives. Quality assurance measures include triangulation of sources, peer review of analytical findings, and validation of conclusions against established legal principles and constitutional requirements.

3. Problem Formulation

The central research question guiding this study is: To what extent does Indonesia's current legal framework adequately address cybersecurity and data protection challenges, and what normative reforms are required to establish a comprehensive, adaptive legal regime that meets international standards while addressing Indonesia's unique socio-legal context?.

4. Results and Discussion

4.1 Comprehensive Analysis of Indonesia's Current Cybersecurity Legal Framework

The Information and Electronic Transactions Law (UU ITE): Foundations and Limitations

The Information and Electronic Transactions Law (UU ITE) is the cornerstone of Indonesia's cybersecurity legislation, establishing fundamental provisions for electronic transactions, digital signatures, electronic evidence, and cybercrime penalties. Initially enacted in 2008 and subsequently amended in 2016, the UU ITE represented a significant advancement in Indonesia's legal modernization efforts, providing the first comprehensive framework for regulating cyberspace activities. However, detailed analysis reveals substantial limitations in the law's capacity to address the sophistication and scale of contemporary cyber threats, particularly those involving state-sponsored actors, advanced persistent threats, and emerging technologies.

The law's cybercrime provisions, outlined in Articles 27-37, demonstrate a traditional approach to digital crime that reflects the technological understanding prevalent at enactment. These provisions focus primarily on content-related offenses, including defamation, hate speech, illegal gambling, and pornography distribution, while providing limited coverage for sophisticated technical attacks such as advanced persistent threats, supply chain compromises, and zero-day exploits. The penalty structure includes imprisonment terms ranging from six to twelve years and monetary fines up to IDR 12 billion. It lacks proportionality mechanisms that could differentiate between various categories of cyber offenses based on their sophistication, impact, and intent.

Critical gaps in the UU ITE's coverage include the absence of specific provisions for critical infrastructure protection, inadequate frameworks for incident response coordination, limited mechanisms for international cooperation in cybercrime investigations, and insufficient provisions for emerging technologies, including artificial intelligence, blockchain, and Internet of Things ecosystems. The law's approach to jurisdiction, while establishing Indonesian authority over cyber offences affecting Indonesian interests, lacks clarity regarding cross-border investigations and evidence collection, particularly in cases involving international criminal networks or state-sponsored attacks.

Institutional Fragmentation and Governance Challenges

Indonesia's cybersecurity governance structure suffers from significant institutional fragmentation, with multiple agencies possessing overlapping mandates but lacking precise coordination mechanisms and unified command structures. The Ministry of Communication and Information Technology (Kominfo) maintains broad regulatory authority over information and communication technology sectors, including content regulation and service provider licensing. The National Cyber and Crypto Agency (BSSN), established in 2017,

serves as the national cybersecurity authority responsible for cybersecurity policy coordination, incident response, and critical infrastructure protection. The Indonesian National Police (Polri) operates specialized cybercrime units responsible for criminal investigations and enforcement. Meanwhile, sector-specific regulators, including Bank Indonesia, the Financial Services Authority (OJK), and others, maintain cybersecurity oversight within their respective domains.

This fragmented approach creates several operational challenges that reduce the effectiveness of Indonesia's cybersecurity response capabilities. Information sharing between agencies remains inconsistent and often relies on personal relationships rather than formal protocols, hindering coordinated threat intelligence analysis and response planning. Jurisdictional conflicts frequently arise, especially in cases involving multiple sectors or agencies, which can delay investigation and response activities. The lack of a unified national cybersecurity command structure also hampers Indonesia's ability to respond effectively to major incidents that require coordinated multi-agency responses, such as attacks on critical infrastructure or large-scale data breaches affecting multiple sectors.

Resource allocation across agencies reflects these coordination challenges, with duplicated capabilities in some areas and significant gaps in others. Technical capacity varies substantially between agencies, with some maintaining sophisticated cyber threat analysis capabilities while others lack basic incident response resources. Training and professional development programs remain largely agency-specific, limiting cross-agency knowledge sharing and collaborative capability development.

Regulatory Gaps in Emerging Technology Governance

The rapid evolution of information and communication technologies has outpaced Indonesia's regulatory development, creating significant gaps in legal frameworks governing emerging technologies with substantial cybersecurity implications. Artificial intelligence systems, increasingly deployed across government and private sector operations, operate without specific cybersecurity requirements or accountability mechanisms for AI-related security failures. While receiving attention for their economic potential, Blockchain and distributed ledger technologies lack comprehensive security standards and regulatory oversight mechanisms.

Internet of Things (IoT) devices, proliferating rapidly across Indonesian households and businesses, operate without mandatory security standards or certification requirements, creating potential entry points for cybercriminals and state-sponsored actors. The absence of IoT security regulations is particularly concerning given the deployment of these devices in critical infrastructure sectors, including energy, transportation, and telecommunications. Cloud computing services, essential for Indonesia's digital transformation initiatives, operate under fragmented regulatory frameworks that vary by sector and fail to provide comprehensive security requirements for cross-border data processing and storage.

Edge computing and 5G network deployments present additional regulatory challenges that current legal frameworks inadequately address. Integrating these technologies in critical infrastructure sectors requires sophisticated cybersecurity measures and regulatory oversight mechanisms that exceed the scope of existing legal instruments. The absence of comprehensive technology-specific regulations creates uncertainty for domestic and international investors while potentially exposing Indonesian users to security risks from inadequately regulated emerging technologies.

4.2 Detailed Evaluation of Emerging Legal Frameworks

The Law on Personal Data Protection: Progress and Persistent Challenges

The Law on Personal Data Protection (UU PDP) represents Indonesia's most significant advancement in data protection regulation, incorporating internationally recognized principles for privacy protection and establishing comprehensive rights for data subjects alongside detailed obligations for data controllers and processors. The draft legislation draws extensively from the European Union's General Data Protection Regulation (GDPR), adapting key provisions including lawful bases for data processing, consent mechanisms, data subject rights, and accountability principles to Indonesia's legal and cultural context.

The RUU PDP establishes seven categories of data subject rights, including rights to information, access, rectification, erasure, restriction of processing, data portability, and objection to processing. These rights substantially enhance data protection provisions in the UU ITE and sector-specific regulations, providing Indonesian citizens with comprehensive mechanisms for controlling their data. The draft law also establishes detailed obligations for

data controllers, including requirements for privacy impact assessments, data protection officer appointments for large-scale processing operations, and notification requirements for data breaches affecting data subject rights.

However, critical gaps in the draft legislation may limit its effectiveness in addressing contemporary data protection challenges. While included in the draft, cross-border data transfer provisions lack specificity regarding adequacy decisions, binding corporate rules, and other mechanisms for ensuring equivalent protection when personal data is transferred outside Indonesia.

The relationship between the UU PDP and existing sectoral data protection regulations remains unclear, particularly regarding financial services data protection rules, healthcare information governance, and telecommunications subscriber data requirements. This regulatory overlap could create compliance uncertainties and enforcement challenges, undermining the law's effectiveness. Additionally, the draft law's implementation timeline and capacity-building requirements for regulatory authorities have not been adequately specified, raising concerns about enforcement readiness upon enactment.

National Cybersecurity Strategy: Implementation Challenges and Gaps

Indonesia's National Cybersecurity Strategy provides a comprehensive policy framework for cybersecurity governance, emphasizing multi-stakeholder coordination, public-private partnerships, and capacity-building initiatives. The strategy identifies five pillars: cybersecurity governance, cyber resilience, cyber defence, cyber diplomacy, and cybersecurity industry development. Implementation progress has been inconsistent, with significant variations across strategic objectives and participating institutions.

The governance pillar, intended to establish clear institutional roles and coordination mechanisms, has faced substantial implementation challenges. While the National Cyber and Crypto Agency (BSSN) has been established as the national cybersecurity coordinator, operational coordination mechanisms remain underdeveloped. Information sharing protocols between government agencies and private sector entities lack formal structure and legal authority, limiting the effectiveness of coordinated threat response capabilities. The absence of specific performance indicators and accountability mechanisms for strategy implementation has hindered progress assessment and adaptive management.

Cyber resilience initiatives, particularly those focused on critical infrastructure protection, have progressed slowly due to resource constraints and regulatory gaps. The strategy envisions comprehensive cybersecurity requirements for critical infrastructure operators, but implementing regulations remains under development for most sectors. Public-private partnerships, essential for effective critical infrastructure protection, lack formal frameworks and incentive structures that could encourage meaningful private sector participation.

The cyber defence pillar, emphasising government cybersecurity capabilities and incident response mechanisms, has achieved mixed results. While technical capabilities have improved through training programs and technology acquisitions, institutional coordination during major incidents remains challenging. The strategy's emphasis on developing indigenous cybersecurity capabilities has produced some successes, including domestic cybersecurity product development and research initiatives. Still, resource constraints and competitive disadvantages relative to international alternatives have limited progress.

4.3 Sectoral Cybersecurity Regulations: Fragmented Approaches and Coordination Challenges

Indonesia's approach to sectoral cybersecurity regulation reflects the broader institutional fragmentation characterizing the country's cybersecurity governance structure. The financial services sector, regulated primarily by Bank Indonesia and the Financial Services Authority (OJK), has developed comprehensive cybersecurity requirements, including mandatory incident reporting, cybersecurity governance frameworks, and periodic security assessments. These regulations represent some of Indonesia's most advanced cybersecurity requirements, incorporating international best practices and providing detailed guidance for implementation.

However, significant variations exist across different sectors, creating inconsistencies in cybersecurity standards and potentially enabling attackers to exploit weaker regulatory environments. While subject to general cybersecurity requirements under the Ministry of Communication and Information Technology regulations, the telecommunications sector lacks comprehensive critical infrastructure protection standards comparable to those in the

financial industry. Despite the vital importance of power generation and distribution systems to national security and economic stability, energy sector cybersecurity regulations remain under development.

Transportation sector cybersecurity requirements vary substantially between different transportation modes. Aviation cybersecurity is subject to international standards through the International Civil Aviation Organization (ICAO). In contrast, maritime and land transportation systems operate under less comprehensive regulatory frameworks. This sectoral variation creates potential vulnerabilities that sophisticated attackers could exploit to access critical infrastructure systems or conduct attacks with cascading effects across multiple sectors.

The absence of cross-sectoral coordination mechanisms further complicates sectoral cybersecurity governance. Information sharing between sectoral regulators occurs primarily through informal channels, limiting the development of comprehensive threat intelligence and coordinated response capabilities. Incident response coordination across sectors remains ad hoc, potentially hampering effective response to attacks affecting multiple critical infrastructure sectors simultaneously.Comprehensive Comparative Analysis with Regional and International Frameworks

ASEAN Cybersecurity Cooperation and Regional Standards

Indonesia's cybersecurity legal framework must be evaluated within the broader context of ASEAN cybersecurity cooperation initiatives and regional harmonization efforts. The ASEAN Cybersecurity Cooperation Strategy provides a framework for information sharing, capacity building, and coordinated response to regional cyber threats, but implementation remains inconsistent across member states. Indonesia's participation in regional initiatives has been active but constrained by domestic capacity limitations and institutional coordination challenges.

Singapore's cybersecurity framework, anchored by the Cybersecurity Act 2018, provides a comprehensive model for critical infrastructure protection and incident response coordination that could inform Indonesia's regulatory development efforts. The Singapore framework establishes apparent authority for the national cybersecurity agency, mandates cybersecurity requirements for critical information infrastructure, and provides robust enforcement mechanisms, including significant monetary penalties. Singapore's approach to public-private partnership, including formal information sharing arrangements and coordinated threat response capabilities, offers valuable lessons for enhancing Indonesia's cybersecurity governance structure.

While less comprehensive than Singapore's, Malaysia's cybersecurity framework provides relevant experience in adapting international cybersecurity standards to developing country contexts. Malaysia's Personal Data Protection Act 2010 and the Strategic Trade Act 2010 offer insights into practical implementation strategies for data protection and cybersecurity export controls that could inform Indonesia's regulatory development. Thailand's cybersecurity framework, established through the Cybersecurity Act 2019, demonstrates approaches to balancing cybersecurity requirements with digital rights protection that may be relevant to Indonesia's constitutional framework.

Regional cooperation mechanisms, including the ASEAN Computer Emergency Response Team (CERT) network and the ASEAN Ministerial Conference on Cybersecurity, provide forums for sharing best practices and coordinating responses to transnational threats. However, the effectiveness of these mechanisms is limited by varying domestic capacity levels and differing regulatory approaches across member states. Indonesia's role in ASEAN provides opportunities to promote regional cybersecurity cooperation while advancing domestic regulatory development objectives.

International Standards and Global Best Practices

International cybersecurity frameworks provide vital benchmarks for evaluating Indonesia's legal and regulatory development needs. The Council of Europe's Budapest Convention on Cybercrime represents the primary international framework for cybercrime cooperation, establishing standards for domestic criminal law, procedural powers for investigation, and international cooperation mechanisms. Indonesia's reluctance to ratify the Budapest Convention limits its participation in international cybercrime cooperation networks and may hinder law enforcement effectiveness in addressing transnational cyber threats.

The European Union's Network and Information Security (NIS) Directive provides a comprehensive framework for cybersecurity governance that has influenced regulatory development globally. The NIS Directive's approach to critical infrastructure identification, cybersecurity requirements, and incident reporting mechanisms offers valuable guidance for Indonesia's regulatory development efforts. However, the adaptation of EU frameworks must consider Indonesia's different institutional capacities, legal traditions, and economic development priorities.

The OECD Guidelines for the Security of Information Systems and Networks provide non-binding but authoritative guidance on cybersecurity governance principles that could inform Indonesia's policy development. These guidelines emphasize awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment as fundamental principles for cybersecurity governance. The guidelines' emphasis on multi-stakeholder participation and adaptive management approaches aligns with Indonesia's declared policy objectives but requires enhanced implementation mechanisms.

International standards organisations, including the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), have developed comprehensive cybersecurity standards that could provide technical frameworks for Indonesia's regulatory requirements. ISO/IEC 27001 information security management standards and ISO/IEC 27032 cybersecurity guidelines offer established frameworks for organizational cybersecurity governance that could inform Indonesian regulatory development.

4.4. Enhanced Analysis of Institutional and Enforcement Challenges

Law Enforcement Capacity and Capability Development

Indonesia's cybercrime law enforcement capabilities have evolved significantly through specialized unit development, training programs, and international cooperation initiatives. The Indonesian National Police's cybercrime directorate operates specialized units for cybercrime investigation, digital forensics, and international cooperation, with personnel trained in advanced technical investigative techniques and legal procedures for digital evidence collection. The Virtual Police initiative represents an innovative approach to online law enforcement presence and crime prevention. It has received international recognition for its effectiveness in addressing online fraud and social media-based criminal activities.

However, substantial capacity gaps limit law enforcement's effectiveness in addressing sophisticated cyber threats. Technical capacity for investigating advanced persistent threats, state-sponsored attacks, and sophisticated financial cybercrime requires continuous enhancement through training, equipment acquisition, and international cooperation. Resource constraints limit the number of specialized cybercrime investigators and digital forensics experts, creating bottlenecks in case processing and investigation quality.

International cooperation capabilities require strengthening to address the transnational nature of contemporary cyber threats effectively. While Indonesia maintains mutual legal assistance treaties with numerous countries, procedural complexities and diplomatic processes often delay international cybercrime investigations beyond the timeframes necessary for practical evidence preservation and suspect apprehension. The absence of specialized cybercrime courts may also limit prosecution effectiveness, as judges may lack the technical expertise required to understand complex cybercrime cases and evaluate digital evidence appropriately.

Public-Private Partnership Development and Information Sharing

Effective cybersecurity governance requires robust public-private partnerships, given the private sector's ownership of critical infrastructure and its role in cybersecurity technology development and implementation. Indonesia's current framework provides limited formal mechanisms for cybersecurity information sharing between government agencies and private sector entities, relying primarily on voluntary cooperation and ad hoc relationships.

The financial services sector demonstrates the most advanced public-private cybersecurity cooperation. Bank Indonesia and the Financial Services Authority maintain formal relationships with financial institutions for cybersecurity information sharing and coordinated incident response . However, these arrangements lack legal frameworks that could protect participating entities from liability concerns and competitive disadvantage that may discourage information sharing about cybersecurity incidents and vulnerabilities.

Critical infrastructure sectors, including telecommunications, energy, and transportation, require enhanced public-private partnership frameworks that balance national security requirements with commercial interests and operational autonomy. International experience suggests that effective information sharing requires legal protections for shared information, incentive structures for participation, and clear guidelines for information use and dissemination. Indonesia's development of such frameworks could benefit from examining successful models, including the United States Cybersecurity Information Sharing Act and similar frameworks in other jurisdictions.

4.5 Technological Adaptation and Emerging Challenge Analysis

Artificial Intelligence and Machine Learning Security Implications

The rapid deployment of artificial intelligence and machine learning technologies across Indonesian government and private sector operations presents novel cybersecurity challenges that existing legal frameworks inadequately address. AI systems' susceptibility to adversarial attacks, data poisoning, and model theft requires specialized security measures and regulatory oversight that current cybersecurity laws do not provide. The use of AI in cybersecurity defence offers significant capability enhancement potential. Still, it raises concerns about algorithmic bias, false favourable rates, and automated decision-making accountability that require careful regulatory consideration.

Machine learning systems' reliance on large datasets for training and operation creates new categories of cybersecurity risks, including training data compromise, model extraction attacks, and privacy violations through inference attacks. Indonesia's evolving data protection framework must address these AI-specific risks while enabling beneficial AI applications in cybersecurity and other critical sectors. The cross-border nature of many AI services and the global concentration of AI technology development also create challenges for national cybersecurity governance and digital sovereignty that require careful policy balance.

Internet of Things and Critical Infrastructure Security

The proliferation of Internet of Things (IoT) devices across Indonesian households, businesses, and critical infrastructure creates unprecedented cybersecurity challenges that current regulatory frameworks inadequately address. IoT devices' limited computational resources, extended operational lifespans, and frequent security vulnerabilities create persistent attack vectors that sophisticated adversaries can exploit for espionage, sabotage, or criminal purposes.

Critical infrastructure sectors' increasing reliance on IoT technologies for operational monitoring, predictive maintenance, and automated control creates new cybersecurity risks requiring specialized regulatory attention. Integrating IoT devices with supervisory control and data acquisition (SCADA) systems and industrial control systems creates potential pathways for cyberattacks to cause physical damage and operational disruption with significant economic and safety implications.

The absence of mandatory cybersecurity standards for IoT devices, particularly those deployed in critical infrastructure contexts, represents a significant regulatory gap that sophisticated adversaries could exploit. International experience suggests that effective IoT cybersecurity governance requires a combination of device-level security standards, network-level protection requirements, and operational security protocols that address the whole IoT ecosystem lifecycle. The current regulatory landscape suffers from fragmented oversight, with multiple agencies possessing cybersecurity mandates but lacking precise coordination mechanisms. The Ministry of Communication and Information Technology (Kominfo), the National Cyber and Crypto Agency (BSSN), and the Indonesian National Police (Polri) each maintain separate cybersecurity responsibilities, creating potential conflicts and gaps in enforcement.

This fragmentation is particularly problematic in incident response and cross-border cooperation. The absence of clear protocols for information sharing between agencies and with international partners limits Indonesia's ability to respond effectively to transnational cyber threats.

4.6 Evaluation of Emerging Legal Frameworks

The Law on Personal Data Protection (UU PDP)

The UU PDP represents a significant advancement in Indonesia's data protection regime, establishing comprehensive rights for data subjects and obligations for data controllers. The draft law incorporates key principles from the European Union's General

Data Protection Regulation (GDPR), including consent mechanisms, data portability rights, and the right to be forgotten.

However, critical gaps remain in the draft legislation. The law lacks specific provisions for cross-border data transfers, particularly regarding adequacy decisions and binding corporate rules. Additionally, while including monetary penalties, the enforcement mechanisms may be insufficient to ensure compliance by large multinational corporations.

National Cybersecurity Strategy Implementation

The National Cybersecurity Strategy provides a comprehensive framework for cybersecurity governance, emphasizing multi-stakeholder coordination and public-private partnerships. However, implementation has been hampered by resource constraints and institutional capacity limitations.

The strategy's emphasis on developing indigenous cybersecurity capabilities is commendable, but the lack of specific timelines and performance indicators limits its effectiveness as a policy instrument. Furthermore, the strategy's focus on defensive measures may be insufficient to address the evolving threat landscape.

4.7. Comparative Analysis with Regional Frameworks

ASEAN Cybersecurity Cooperation

Indonesia's cybersecurity legal framework must be evaluated within the context of ASEAN cybersecurity cooperation initiatives. The ASEAN Cybersecurity Cooperation Strategy provides a regional framework for information sharing and capacity building, but implementation remains inconsistent across member states.

Singapore's comprehensive cybersecurity legislation, including the Cybersecurity Act 2018, provides a model for proactive threat mitigation and critical infrastructure protection. Malaysia's Personal Data Protection Act 2010 offers insights into effective data protection enforcement mechanisms that could inform Indonesia's regulatory development.

International Standards and Best Practices

International frameworks such as the Budapest Convention on Cybercrime and the OECD Guidelines on the Security of Information Systems provide normative standards for cybersecurity legislation. Indonesia's reluctance to ratify the Budapest Convention limits its ability to participate in international cybercrime cooperation mechanisms.

The European Union's NIS Directive offers a comprehensive approach to network and information security that could inform Indonesia's critical infrastructure protection efforts. However, the adaptation of these frameworks must consider Indonesia's unique legal traditions and institutional capacity constraints.

4.8. Institutional and Enforcement Challenges

Law Enforcement Capacity

Indonesia's cybercrime enforcement capabilities have improved significantly through initiatives such as the Virtual Police program and specialized cybercrime units within the National Police. However, challenges remain in technical capacity, international cooperation, and resource allocation.

Establishing the National Cyber and Crypto Agency (BSSN) represents a significant institutional advancement, but the agency's coordination mechanisms with other law enforcement bodies require strengthening. Additionally, the lack of specialized cybercrime courts may limit the effectiveness of prosecution efforts.

Public-Private Collaboration

Effective cybersecurity governance requires robust public-private partnerships, particularly given the private sector's ownership of critical infrastructure. Indonesia's current framework provides limited mechanisms for information sharing and collaborative threat mitigation.

Establishing sector-specific cybersecurity requirements, as implemented in the financial services sector through Bank Indonesia regulations, demonstrates the potential for targeted regulatory approaches. However, these efforts require expansion to other critical industries, including telecommunications, energy, and transportation.

4.9. Technological Adaptation and Future Challenges

Emerging Technologies

The rapid adoption of emerging technologies, including artificial intelligence, blockchain, and Internet of Things devices, presents new challenges for cybersecurity regulation. Indonesia's current legal framework lacks specific provisions for addressing the security implications of these technologies.

Integrating cybersecurity mesh and edge computing technologies in critical sectors requires adaptive regulatory frameworks that can accommodate technological innovation while ensuring compliance with national security requirements. The static approach to cybersecurity regulation may be inadequate for addressing these dynamic technological challenges.

Digital Sovereignty and Cross-Border Data Governance

Indonesia's digital sovereignty initiatives, including data localization requirements and restrictions on cross-border data transfers, reflect legitimate national security concerns but may conflict with international trade obligations and global digital economy participation. The balance between digital sovereignty and international cooperation requires careful consideration in regulatory design. Indonesia's approach must ensure national security while participating in global digital value chains and international cybersecurity cooperation mechanisms.

5. Conclusion

Indonesia's current legal framework for cybersecurity and data protection provides a foundational structure but remains inadequate for addressing the complexity and sophistication of contemporary cyber threats. The analysis reveals significant gaps in existing legislation, particularly the UU ITE, which fails to address advanced persistent threats, state-sponsored cyber attacks, and the security implications of emerging technologies.

The Law on Personal Data Protection represents a significant advancement in Indonesia's data protection regime, but implementation challenges and regulatory gaps persist. The fragmented nature of cybersecurity governance, with multiple agencies possessing overlapping jurisdictions, limits the effectiveness of enforcement efforts and international cooperation.

The comparative analysis with regional frameworks demonstrates that Indonesia lags behind neighbouring countries in developing comprehensive cybersecurity legislation. The reluctance to ratify international instruments such as the Budapest Convention limits Indonesia's ability to participate in global cybercrime cooperation mechanisms.

Technological adaptation presents ongoing challenges, with emerging technologies outpacing regulatory development. The static approach to cybersecurity regulation may be inadequate for addressing dynamic technological challenges and evolving threat landscapes.

6. Recommendations

Based on a comprehensive analysis of Indonesia's cybersecurity and data protection legal framework, this study recommends a systematic approach to legal reform that addresses identified gaps while building upon existing institutional foundations. The acceleration of the Law on Personal Data Protection (UU PDP) enactment should be prioritised as the foundational element of Indonesia's enhanced data protection regime, with implementing regulations developed concurrently to ensure effective enforcement upon legislative passage. This legislation must incorporate strengthened provisions for cross-border data transfers, enhanced enforcement mechanisms including administrative and criminal sanctions, and clear coordination protocols with existing sectoral data protection requirements. Simultaneously, a comprehensive revision of the Information and Electronic Transactions Law (UU ITE) is essential to address sophisticated cyber threats, including advanced persistent threats, state-sponsored attacks, and emerging technology security challenges, with adaptive regulatory mechanisms that enable regular updates without requiring lengthy legislative processes.

The establishment of unified cybersecurity governance structures is a key institutional reform priority. It requires developing formal coordination protocols among the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information Technology (Kominfo), the Indonesian National Police (Polri), and sectoral regulators to resolve jurisdictional conflicts and improve coordinated threat response. This governance framework should include comprehensive public-private partnership mechanisms with legal

protections for sharing cybersecurity information, incentive structures to encourage private sector involvement, and sector-specific cybersecurity requirements that protect critical infrastructure across telecommunications, energy, financial services, and transportation sectors. Improving law enforcement capabilities through establishing specialised cybercrime courts, expanding international cooperation agreements, such as ratifying the Budapest Convention, and continuous capacity-building programs for technical investigative skills and digital forensics will strengthen Indonesia's ability to deter and prosecute cybercrime effectively. Additionally, implementing broad public awareness and digital literacy programmes, cybersecurity education and professional certification, investments in indigenous cybersecurity research and development, and adaptive regulatory frameworks with sunset clauses and delegated technical authority, will lay the foundation for Indonesia's long-term cybersecurity resilience and digital sovereignty. These efforts will also ensure meaningful participation in international cybersecurity cooperation and integration into the global digital economy.

References

Adiningsih, S. (2019). *Indonesia's digital-based economic transformation: The emergence of new technological, business, economic, and policy trends in Indonesia*. Jakarta, Indonesia: Gramedia Pustaka Utama.

Ajayi, E. F. G. (2016). Challenges to enforcement of cybercrime laws and policy. *Journal of Internet and Information Systems, 6*(1). https://doi.org/10.5897/JIIS2015.0089

Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive, 11*(1). https://doi.org/10.30574/ijsra.2024.11.1.0217

Arliman, L. (2017). Undang-undang Nomor 17 Tahun 2016 tentang Penetapan Perppu 1 Tahun 2016 sebagai wujud perlindungan anak ditinjau dari perspektif hukum tata negara. *Jurnal Hukum POSITUM, 1*(2). https://doi.org/10.35706/positum.v1i2.846

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance, 31*(3). https://doi.org/10.1111/gove.12309

Bunse, S., & Fritz, V. (2012). Making public sector reforms work: Political and economic contexts, incentives, and strategies. *World Bank Policy Research Working Paper, 6174*. https://doi.org/10.1596/1813-9450-6174

Gustryan, M., & Sulaiman, A. (2025). The urgency of regulatory reformulation and strengthening the capacity of law enforcers in combating cybercrime through a criminal law approach in Indonesia. *Greenation International Journal of Law and Social Sciences, 3*(2). https://doi.org/10.38035/gijlss.v3i2.416

Haber, E., & Zarsky, T. (2016). Cybersecurity for infrastructure: A critical analysis. *Florida State University Law Review*.

Hidayat, T. (2024). Juridical review article 27A of Law number 1 of 2024 concerning the second amendment to Law number 11 of 2008 concerning information and electronic transactions. *Jurnal Hukum Samudra Keadilan, 19*(2). https://doi.org/10.33059/jhsk.v19i2.10650

Hoofnagle, C. J., Van Der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1). https://doi.org/10.1080/13600834.2019.1573501

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review, 17*(1). https://doi.org/10.21153/dlr2012vol17no1art70

Ihsan, F., & Bintarsari, N. K. (2021). Internet governance forum analysis on artificial intelligence in cybersecurity. *Insignia: Journal of International Relations*.

Imran, M. F. (2023). Preventing and combating cybercrime in Indonesia. *International Journal of Cyber Criminology, 17*(1).

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information security management systems*. https://www.iso.org/standard/54534.html

IT Governance Privacy Team. (2025). *EU General Data Protection Regulation (GDPR): An implementation and compliance guide*. Packt Publishing Ltd.

Jeelan, P. M., Saini, R., Parida, S., Minhas, D., & Agarwal, A. (2025). The threat landscape of ransomware in critical infrastructure: An optimization perspective. In *Proceedings of the 2025 International Conference on Automation and Computation (AUTOCOM)* (pp. 917–922). IEEE. https://doi.org/10.1109/AUTOCOM64127.2025.10957218

Jiwantara, F. A., & Maksudi, K. (2020). How are government's liability in Indonesia and Netherland?: Juridical-normative study with a comparative approach. *Prof. (Dr) RK Sharma, 20*(4). https://doi.org/10.37506/mlu.v20i4.2018

Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights, 3*(1). https://doi.org/10.58812/eslhr.v3i01.351

Litman, J. (1989). Copyright legislation and technological change. *Oregon Law Review*.

Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy, 3*(3). https://doi.org/10.3390/jcp3030017

Nansi, M. (2024). Bridging legal theory and comparative law: Implications for cyber law and its role in modern society.

Neta, Y., Awanisa, A., & Melisa, M. (2022). The urgency of establishing independent supervisory authority for personal data protection in Indonesia. *Constitutionale, 3*(1). https://doi.org/10.25041/constitutionale.v3i1.2535

Norris, D. F., Mateczun, L. K., & Forno, R. F. (2022). *Cybersecurity and local government*. John Wiley & Sons. https://doi.org/10.1002/9781119788317

Praditya, E., et al. (2023). National cybersecurity policy analysis for effective decision-making in the age of artificial intelligence. *Journal of Human Security, 19*(2).

Rahman, F. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new personal data protection act in Indonesia. *UUM Journal of Legal Studies, 16*(1). https://doi.org/10.32890/uumjls2025.16.1.1

Ristovska, T., Gospodinov, G., Gotsev, L., Syarova, S., & Angelova, V. (2025). A review on AI in cybersecurity: Ethical challenges and regulatory frameworks. In *Proceedings of the International Scientific and Practical Conference: Environment. Technology. Resources* (Vol. 2, pp. 285–291).

Riswanih, I., & Aridhayandi, M. R. (2025). Effectiveness of the Ministry of Communication and Information in handling the misuse of personal data. *Jurnal Hukum De'Rechtsstaat (JHD)*.

Santoso, P. A. (2024). The role of threat intelligence sharing in strengthening collective cyber defense across organizations. *Global Research Perspectives on Cybersecurity Governance, Policy, and Management, 8*(12).

Shidiqque, M. R., & Juned, M. (2023). Human capital development for cybersecurity: Examining BSSN's contributions in the Indonesia-Australia Cyber Policy Dialogue (2018–2020). *Journal of Social and Political Sciences, 6*(4). https://doi.org/10.31014/aior.1991.06.04.457

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science, 192*, 3217–3225. https://doi.org/10.1016/j.procs.2021.08.003

Susanto, D. (2022a). Sharia-based legal formula for personal data protection in the financial services industry post-COVID-19 pandemic. *BULLET: Jurnal Multidisiplin Ilmu, 1*(4).

Susanto, D. (2022b). Urgensi pengaturan data digital/elektronik pribadi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 2*(3). https://doi.org/10.53363/bureau.v2i3.110

Tan, E. E. G., & Ang, B. (2022). ASEAN ambiguity on international law and norms for cyberspace. *Baltic Yearbook of International Law Online, 20*(1). https://doi.org/10.1163/22115897_02001_008

Widiatno, M. I. F. R., & Gunadi, A. (2022). Electronic operator's legal responsibility for personal data leakage. *The Seybold Report*.

Xi, W. (2024). Regulatory changes and compliance challenges. In *Strategic financial management: A managerial approach* (pp. 119–134). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83608-106-720241008