JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

Digital Privacy and Personal Data Protection in Southeast Asia: Challenges and Efforts toward Legal Harmonization

Arwansyah bin Kirin[1*], Yana Chaeru Taufik Ismail[2]
[1]Universiti Tun Hussein Onn Malaysia, Malaysia
[2]Universitas Islam Nusantara, Indonesia

[*]Corresponding Author Email: arwansyah@uthm.edu.my

Article History:
Submitted: Agustus 8, 2024 | Revised: April 5, 2025 | Accepted: May 22, 2025 | Published: June 30, 2025

Citation (APA Style):
Bin Kirin, A., & Ismail, Y. C. T. (2025). Digital privacy and personal data protection in Southeast Asia: Challenges and efforts toward legal harmonization. *Justitia Nova: Indonesian Journal of Modern Law, 1*(1), 32–49.

Abstract
Rapid digital transformation and increasing cross-border data flows have intensified concerns regarding digital privacy and personal data protection in Southeast Asia. This study aims to analyze the principal legal and institutional challenges hindering the harmonization of digital privacy regulation within ASEAN and to evaluate strategies for strengthening regional digital governance cooperation. Using a normative juridical method with statutory, conceptual, and comparative approaches, this research examines digital governance frameworks in several Southeast Asian countries alongside ASEAN initiatives and international standards such as the General Data Protection Regulation (GDPR). The study finds that ASEAN member states continue to experience significant disparities in legal definitions, enforcement mechanisms, cybersecurity governance, and institutional capacity, resulting in regulatory fragmentation and weak regional interoperability. The findings further demonstrate that ASEAN's digital governance framework remains predominantly soft-law oriented and institutionally fragmented, limiting the effectiveness of regional harmonization efforts. In addition, emerging technologies such as artificial intelligence, fintech systems, and biometric data processing create new regulatory challenges concerning accountability, digital sovereignty, and consumer protection. The novelty of this research lies in its integrated comparative analysis combining digital privacy, cybersecurity, artificial intelligence governance, and adaptive governance perspectives within a unified Southeast Asian legal framework, which remains underexplored in previous studies. Nevertheless, this study is limited by its doctrinal and desk-based methodology without empirical investigation or stakeholder interviews.

Keywords:
ASEAN digital governance; cybersecurity; digital privacy; harmonization; personal data protection

1. Introduction
The rapid expansion of the digital economy in Southeast Asia has transformed the way governments, businesses, and individuals interact within digital environments. The increasing use of e-commerce platforms, digital financial services, artificial intelligence, biometric systems, cloud computing, and cross-border digital transactions has significantly increased the

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

volume of personal data collected and processed across the region. ASEAN countries are currently among the fastest-growing digital markets globally, driven by widespread internet penetration and mobile technology adoption. However, this rapid digital transformation has also intensified concerns regarding digital privacy, cybersecurity, misuse of personal data, algorithmic discrimination, and inadequate legal protection for users. Recent studies indicate that Southeast Asian countries continue to face structural and regulatory barriers in adapting their legal systems to the evolving digital environment (Abdurrahman, 2025; Yi et al., 2024). The growing reliance on digital systems in sectors such as healthcare, banking, public administration, and online commerce further demonstrates the urgency of establishing comprehensive legal frameworks capable of protecting personal data while simultaneously supporting innovation and economic growth. Consequently, digital privacy and personal data protection have become central issues in contemporary legal governance discussions within Southeast Asia.

Despite the increasing recognition of data protection as a fundamental legal concern, the legal frameworks governing digital privacy across Southeast Asia remain fragmented and uneven. Countries such as Singapore and Thailand have established relatively comprehensive personal data protection regulations, while others are still in the process of developing institutional and regulatory capacities. Indonesia, for example, recently enacted the Personal Data Protection Law, yet significant challenges remain regarding implementation, institutional readiness, and enforcement mechanisms. Comparative studies reveal that legal harmonization in the region is complicated by differing political systems, legal traditions, economic priorities, and national sovereignty concerns (Lim et al., 2025; Dolzhenko, 2025). Furthermore, the increasing use of biometric technologies, AI-driven systems, and digital surveillance mechanisms has created new legal complexities concerning consent, accountability, transparency, and data ownership. Research on algorithmic bias and AI governance also highlights that emerging technologies may produce discriminatory outcomes when legal safeguards are insufficient (Borba et al., 2024; Xiao, 2025). In addition, cross-border digital trade and international data transfers create regulatory tensions between national security interests and global economic integration (Ma et al., 2024; Zhang & Gao, 2025). These conditions indicate that the absence of harmonized legal standards not only weakens public trust, but also creates regulatory uncertainty that may hinder sustainable regional digital integration.

The legal challenges associated with digital privacy are also increasingly interconnected with broader issues of cybersecurity, consumer protection, electronic evidence, and digital governance. The growth of online transactions and digital platforms has exposed users to cyber threats, unauthorized data processing, and exploitative contractual arrangements. Studies concerning digital transactions and consumer protection emphasize that existing legal systems often struggle to address unfair digital practices, particularly in relation to click-wrap agreements, platform monopolies, and unequal bargaining positions between corporations and consumers (Panjaitan et al., 2025; Syahputra et al., 2025). Similarly, developments in electronic court systems and digital evidence demonstrate the need for procedural reforms capable of accommodating technological advancements within legal institutions (Adinda et al., 2025; Mardyansyah et al., 2025). Cybersecurity governance has also become a crucial issue due to the increasing vulnerability of digital infrastructure to cyberattacks and transnational

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

cybercrime (Balarabe, 2025; Senarak, 2025). These developments demonstrate that digital privacy protection cannot be examined separately from broader issues of cybersecurity resilience, digital accountability, and institutional governance. Therefore, legal harmonization requires not only substantive data protection regulations but also coordinated institutional mechanisms capable of responding to evolving digital risks across jurisdictions.

At the regional level, ASEAN has attempted to encourage cooperation in digital governance through various policy initiatives and frameworks. Nevertheless, the implementation of regional standards remains inconsistent due to varying levels of legal development and enforcement capacity among member states. The challenge of harmonization is further complicated by the influence of global regulatory models such as the European Union's General Data Protection Regulation (GDPR), which has shaped legal reforms in several Southeast Asian countries while simultaneously raising concerns regarding legal transplantation and compatibility with local socio-legal conditions (Azhari et al., 2025). The need to balance economic integration, state sovereignty, technological innovation, and human rights protection creates a complex regulatory environment requiring multidimensional legal approaches. Moreover, the increasing integration of digital technologies into healthcare systems, financial services, and public administration has intensified demands for stronger accountability and privacy safeguards (Anshari et al., 2024; Amirulloh et al., 2025). Accordingly, legal harmonization should be understood not merely as regulatory alignment, but as a broader effort to establish legal certainty, institutional trust, and sustainable digital governance within ASEAN.

Although previous studies have discussed digital governance, cybersecurity, and data protection in Southeast Asia, most of them remain sectoral and nationally oriented. Limited scholarship comprehensively examines how ASEAN countries can harmonize digital privacy regulation while simultaneously addressing cross-border data governance, technological disruption, and institutional disparities at the regional level. This gap demonstrates the need for a broader comparative legal analysis capable of explaining both the structural obstacles and potential institutional strategies for strengthening regional digital privacy governance.

Based on these developments, this study examines the challenges and efforts toward the harmonization of digital privacy and personal data protection laws in Southeast Asia. This study specifically aims to: (1) identify the principal legal and institutional challenges hindering the harmonization of digital privacy and personal data protection laws in Southeast Asia; and (2) analyze the legal and institutional efforts capable of strengthening regional cooperation and improving the effectiveness of digital privacy governance within ASEAN. Unlike previous studies that primarily focus on sector-specific digital regulation or individual national frameworks, the novelty of this research lies in its multidimensional comparative approach integrating discussions on cybersecurity, cross-border data governance, digital trade, and emerging technologies within the broader framework of ASEAN legal harmonization. Accordingly, this study seeks to answer the following research questions: (1) What are the principal challenges facing the harmonization of digital privacy and personal data protection laws in Southeast Asia? and (2) What legal and institutional efforts can strengthen regional cooperation and improve the effectiveness of digital privacy governance in the region?

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

Although this study provides a broader regional legal analysis, it is limited by its normative and doctrinal approach, which relies primarily on legal documents, regulations, and secondary scholarly sources without empirical field investigation. Through this analysis, the study aims to contribute to the development of more adaptive, collaborative, and rights-oriented legal frameworks capable of addressing the complexities of digital transformation in Southeast Asia.

2. Literature Review

The discourse on digital privacy and personal data protection has expanded significantly alongside the rapid growth of the digital economy and technological innovation in Southeast Asia. Existing studies generally argue that digital transformation creates both economic opportunities and regulatory challenges, particularly concerning data governance, cybersecurity, cross-border digital transactions, and legal accountability. Abdurrahman (2025) explains that the development of Indonesia's digital economy is strongly influenced by institutional readiness, digital culture, and technological infrastructure, indicating that digital governance cannot be separated from legal adaptation. Similarly, Anshari et al. (2024) and Yi et al. (2024) demonstrate that digital transformation in healthcare systems across ASEAN countries increases dependence on digital infrastructures processing sensitive personal data. These developments intensify the need for comprehensive legal frameworks capable of balancing innovation, economic growth, and individual privacy rights. Consequently, digital governance and legal harmonization theories have become important analytical foundations in examining the evolution of data protection regulation in Southeast Asia.

The theoretical foundation of this study is primarily based on the concepts of legal harmonization and adaptive digital governance. Legal harmonization refers to efforts to reduce inconsistencies among national legal systems in order to establish compatible regulatory standards while respecting state sovereignty and socio-legal diversity. Azhari et al. (2025) describe this process through the concept of legal isomorphism, where states adopt foreign legal models while simultaneously adapting them to domestic legal traditions and institutional conditions. Within Southeast Asia, the influence of international regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) has encouraged ASEAN member states to modernize personal data protection laws, although implementation remains uneven (Dolzhenko, 2025). In addition, adaptive governance theory emphasizes regulatory flexibility, institutional responsiveness, and policy coordination in addressing technological disruption**.** Xiao (2025) argues that agile governance models are necessary to regulate emerging technologies such as artificial intelligence, while Balarabe (2025) emphasizes that cybersecurity governance increasingly intersects with issues of sovereignty, digital borders, and transnational regulation. Therefore, digital privacy harmonization cannot merely focus on formal legal similarity, but must also incorporate institutional cooperation, technological adaptability, and regional governance capacity.

Several studies have examined the relationship between emerging technologies and digital privacy protection. Lim et al. (2025) discuss the growing use of biometric technologies in Southeast Asia and identify concerns regarding surveillance, consent, data misuse, and regulatory fragmentation. Likewise, Liébana-Cabanillas et al. (2025) demonstrate that biometric payment systems simultaneously increase transactional efficiency and privacy risks

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

because biometric information constitutes highly sensitive personal data. Research concerning artificial intelligence further reveals legal and ethical risks related to algorithmic discrimination and automated decision-making. Borba et al. (2024) argue that AI systems may generate discriminatory outcomes when transparency and accountability mechanisms remain inadequate. Praja et al. (2025) additionally highlight unresolved issues regarding ownership and authorship of AI-generated works, reflecting broader debates concerning accountability and digital rights. Cybersecurity scholarship also emphasizes the growing vulnerability of digital infrastructures. Parambil et al. (2024) underline the importance of integrating AI-based and conventional cybersecurity systems, while Senarak (2025) explains that cyber resilience requires coordinated legal and institutional responses to transnational cyber threats. Collectively, these studies indicate that digital privacy governance is increasingly interconnected with cybersecurity regulation, AI governance, and emerging digital technologies.

Existing scholarship further demonstrates that digital privacy issues overlap with consumer protection, digital transactions, judicial reform, and international economic governance. Panjaitan et al. (2025) explain that click-wrap agreements and platform contracts often create unequal bargaining positions between corporations and consumers, thereby requiring stronger legal safeguards in digital commerce. Syahputra et al. (2025) similarly discuss the risks of platform dominance within Indonesia's digital marketplace. Studies concerning judicial digitalization also reveal continuing institutional adaptation challenges. Adinda et al. (2025) identify legal uncertainty regarding the admissibility of electronic evidence, while Mardyansyah et al. (2025) examine the legitimacy of electronic summons within Indonesian procedural law. At the international level, Ma et al. (2024) and Zhang and Gao (2025) argue that cross-border data flow regulation increasingly affects digital trade and global economic integration. These studies collectively demonstrate that digital privacy governance has evolved into an interdisciplinary legal issue extending beyond traditional data protection frameworks.

Despite the growing body of literature, several important gaps remain insufficiently explored. First, most existing studies focus on sector-specific issues such as AI governance, cybersecurity, healthcare technology, or digital trade without comprehensively examining their interaction within broader regional harmonization efforts. Second, prior scholarship predominantly analyzes individual national legal frameworks rather than comparatively assessing ASEAN as an interconnected digital governance region. Third, limited research specifically evaluates the relationship between legal harmonization, institutional capacity, and regional cooperation mechanisms in Southeast Asia. This study addresses those gaps by integrating discussions on digital privacy, cybersecurity, cross-border data governance, digital trade, consumer protection, and emerging technologies into a comparative ASEAN legal analysis. The novelty of this research lies in its multidimensional and regional approach, which combines legal harmonization theory and adaptive governance perspectives to evaluate both the obstacles and opportunities for developing coherent personal data protection standards in Southeast Asia. Through this approach, the study contributes to contemporary legal scholarship by providing a broader analytical framework for understanding regional digital privacy governance amid ongoing technological transformation.

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

3. Methodology

This study employs a normative juridical legal research method to examine the harmonization of digital privacy and personal data protection laws in Southeast Asia within the broader context of digital governance, cybersecurity, and cross-border data regulation. Normative legal research focuses on the analysis of legal norms, statutory regulations, legal principles, doctrines, and scholarly interpretations related to the issues discussed in this study. This method is considered appropriate because the research primarily evaluates the adequacy, consistency, and harmonization of legal frameworks governing digital privacy across ASEAN member states. The study applies several complementary approaches, namely the statutory approach, conceptual approach, comparative approach, and analytical approach. The statutory approach is used to examine laws and regulations concerning personal data protection, digital transactions, cybersecurity, consumer protection, electronic evidence, and artificial intelligence governance in several Southeast Asian countries, particularly Indonesia, Singapore, Malaysia, Thailand, and the Philippines. The analysis also incorporates ASEAN regional frameworks and international legal instruments, including the European Union's General Data Protection Regulation (GDPR), in order to assess the extent of regional regulatory convergence and divergence. Relevant legal developments concerning electronic evidence, digital procedural systems, and data governance are examined through recent scholarly discussions presented by Adinda et al. (2025), Mardyansyah et al. (2025), Amirulloh et al. (2025), Panjaitan et al. (2025), and Syahputra et al. (2025).

The conceptual approach is employed to analyze theoretical perspectives concerning legal harmonization, adaptive governance, digital sovereignty, cybersecurity resilience, and algorithmic regulation. This approach enables the study to identify the legal principles and governance concepts underlying contemporary digital regulation in Southeast Asia. The research draws upon the theories of legal isomorphism and regulatory adaptation discussed by Azhari et al. (2025), cybersecurity sovereignty proposed by Balarabe (2025), agile governance models examined by Xiao (2025), and cross-border data governance frameworks analyzed by Zhang and Gao (2025). These theoretical perspectives are important for explaining how ASEAN countries attempt to balance technological innovation, state sovereignty, regional cooperation, and privacy protection within rapidly evolving digital environments. The comparative approach is further utilized to compare regulatory frameworks and institutional practices among ASEAN member states. Comparative analysis is necessary because issues concerning digital privacy, biometric governance, artificial intelligence, and cross-border data flows are inherently transnational and cannot be adequately understood solely through a single national legal perspective. Accordingly, this study refers to comparative findings presented by Lim et al. (2025), Dolzhenko (2025), and Anshari et al. (2024) to identify similarities, differences, and governance gaps among Southeast Asian jurisdictions.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include statutory regulations, ASEAN policy frameworks, government regulations, and international legal instruments related to digital governance and personal data protection. Secondary legal materials include journal articles, academic books, conference proceedings, and scientific publications relevant to the research topic, particularly studies published between 2024 and 2025. Tertiary legal materials include legal dictionaries,

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

encyclopedias, and supporting digital databases. Data collection is conducted through library research and document analysis, while the collected legal materials are analyzed qualitatively using descriptive-analytical techniques to identify regulatory inconsistencies, institutional barriers, and opportunities for strengthening regional digital privacy harmonization in Southeast Asia. The novelty of this methodological approach lies in its integration of comparative ASEAN legal analysis with adaptive governance and digital harmonization perspectives, enabling a broader evaluation of regional privacy governance beyond sector-specific studies. Nevertheless, this study is limited by its doctrinal and desk-based nature because it relies primarily on legal documents and secondary scholarly sources without empirical interviews or field-based institutional assessment. Consequently, the findings mainly reflect normative legal analysis rather than empirical measurement of regulatory implementation effectiveness across ASEAN member states.

4. Results & Discussion

4.1. Indonesia's Digital Governance Transformation

Indonesia's digital governance transformation reflects the state's attempt to adapt legal and institutional frameworks to rapid technological change and regional digital economic integration. The expansion of e-commerce, fintech services, artificial intelligence (AI), electronic courts, and digital public administration has significantly altered the relationship between the state, market actors, and society. This transformation demonstrates that digital governance is no longer limited to technological modernization, but has evolved into a multidimensional legal governance issue involving cybersecurity, data protection, regulatory coordination, and institutional accountability. Indonesia's digital economy growth is strongly influenced by institutional readiness, digital infrastructure, innovation ecosystems, and regulatory effectiveness (Abdurrahman, 2025). At the same time, ASEAN countries continue to experience uneven regulatory development concerning personal data protection and digital governance harmonization (Dolzhenko, 2025). Consequently, Indonesia faces the dual challenge of accelerating digital innovation while simultaneously ensuring legal certainty, public trust, and regional interoperability within Southeast Asia's increasingly interconnected digital environment.

The transformation of Indonesia's digital ecosystem has generated important opportunities alongside substantial governance risks. The growth of digital platforms and fintech systems has expanded financial inclusion and commercial efficiency, yet it has also intensified concerns regarding monopolistic practices, biometric surveillance, cybersecurity vulnerabilities, and algorithmic discrimination. Syahputra et al. (2025) explain that dominant digital platforms may create unfair competition structures capable of weakening consumer protection and market equality. Similarly, Lim et al. (2025) emphasize that Southeast Asian countries still possess fragmented biometric data governance standards, creating legal uncertainty regarding privacy protection and institutional enforcement. AI technologies additionally create regulatory challenges concerning accountability and discriminatory decision-making processes (Borba et al., 2024). In the judicial sector, electronic evidence and digital court systems have improved procedural efficiency but continue to face doctrinal and evidentiary limitations (Adinda et al., 2025; Mardyansyah et al., 2025). These developments indicate that Indonesia's digital governance framework remains institutionally adaptive but legally fragmented, particularly

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

regarding coordination between data protection, cybersecurity, consumer protection, and AI governance mechanisms. The findings therefore confirm that technological transformation has progressed more rapidly than the harmonization of legal and institutional safeguards.

From a broader ASEAN perspective, Indonesia's digital governance transformation illustrates the wider regional challenge of balancing innovation, sovereignty, and legal protection within evolving digital economies. Countries such as Singapore have developed more integrated personal data protection and AI governance systems, while Indonesia continues to rely on sectoral and incremental regulatory reforms (Lim et al., 2025). Cross-border data flows, digital trade expansion, and cybersecurity threats further complicate regional harmonization efforts because ASEAN member states maintain different legal traditions, institutional capacities, and regulatory priorities (Zhang & Gao, 2025; Ma et al., 2024). Accordingly, Indonesia's experience demonstrates that future digital governance effectiveness depends not only on regulatory expansion, but also on the establishment of adaptive and coordinated governance mechanisms capable of integrating cybersecurity resilience, personal data protection, judicial modernization, and digital economic regulation. This finding directly answers the study's first research question by showing that the principal challenge of digital privacy harmonization in Southeast Asia lies in fragmented institutional structures, inconsistent enforcement capacity, and differing national regulatory approaches toward emerging digital technologies.

Table 1. Major Dimensions of Indonesia's Digital Governance Transformation

Dimension	Digital Development	Legal and Governance Implications
Digital Economy	Expansion of e-commerce and platform businesses	Competition law and consumer protection challenges
E-Government	Online public services and digital administration	Transparency, efficiency, and procedural legality
Judicial Digitalization	Electronic summons and digital evidence	Evidentiary harmonization and access to justice
Financial Technology	Biometric payments and fintech services	Data privacy and cybersecurity protection
Artificial Intelligence	Automated systems and AI-generated content	Accountability, bias, and intellectual property issues

Source: Author's analysis, 2024.

4.2. Cybersecurity, Data Protection, and AI Regulation Challenges

Indonesia's rapid digital transformation has intensified cybersecurity vulnerabilities, data protection concerns, and artificial intelligence (AI) governance challenges. The expansion of e-government systems, fintech platforms, electronic commerce, cloud computing, and AI-based services has increased the dependency of state institutions, businesses, and citizens on interconnected digital infrastructures. This condition demonstrates that cybersecurity is no longer merely a technical issue, but also a legal and governance concern closely related to digital sovereignty, institutional legitimacy, and public trust**.** Balarabe (2025) explains that cybersecurity governance increasingly intersects with international law and state sovereignty in the digital era. In Indonesia, cybersecurity risks are amplified by fragmented institutional coordination, uneven technological readiness, and overlapping regulatory authority. The growing use of electronic evidence and digital court systems further illustrates these challenges. Adinda et al. (2025) note that electronic evidence admissibility in Indonesian procedural law still faces weaknesses regarding authentication and verification standards, while Mardyansyah

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

et al. (2025) emphasize that electronic summons systems require clearer legal safeguards and procedural certainty. These findings indicate that Indonesia's digital governance framework remains reactive and sectoral, limiting the effectiveness of cybersecurity protection and digital legal enforcement.

The protection of personal and biometric data has also become a major regulatory challenge within Indonesia's digital governance system. The increasing use of biometric verification, digital banking, online healthcare services, and AI-driven platforms has significantly expanded the collection and processing of sensitive personal information. Liébana-Cabanillas et al. (2025) explain that biometric payment systems improve efficiency and convenience but simultaneously create serious privacy risks because compromised biometric data cannot easily be replaced. Similarly, Lim et al. (2025) argue that Southeast Asian countries continue to face fragmented biometric governance frameworks and inconsistent privacy protection standards. Indonesia has attempted to strengthen legal protection through the enactment of the Personal Data Protection Law; however, implementation remains constrained by institutional fragmentation and weak supervisory mechanisms (Amirulloh et al., 2025). Cross-border digital transactions further complicate data governance because global digital platforms facilitate the continuous transfer of personal and commercial data across jurisdictions. Ma et al. (2024) demonstrate that restrictions on cross-border data flows may affect digital trade competitiveness, while Zhang and Gao (2025) identify increasing tensions between economic openness and digital sovereignty in global data governance. Consequently, Indonesia faces a dual challenge of encouraging digital economic growth while simultaneously protecting national sovereignty, privacy rights, and cybersecurity resilience within transnational digital ecosystems.

Artificial intelligence regulation represents another important challenge in Indonesia's digital governance transformation. AI technologies are increasingly utilized in digital commerce, financial systems, public administration, education, and automated decision-making processes. Nevertheless, AI development also generates legal concerns involving algorithmic bias, accountability, discrimination, and market dominance. Borba et al. (2024) explain that algorithmic systems may produce discriminatory outcomes due to biased datasets and opaque decision-making mechanisms, while Herani (2025) emphasizes that algorithmic governance may distort fair competition within digital marketplaces if effective regulatory supervision is absent. Indonesia additionally faces uncertainty regarding cryptocurrency and digital asset regulation because legal frameworks remain fragmented across financial, technological, and cybersecurity sectors (AlQudah & Bariviera, 2025). Xiao (2025) therefore argues that adaptive and iterative governance models are necessary to address rapidly evolving technological risks. These developments indicate that Indonesia requires a more integrated governance framework capable of harmonizing cybersecurity protection, AI accountability, cross-border data governance, and digital financial supervision to ensure legal certainty and sustainable digital governance.

Table 2. Major Regulatory Challenges in Indonesia's Digital Governance

Regulatory Area	Key Challenges	Governance Implications
Cybersecurity	Cyberattacks and digital infrastructure vulnerabilities	Institutional resilience and national security

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

Regulatory Area	Key Challenges	Governance Implications
Personal Data Protection	Weak harmonization of biometric and personal data regulation	Privacy and citizen protection
Artificial Intelligence	Algorithmic bias and opaque decision-making	Accountability and fairness
Cross-Border Data Flow	Jurisdictional conflicts and digital sovereignty	International regulatory coordination
Cryptocurrency and Fintech	Regulatory fragmentation and financial risks	Consumer trust and market stability

Source: Author's analysis, 2024.

4.3. Comparative ASEAN Digital Governance Perspectives

The development of digital governance in Indonesia must be understood within the broader context of ASEAN's rapidly expanding digital economy. Southeast Asia has emerged as one of the world's fastest-growing digital regions, driven by the expansion of e-commerce, fintech services, artificial intelligence, and digital public administration. Nevertheless, ASEAN member states demonstrate different levels of legal readiness, institutional capacity, and regulatory effectiveness in responding to technological transformation. This variation indicates that digital governance in ASEAN is shaped not only by technological development, but also by constitutional structures, political priorities, and institutional capabilities within each jurisdiction. Dolzhenko (2025) explains that Southeast Asian countries continue to adopt diverse approaches toward personal data protection and digital governance due to differences in national legal systems and policy priorities. Singapore represents one of the most advanced governance models in ASEAN, particularly in data protection, cybersecurity, and AI regulation. Through the Personal Data Protection Act (PDPA), Singapore has established relatively comprehensive legal safeguards supported by strong institutional oversight and regulatory coordination. Lim et al. (2025) further note that Singapore's biometric governance framework successfully combines technological innovation with accountability and privacy protection. In contrast, Indonesia's digital governance framework remains more fragmented because regulatory authority is distributed across multiple institutions and sectoral regulations. Although Indonesia has enacted the Personal Data Protection Law, implementation challenges persist due to overlapping authority and uneven institutional readiness (Amirulloh et al., 2025). These comparisons demonstrate that effective digital governance depends not solely on legislative enactment, but also on institutional coordination, enforcement consistency, and administrative capacity.

Comparative perspectives from Vietnam, Malaysia, and Thailand further illustrate ASEAN's diverse regulatory trajectories in managing digital transformation. Vietnam adopts a more state-centered governance approach emphasizing digital sovereignty, cybersecurity supervision, and data localization requirements for foreign digital platforms. Zhang and Gao (2025) explain that many Asian countries increasingly regard data governance as a strategic sovereignty issue rather than merely an economic or technical concern. Indonesia shares similar concerns regarding platform accountability and national control over digital infrastructures; however, Indonesia tends to apply a more adaptive and hybrid regulatory approach balancing economic openness with regulatory supervision (Ma et al., 2024). Malaysia provides another important comparison in relation to whistleblower protection, fintech supervision, and institutional accountability. Hosnah et al. (2025) argue that Malaysia possesses relatively stronger mechanisms for protecting public-interest disclosures within digital governance systems, while

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

Indonesia still experiences regulatory uncertainty concerning cybersecurity reporting and institutional transparency. Similar issues appear within digital financial governance, where fragmented cryptocurrency and fintech regulation creates legal uncertainty regarding consumer protection and cybersecurity supervision (AlQudah & Bariviera, 2025). Thailand and Indonesia also face comparable challenges involving digital market dominance, institutional fragmentation, and regulatory adaptation. Haliwela and Chansrakaeo (2025) explain that digital governance reforms in both countries increasingly intersect with sustainability and corporate governance concerns. Syahputra et al. (2025) further demonstrate that Indonesia's competition law framework still struggles to address monopolistic tendencies within digital marketplaces effectively. These ASEAN comparisons indicate that developing digital economies commonly encounter structural problems involving fragmented governance, limited enforcement capacity, and technological asymmetry.

ASEAN comparative analysis additionally reveals common regional concerns regarding cybersecurity resilience and judicial digitalization. Cybersecurity governance has become increasingly important because digital public services, fintech systems, and e-government platforms remain vulnerable to cyber threats and transnational cybercrime. Balarabe (2025) argues that cybersecurity governance now intersects closely with sovereignty, digital borders, and international legal cooperation, while Senarak (2025) emphasizes the importance of integrated prevention, response, and recovery mechanisms for cyber resilience. Indonesia faces similar challenges because institutional coordination and cybersecurity readiness remain uneven across sectors. In the judicial sector, ASEAN countries also demonstrate varying levels of digital legal modernization. Indonesia has implemented e-court systems and electronic summons as part of broader judicial digitalization reforms aimed at improving procedural efficiency and public access to justice (Mardyansyah et al., 2025). However, legal uncertainty concerning electronic evidence admissibility and digital procedural safeguards continues to create implementation challenges (Adinda et al., 2025). Singapore and Malaysia possess more mature judicial technology systems with stronger procedural integration and institutional support, whereas Indonesia remains in a transitional adaptation phase. Nasrullah et al. (2025) explain that successful judicial digitalization requires not only technological infrastructure but also legal certainty, administrative integrity, and institutional trust. Overall, comparative ASEAN analysis demonstrates that Indonesia's digital governance model reflects a hybrid and adaptive approach, yet future governance effectiveness will depend on stronger institutional harmonization, cybersecurity coordination, and integrated regional digital cooperation.

4.4. Theoretical Interpretation and Adaptive Governance Analysis

The findings of this study demonstrate that Indonesia's digital governance transformation cannot be adequately interpreted through conventional legal positivism alone because digital regulation develops through dynamic interactions among technology, institutions, markets, and transnational governance influences. The rapid expansion of fintech systems, electronic commerce, AI-based technologies, digital public administration, and cross-border data flows has created a regulatory environment characterized by uncertainty, complexity, and institutional adaptation. Accordingly, this study applies an adaptive governance perspective to explain how Indonesian legal institutions respond to technological disruption through flexible and incremental regulatory adjustments rather than rigid legislative codification**.** Adaptive

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

governance theory emphasizes institutional learning, policy responsiveness, collaborative regulation, and legal flexibility in addressing rapidly evolving technological conditions. Xiao (2025) argues that agile and iterative governance approaches are increasingly necessary because static legal frameworks cannot adequately respond to the speed of AI development and digital innovation. Indonesia reflects this adaptive pattern through the gradual evolution of regulations concerning electronic evidence, digital consumer protection, cybersecurity, and fintech supervision (Adinda et al., 2025; Panjaitan et al., 2025). Rather than adopting a single comprehensive digital governance code, Indonesia continues to develop sectoral regulations responding to emerging technological risks and policy demands. This fragmented but adaptive regulatory model demonstrates the state's attempt to balance technological innovation with legal certainty and governance flexibility.

From a theoretical perspective, Indonesia's digital governance transformation also illustrates the operation of legal isomorphism within contemporary regulatory development. Azhari et al. (2025) explain that Indonesian legal reform frequently adopts external legal principles while simultaneously adapting them to domestic constitutional identity and socio-political conditions. This phenomenon is visible in Indonesia's adoption of international standards concerning data protection, AI governance, cybersecurity regulation, and digital trade supervision. Nevertheless, Indonesia does not completely replicate foreign regulatory models because legal adaptation remains influenced by domestic political priorities, economic interests, and institutional capacity. The enactment of the Personal Data Protection Law, for example, reflects global data governance influences while remaining shaped by Indonesia's constitutional structure and administrative framework. Balarabe (2025) further argues that digital governance increasingly intersects with cybersecurity, sovereignty, economic policy, and international law, thereby requiring multidimensional institutional involvement. Consequently, Indonesia distributes regulatory authority across various institutions, including Kominfo, OJK, Bank Indonesia, BSSN, and judicial bodies. Although this decentralized structure allows adaptive responses to technological complexity, overlapping authority and inconsistent coordination continue to weaken enforcement effectiveness. The adaptive governance framework therefore explains both the strengths and limitations of Indonesia's pluralistic digital governance system, particularly its ability to accommodate innovation while struggling to maintain institutional coherence and regulatory integration.

The theoretical interpretation additionally highlights the importance of regulatory balancing and institutional legitimacy within Indonesia's digital governance transformation. Herani (2025) explains that effective digital governance requires balancing innovation promotion with safeguards against algorithmic bias, consumer vulnerability, market dominance, and cybersecurity risks. Indonesia's digital governance framework consistently reflects this dual orientation. On one hand, the government actively promotes fintech expansion, digital trade, and AI-driven economic modernization as instruments of national development (Abdurrahman, 2025). On the other hand, increasing concerns regarding privacy violations, discriminatory algorithms, cybersecurity threats, and monopolistic digital platforms require stronger legal intervention and accountability mechanisms. Borba et al. (2024) explain that algorithmic systems may produce discriminatory outcomes when transparency and oversight mechanisms remain weak, while Lim et al. (2025) emphasize that biometric governance requires stronger

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

legal safeguards to maintain public trust and prevent misuse of sensitive personal data. Similar adaptive challenges appear in judicial digitalization reforms. Mardyansyah et al. (2025) and Nasrullah et al. (2025) argue that electronic courts and digital procedural systems require continuous institutional learning, technological accountability, and procedural harmonization to preserve access to justice and legal legitimacy. Furthermore, Indonesia's adaptive governance model remains strongly influenced by developmental state priorities emphasizing economic competitiveness, financial inclusion, and administrative modernization (Keumala et al., 2025). Overall, the study confirms that Indonesia's digital governance transformation reflects an evolving adaptive governance model characterized by regulatory flexibility, selective legal convergence, institutional pluralism, and developmental policy orientation, although future effectiveness will depend on stronger coordination mechanisms and more coherent regulatory integration.

4.5. Legal Reform and Future Digital Governance Framework

Indonesia's rapid digital transformation demonstrates the urgent need for comprehensive and integrated legal reform capable of addressing the intersection between technological innovation, economic development, cybersecurity, and protection of fundamental rights. The findings of this study indicate that Indonesia has made important progress through the enactment of the Personal Data Protection Law, expansion of fintech supervision, judicial digitalization, and electronic governance systems. Nevertheless, significant challenges remain regarding institutional fragmentation, overlapping regulatory authority, inconsistent enforcement, and limited technological readiness. These conditions confirm that Indonesia's current digital governance framework remains sectoral and insufficiently coordinated to address increasingly complex digital risks within the ASEAN digital ecosystem. Abdurrahman (2025) explains that digital economic development is highly dependent on institutional readiness and governance effectiveness, while Balarabe (2025) emphasizes that cybersecurity governance increasingly intersects with sovereignty and international legal coordination. Furthermore, Lim et al. (2025) demonstrate that Southeast Asian countries continue to face major regulatory inconsistencies regarding biometric governance and personal data protection. Accordingly, future legal reform should focus not only on regulatory expansion but also on institutional harmonization capable of integrating cybersecurity governance, data protection, digital trade regulation, and artificial intelligence supervision within a coherent adaptive governance framework.

One of the primary priorities of future reform concerns cybersecurity resilience, personal data protection, and artificial intelligence governance. Indonesia's expanding digital economy has significantly increased the circulation of personal, financial, and biometric data across public institutions and digital platforms, thereby intensifying risks involving cyberattacks, data misuse, and algorithmic discrimination. Amirulloh et al. (2025) note that institutional readiness in implementing privacy protection mechanisms remains limited, while Senarak (2025) argues that effective cyber resilience requires coordinated legal, technological, and institutional responses. In the field of artificial intelligence, Borba et al. (2024) identify that algorithmic systems may generate discriminatory outcomes when transparency and accountability mechanisms remain weak. Similarly, Praja et al. (2025) highlight unresolved legal questions concerning AI-generated works and intellectual property ownership. These findings indicate

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

that Indonesia still lacks comprehensive AI-specific regulation capable of balancing technological innovation with ethical safeguards and human rights protection. Comparative experiences from ASEAN and China further demonstrate the importance of adaptive and iterative governance models in responding to technological disruption (Xiao, 2025). Therefore, Indonesia should establish an integrated digital governance strategy emphasizing centralized data protection supervision, AI accountability standards, cybersecurity coordination, and cross-sector institutional cooperation. Such reforms are necessary to strengthen public trust, regulatory certainty, and long-term digital governance sustainability.

In addition to domestic reform, Indonesia's future digital governance framework must also strengthen regional cooperation and institutional integration within ASEAN. Cross-border data flows, digital trade, fintech expansion, and transnational cyber threats increasingly require interoperable regional governance mechanisms. Dolzhenko (2025) explains that ASEAN countries are gradually converging toward more comprehensive data governance systems despite differing implementation capacities and national legal priorities. Panjaitan et al. (2025) further emphasize the need for stronger consumer protection within digital transactions, while Syahputra et al. (2025) demonstrate that platform dominance and monopolistic practices continue to challenge market fairness in digital economies. Judicial digitalization similarly requires procedural harmonization and cybersecurity safeguards to maintain legal certainty and public trust (Adinda et al., 2025; Mardyansyah et al., 2025). Therefore, future legal reform should adopt an integrated adaptive governance model combining institutional coordination, regional cooperation, technological responsiveness, and continuous policy evaluation.

Table 3 summarizes the key areas of future legal reform identified in this study.

Legal Reform Area	Main Challenges	Recommended Future Framework
Data Protection	Fragmented supervision and weak enforcement	Independent data protection authority
Cybersecurity	Sectoral coordination weaknesses	Integrated national cybersecurity framework
Artificial Intelligence	Regulatory vacuum and ethical risks	Adaptive AI governance regulation
Digital Economy	Platform dominance and consumer vulnerability	Integrated platform governance
Judicial Digitalization	Procedural uncertainty and cybersecurity concerns	Harmonized digital procedural law
ASEAN Cooperation	Cross-border governance inconsistency	Regional digital governance collaboration

Source: Researcher's analysis, 2024.

Overall, the future effectiveness of Indonesia's digital governance depends on the ability of legal institutions to construct coherent, adaptive, and collaborative governance systems capable of balancing innovation, sovereignty, accountability, economic competitiveness, and protection of digital rights within the evolving regional digital environment.

5. Conclusion

This study demonstrates that the harmonization of digital privacy and personal data protection laws in Southeast Asia remains constrained by regulatory fragmentation, uneven institutional capacity, differing national legal priorities, and inconsistent enforcement mechanisms across

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

ASEAN countries. The findings show that rapid digital transformation, cross-border data flows, artificial intelligence adoption, and expanding digital economic activities have intensified the urgency of establishing coherent and adaptive digital governance frameworks within the region. In answering the first research question, this study finds that the principal challenges of harmonization include disparities in legal definitions, weak cybersecurity coordination, limited supervisory institutions, data sovereignty concerns, and regulatory incompatibility among ASEAN member states. In answering the second research question, the study identifies that stronger regional cooperation, institutional coordination, adaptive legal reform, and interoperability of digital governance standards are necessary to strengthen personal data protection and improve regional digital governance effectiveness in Southeast Asia.

This study further argues that ASEAN digital governance should move beyond fragmented sectoral regulation toward a more integrated adaptive governance model capable of balancing innovation, economic development, legal certainty, cybersecurity resilience, and human rights protection. The novelty of this research lies in its multidimensional comparative approach integrating digital privacy, cybersecurity, artificial intelligence governance, cross-border data governance, consumer protection, and regional legal harmonization within a unified Southeast Asian legal analysis. Unlike previous studies that predominantly focus on single-country frameworks or sector-specific regulation, this study contributes a broader regional perspective by combining legal harmonization theory and adaptive governance analysis to evaluate both regulatory challenges and future governance opportunities within ASEAN digital transformation. Accordingly, this research contributes both theoretically to the development of digital governance scholarship and practically to policy formulation concerning regional regulatory coordination and institutional reform in Southeast Asia.

Nevertheless, this study has several limitations. First, the research adopts a normative juridical and doctrinal approach relying primarily on statutory regulations, policy documents, and secondary literature without empirical field investigation or stakeholder interviews. Second, the comparative analysis focuses mainly on selected ASEAN countries and therefore may not fully represent all legal and institutional variations across Southeast Asia. Third, the rapid evolution of digital technologies and regulatory policies may significantly alter future governance dynamics and legal developments. Accordingly, future research should incorporate empirical methods, interdisciplinary perspectives, and broader comparative analysis involving governmental institutions, private sector actors, and regional organizations to strengthen understanding of digital governance harmonization within ASEAN.

Acknowledgments

The authors would like to express sincere gratitude to colleagues and academic partners who provided valuable insights and constructive feedback throughout the preparation of this article. Appreciation is also extended to the affiliated institutions for their academic support in facilitating this research on digital governance and legal transformation in Indonesia. The authors acknowledge all scholars whose works contributed significantly to the theoretical and comparative perspectives developed in this study.

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

References

Abdurrahman, A. (2025). Extending the IBCDE framework to explore barriers and drivers in Indonesia's digital economy. *Journal of Digital Economy*, *4*, 123–143. https://doi.org/10.1016/j.jdec.2025.08.003

Adinda, F. A., Rahmawati, E., Suparman, E., Arifin, R., & Ezzerouali, S. (2025). The Challenge of Admitting Electronic Evidence in Civil Procedure Law. *Jurnal IUS Kajian Hukum Dan Keadilan*, *13*(3), 656–680. https://doi.org/10.29303/ius.v13i3.1873

AlQudah, M. Z., & Bariviera, A. F. (2025). Systematic and bibliometric reviews of cryptocurrency market regulation: Trends, influential contributions, and future directions. *Journal of Financial Regulation and Compliance*, *34*(1), 1–37. https://doi.org/10.1108/JFRC-11-2024-0232

Amirulloh, M., Suparman, E., Muchtar, H. N., & Hasanah, H. (2025). Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification. *Jurnal IUS Kajian Hukum dan Keadilan*, *13*(3), 545–558. https://doi.org/10.29303/ius.v13i3.1777

Anshari, M., de Pablos, P. O., & Almunawar, M. N. (2024). Chapter 10—Digital health in ASEAN an exploratory analysis. In P. O. de Pablos (Ed.), *Digital Healthcare in Asia and Gulf Region for Healthy Aging and More Inclusive Societies* (Vol. 4, pp. 169–198). Academic Press. https://doi.org/10.1016/B978-0-443-23637-2.00021-7

Azhari, A. F., Rizka, R., Setiawati, D., Almira, S. D. A., & Salmande, A. (2025). The Legal Isomorphism in Indonesian Constitutional Amendment: Interplay Between Foreign Influence and National Identity. *Jurnal Hukum*, *41*(4), 842–860. https://doi.org/10.26532/jh.v41i4.44109

Balarabe, K. (2025). Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. *Computer Law & Security Review*, *58*, 106180. https://doi.org/10.1016/j.clsr.2025.106180

Borba, R. L., de Paula Ferreira, I. E., & Bertucci Ramos, P. H. (2024). Addressing discriminatory bias in artificial intelligence systems operated by companies: An analysis of end-user perspectives. *Technovation*, *138*, 103118. https://doi.org/10.1016/j.technovation.2024.103118

Dolzhenko, N. (2025, June 17). *Navigating Southeast Asia's evolving data protection laws: Insights from Singapore, Indonesia, Vietnam & Thailand*. InCountry. https://incountry.com/blog/navigating-southeast-asias-evolving-data-protection-laws-insights-from-singapore-indonesia-vietnam-thailand/

Haliwela, N. S., & Chansrakaeo, R. (2025). The Corporate Social Responsibility Regulation in the Development of Business Law: Comparison of Indonesia and Thailand. *Jurnal Hukum Bisnis Bonum Commune*, 194–212. https://doi.org/10.30996/jhbbc.v8i1.12853

Heniarti, D. D., & Setiadi, E. (2025). Effectiveness of Countering Acts of Terrorism Within Asean: Challenges and the Path Forward. *Jurnal Hukum*, *41*(3), 548–566. https://doi.org/10.26532/jh.v41i3.37061

Herani, R. (2025). Should we play an unfair game? The roles of regulatory effectiveness, government support and algorithmic bias in e-commerce entrepreneurial readiness.

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

Journal of Entrepreneurship in Emerging Economies, *18*(1), 237–265. https://doi.org/10.1108/JEEE-02-2025-0103

Hosnah, A. ul, Ghapa, N. binti, Nuraeny, H., Putro, S. H. D., & Prihatini, L. (2025). Comparison of Malaysian and Indonesian Whistleblower Legal Protection as a Tool for Criminalization Elimination. *Jurnal Media Hukum*, *32*(1), 114–133. https://doi.org/10.18196/jmh.v32i1.24751

Keumala, D., Sabirin, A., Setiyono, S., Az, M. F., & Arranchado, J. R. (2025). Indonesia's Sustainable Green Economy Policy in the Energy Sector: Challenges and Expectations. *Jurnal Media Hukum*, *32*(1), 1–20. https://doi.org/10.18196/jmh.v32i1.24109

Kurniawan, I. G. A., Samsithawrati, P. A., Disantara, F. P., Thuong, M. T. H., & Nutakor, B. S. M. (2025). The Philosophical Approach to the Existence of Business Law: Comparison of Indonesia, Vietnam, and Ghana. *Jurnal Hukum Bisnis Bonum Commune*, 55–76. https://doi.org/10.30996/jhbbc.v8i1.12382

Liébana-Cabanillas, F., Abbasi, G. A., Higueras-Castillo, E., & Wagner, R. (2025). Press to pay: The power of biometrics in financial transactions investigated by PLS-SEM, fsQCA, and NCA. *Technological Forecasting and Social Change*, *221*, 124365. https://doi.org/10.1016/j.techfore.2025.124365

Lim, A. C. M., Ng, L. H. X., & Taeihagh, A. (2025). Biometric data landscape in Southeast Asia: Challenges and opportunities for effective regulation. *Computer Law & Security Review*, *56*, 106095. https://doi.org/10.1016/j.clsr.2024.106095

Ma, S., Huang, S., & Wu, P. (2024). Data policy restrictions and cross-border E-commerce: Evidence from China. *Journal of Asian Economics*, *95*, 101826. https://doi.org/10.1016/j.asieco.2024.101826

Mardyansyah, D. N., Sukarmi, S., Kusumaningrum, A., & Widyanti, Y. E. (2025). Legal Validity of Electronic Summons in Indonesia's Civil Procedural Law: A Study of Supreme Court Regulation No. 7 of 2022. *Jurnal Hukum*, *41*(4), 1055–1077. https://doi.org/10.26532/jh.v41i4.45276

Mauludin, N. A., Wahyudi, A., & Ulum, H. (2025). Legal Policy Model of the Red and White Village Cooperative (KDMP): Implementation Factors and Comparative Insights from Brazil, Denmark, and Japan. *Jurnal IUS Kajian Hukum Dan Keadilan*, *13*(3), 682–707. https://doi.org/10.29303/ius.v13i3.1894

Nainggolan, B., Pramono, A. J., & Koos, S. (2025). Legal Protection of Intellectual Property for Digital Works by Utilizing Emerging Technologies. *Jurnal Hukum*, *41*(4), 897–924. https://doi.org/10.26532/jh.v41i4.40811

Nasrullah, Handayani, I. G. A. K. R., Karjoko, L., Susilo, A. B., & Zada, M. Z. Q. (2025). Optimizing the Role of Information and Communications Technology within the State Administrative Court Environment. *Jurnal Media Hukum*, *32*(1), 78–95. https://doi.org/10.18196/jmh.v32i1.25118

Panjaitan, H., Girsang, J., Djanegara, M. S., & Fahim, M. H. K. (2025). Strengthening Consumer Protection in Digital Transactions: A Legal Perspective on Click-Wrap Agreements Under the Consumer Protection Law. *Jurnal Hukum*, *41*(3), 666–693. https://doi.org/10.26532/jh.v41i3.47262

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers*

JUSTITIA NOVA
Indonesian Journal of Modern Law
e-ISSN: 3109-3469
Vol. 1, No. 1, June 2025
https://doi.org/10.5281/zenodo.20450137

and Education: Artificial Intelligence, *7*, 100327. https://doi.org/10.1016/j.caeai.2024.100327

Praja, C. B. E., Riswandi, B. A., Wartini, S., Hakim, H. A., & Espares, G. A. (2025). Authorship and Ownership of AI-Generated Works in Indonesia: A Doctrinal and Comparative Review. *Jurnal Media Hukum*, *32*(1), 151–170. https://doi.org/10.18196/jmh.v32i1.25383

Senarak, C. (2025). Leveraging advanced technologies and strategies for port cyber resilience: Strengthening incident response and recovery. *Transportation Research Interdisciplinary Perspectives*, *34*, 101666. https://doi.org/10.1016/j.trip.2025.101666

Sudiyana, S., & Dare, F. M. (2025). The Legal Capital Market Protection: Justice for Minority Stock Investors. *Jurnal Hukum*, *41*(3), 608–625. https://doi.org/10.26532/jh.v41i3.44218

Sulastri, D., Arifin, F., Susanto, A. F., Huda, U. N., & Nor, M. Z. M. (2025). Institutional Integrity and Challenges in the Indonesian Constitutional Court Institution. *Jurnal Media Hukum*, *32*(1), 40–58. https://doi.org/10.18196/jmh.v32i1.24100

Syahputra, R. D., Latumahina, R. E., & Shrestha, A. K. (2025). Legal Analysis of Shopee's Monopoly Practices concerning Business Competition in Indonesia. *Jurnal Hukum Bisnis Bonum Commune*, 95–107. https://doi.org/10.30996/jhbbc.v8i1.12172

Wahyuntara, J. K., Alzyoud, N. S. A., Almanasra, M., & Nurfatmawati, A. (2025). The Legal System for Professional Discipline of Medical Personnel: Constructing Justice and Dignity. *Jurnal Hukum*, *41*(4), 1037–1054. https://doi.org/10.26532/jh.v41i4.49126

Widiarty, W. S., Park, J., & Putra, T. S. (2025). A Legal Analysis of the Influence of International Trade on Import Restriction Policies in Indonesia. *Jurnal Hukum*, *41*(3), 741–766. https://doi.org/10.26532/jh.v41i3.46981

Xiao, B. (2025). Agile and iterative governance: China's regulatory response to AI. *Computer Law & Security Review*, *58*, 106183. https://doi.org/10.1016/j.clsr.2025.106183

Yi, S., Yam, E. L. Y., Cheruvettolil, K., Linos, E., Gupta, A., Palaniappan, L., Rajeshuni, N., Vaska, K. G., Schulman, K., & Eggleston, K. N. (2024). Perspectives of Digital Health Innovations in Low- and Middle-Income Health Care Systems From South and Southeast Asia. *Journal of Medical Internet Research*, *26*. https://doi.org/10.2196/57612

Zhang, S., & Gao, H. (2025). Bridging the Great Wall: China's Evolving Cross-Border Data Flow Policies and Implications for Global Data Governance. *Computer Law & Security Review*, *59*, 106208. https://doi.org/10.1016/j.clsr.2025.106208

Zulkifli, Z., Almusawir, A., & Tira, A. (2025). Communal Intellectual Property Rights and Creative Industry Development Through Integration Patterns. *Jurnal Hukum*, *41*(3), 767–793. https://doi.org/10.26532/jh.v41i3.46980