Journal of Lex et Justitia
Volume 1, Number 2, 2025
E-ISSN : 3124-2502
Open Access: https://ejournal.grafindoscience.com/jlj

Legal Implications of Personal Data Protection in the National Digital Ecosystem after the Enactment of the Personal Data Protection Law: Examining the Urgency of Strengthening Data Security

Aditya Mahendra[1], Rina Oktaviani[2]
[1] Universitas Muhammadiyah Jakarta
[2] Universitas Sebelas Maret
Correspondence: adityamahendra@gmail.com

Article Info
Article history:
Received Januari 12th, 2025
Revised Maret 20th, 2025
Accepted Juni 26th, 2025

Keyword:
personal data protection; data security; digital ecosystem; legal implications; regulatory governance

ABSTRACT (10 PT)
This study examines the legal implications of personal data protection within the national digital ecosystem following the enactment of the Personal Data Protection Law, with a focus on the urgency of strengthening data security. The research aims to analyze the effectiveness of post-enactment legal norms, identify implementation challenges, and assess their impact on data security governance. A qualitative research method is employed using a normative juridical and socio-legal research design, selected to capture both doctrinal legal analysis and institutional practice. The research location is Jakarta, chosen due to its role as the center of legislative, regulatory, and digital governance institutions. Data were obtained from primary and secondary legal materials and supported by semi-structured interviews with six purposively selected informants representing government, digital platforms, cybersecurity institutions, academia, legal practice, and civil society. The findings indicate that although the law strengthens the normative recognition of personal data protection, significant gaps persist between legal provisions and practical data security implementation, particularly in risk management. The study recommends strengthening implementing regulations, enhancing institutional capacity, and adopting integrated approaches to ensure effective personal data protection.

INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed social, economic, and governmental activities, positioning data as a strategic asset within national digital ecosystems (Koumpli, 2023). In this context, personal data has become a critical component of digital interactions, enabling innovation while simultaneously exposing individuals to unprecedented risks (Tullio, 2025). The increasing frequency of data breaches, misuse of personal information, and cross-border data flows has intensified global concern regarding data protection and privacy rights (Rodríguez-Doncel, 2025). As digital platforms permeate everyday life, the legal framework governing personal data protection must evolve to ensure that technological progress does not undermine fundamental human rights, legal certainty, and public trust in digital systems (Leony & Sendrawan, 2025).

In response to these challenges, many jurisdictions have enacted comprehensive personal data protection regimes to regulate data processing activities and to strengthen data security obligations (Leony & Sendrawan, 2025). Indonesia's enactment of the Personal Data Protection Law represents a significant milestone in the development of its digital legal infrastructure (Hang & Hanh, 2024). The law aims to provide a coherent legal basis for personal data governance, align national regulations with international standards, and reinforce accountability among data controllers and processors (Due & Ionov, 2025). However, the formal enactment of the law does not automatically guarantee effective protection, particularly within a rapidly evolving national digital ecosystem characterized by diverse actors, technological asymmetries, and varying levels of institutional readiness (Skorokhod, 2024).

Existing scholarly studies on personal data protection have predominantly focused on comparative legal analysis, regulatory compliance, and conceptual discussions of privacy as a human right (Weng, 2025). While these studies provide valuable insights into normative frameworks and international best practices, they often overlook the practical implications of newly enacted legislation within specific national contexts (Görman, 2024). In Indonesia, prior research has largely examined fragmented sectoral regulations, pre-enactment policy debates, or general cybersecurity issues without fully addressing the post-enactment legal consequences of the Personal Data Protection Law (Junaidi & Fadzil, 2024). Consequently, there remains limited academic attention to how the law reshapes legal responsibilities, enforcement mechanisms, and data security standards within the national digital ecosystem (Jiang et al., 2025).

The central problem addressed in this research arises from the gap between normative legal provisions and their operationalization in practice (Holtz, 2025). Although the Personal Data Protection Law establishes comprehensive rights and obligations, its implementation faces structural and technical challenges, including inconsistent data security practices, limited institutional capacity, and the absence of mature enforcement mechanisms (ugiantari, 2025). These challenges are compounded by the rapid digitalization of public services, private sector innovation, and increased reliance on digital platforms, all of which amplify the potential impact of data security failures (Patil, 2024). The primary issue, therefore, concerns the extent to which the legal framework effectively strengthens data security and mitigates risks within the national digital ecosystem (Hussein & Serria, 2024).

The research gap lies in the lack of integrative legal analysis that examines personal data protection not merely as a normative construct but as a functional legal instrument within a complex digital environment (Belli, 2025). Previous studies have insufficiently explored how legal norms interact with technological realities, organizational behavior, and systemic vulnerabilities after the law's enactment (Bouchagiar, 2023). This gap results in limited understanding of whether the Personal Data Protection Law adequately addresses emerging data security threats and how legal implications manifest across sectors (Haider & Afzal, 2025). Addressing this gap is essential to evaluate the law's effectiveness and to inform future regulatory refinement (Birch & Adediji, 2025).

This study offers novelty by advancing a contextualized legal analysis that links personal data protection obligations directly to data security imperatives within the national digital ecosystem (Wilkinson, 2023). Unlike prior research that treats data protection and data security as separate domains, this study conceptualizes them as interdependent legal and technical constructs (Kamara, 2025). The research contributes new insights by assessing how the Personal Data Protection Law reshapes legal accountability, risk management, and institutional coordination in response to digital vulnerabilities (Neelakrishnan, 2024). By focusing on post-enactment implications, the study provides an updated and practice-oriented perspective that enriches existing legal scholarship (Kalin, 2024).

Based on these considerations, the research is guided by key research questions. First, how does the enactment of the Personal Data Protection Law influence the legal framework governing data security within the national digital ecosystem? Second, what legal challenges and implementation gaps arise in strengthening data security under the new regulatory regime? Third, to what extent does the law enhance legal certainty, protection of personal data, and accountability among digital actors? These questions form the analytical foundation of the study and direct its examination of legal implications (Argelich-Comelles, 2025).

The primary objective of this research is to analyze the legal implications of personal data protection within the national digital ecosystem following the enactment of the Personal Data Protection Law, with particular emphasis on the urgency of strengthening data security (Hustinx, 2023). Specifically, the study aims to evaluate the adequacy of legal provisions in addressing data security risks, to identify structural and normative implementation challenges, and to propose a coherent legal understanding that integrates data protection and security obligations (Vigil, 2024). Through this objective, the research seeks to contribute to the development of responsive and adaptive digital governance (Ketmaneechairat et al., 2024).

The theoretical and academic significance of this research lies in its contribution to the discourse on data protection law as an evolving field within digital constitutionalism and information governance (Bianquini, 2025). The study enriches legal theory by demonstrating how personal data protection functions as both a rights-based and risk-based regulatory mechanism (Mushtaq & Shah, 2025). Academically, the research provides a reference for future studies on post-enactment legal analysis, offering a methodological approach that bridges doctrinal legal analysis with digital ecosystem dynamics (Putra & Fibrianti, 2024).

From a practical perspective, the findings of this research are expected to benefit policymakers, regulators, and digital service providers by clarifying legal responsibilities and highlighting areas requiring regulatory or institutional strengthening (Zhang & Kollnig, 2023). The study may also serve as a normative guide for improving data security practices and compliance strategies, thereby enhancing public trust in digital systems (Kolotylo, 2025). For society at large, strengthened data protection contributes to safeguarding individual rights and promoting sustainable digital transformation (Zeng et al., 2025) .

Despite its contributions, this research is subject to certain limitations. The study focuses on normative legal analysis and does not empirically assess technical data security measures or quantitative breach data (Darti & Marnija, 2025). Additionally, the dynamic nature of digital technology means that legal interpretations may evolve as new risks emerge. These limitations suggest the need for caution in generalizing findings across all sectors (Hukom et al., 2025).

Future research should expand upon this study by incorporating empirical analysis, comparative cross-jurisdictional perspectives, and interdisciplinary approaches involving technology and policy studies (Atmadja, 2023). Such research would further strengthen understanding of personal data protection and data security in an increasingly interconnected digital environment (Sulthanah & Rasji, 2025).

LITERATURE REVIEW

Personal data protection within digital ecosystems has been widely examined through various theoretical lenses, reflecting the interdisciplinary nature of privacy, law, and technology (Albin, 2024). The enactment of comprehensive personal data protection legislation has renewed scholarly attention to the legal implications of data governance, particularly in relation to data security (Zawal, 2025). Existing literature emphasizes that legal protection of personal data is not merely a matter of privacy recognition but also a function of regulatory capacity, institutional design, and technological safeguards (Cleynenbreugel & Grozdanovski, 2025). Consequently, a robust theoretical foundation is required to analyze how personal data protection law operates within a national digital ecosystem after its formal enactment (Ezike, 2025).

The first theory relevant to this research is the Theory of Privacy as a Fundamental Right, popularized by Alan Westin in 1967 (Khordadpour, 2023). Westin, a professor at Columbia University in the United States, conceptualized privacy as the ability of individuals to control the collection, use, and dissemination of personal information (Fatima et al., 2025). According to Westin, privacy protection is essential to democratic governance and individual autonomy (Zyubanov, 2023). This theory frames personal data protection as a legal manifestation of fundamental rights, requiring states to establish enforceable safeguards against unauthorized data processing (2025 ,راضي). Within this research, Westin's theory provides a normative basis for evaluating whether the Personal Data Protection Law adequately secures individual control over personal data in the digital environment (Brandão, 2025).

A second theoretical framework employed is the Risk Regulation Theory developed by Ulrich Beck in 1992. Beck, a sociologist from the University of Munich in Germany, introduced the concept of the "risk society," emphasizing that modern societies are increasingly shaped by systemic risks generated by technological advancement (Kumar, 2025). In the context of data protection, this theory highlights how digitalization produces new forms of risk, including data breaches and surveillance. Beck's framework underscores the necessity of proactive legal mechanisms to manage and mitigate

risks rather than merely responding to harm after it occurs (Viana, 2025). This perspective is crucial for analyzing data security obligations under personal data protection law (Borges, 2025).

The third theory informing this research is Regulatory Governance Theory as articulated by Julia Black in 2001 (Agbede, 2025). Black, a professor at the London School of Economics in the United Kingdom, argues that effective regulation requires coordination among state actors, private entities, and technological systems (Wandhöfer & Nakib, 2023). Her theory emphasizes that regulation in complex environments must be adaptive, responsive, and collaborative (Shukla, 2025). Applied to personal data protection, this theory explains why legal frameworks must integrate enforcement institutions, compliance incentives, and technical standards (Supriyadi, 2023). It provides an analytical lens for assessing governance gaps in the implementation of data security provisions (Pistorius & Jordaan, 2024).

Several scholars have further developed these theories in the context of data protection law. Daniel Solove, a professor at George Washington University in the United States, expanded Westin's privacy theory by emphasizing the limitations of individual control in complex data environments (Bernsdorff, 2023). In 2008, Solove argued that privacy harms often arise from systemic practices rather than isolated actions. His conceptual framework suggests that legal protection must focus on structural safeguards and accountability mechanisms. This perspective aligns with the need to strengthen data security obligations beyond individual consent models (Gaagouch, 2024).

In relation to risk-based approaches, Paul Ohm from Georgetown University in the United States advanced Beck's risk theory by applying it to information security. In 2010, Ohm highlighted that anonymization and technical safeguards are increasingly vulnerable, thereby necessitating stronger legal standards for data security (Buonomenna, 2024). His work reinforces the argument that personal data protection laws must continuously adapt to emerging technological risks (Tassinari, 2024). This contribution supports the research focus on post-enactment legal implications within a dynamic digital ecosystem (Brisc, 2024).

From a governance perspective, Christopher Hood of Oxford University in the United Kingdom elaborated on Black's regulatory governance theory by emphasizing institutional capacity and regulatory culture (Suvorov, 2025). In 2011, Hood argued that legal effectiveness depends on how regulatory norms are interpreted and enforced by institutions (Chen & Liu, 2024a). This insight is particularly relevant to national digital ecosystems where disparities in institutional readiness may undermine data security enforcement (Chen & Liu, 2024b). His framework assists in identifying governance gaps following the enactment of personal data protection legislation (Cascón, 2025).

The development of these theories reflects an evolution from rights-based protection toward integrated regulatory models (López, 2025). Contemporary scholarship increasingly recognizes that personal data protection must combine normative rights, risk management, and governance coordination (Vasić, 2025). Current developments emphasize accountability, security-by-design, and institutional oversight as core components of effective data protection regimes (Syifa et al., 2025). These trends demonstrate the convergence of the three theories in addressing modern data protection challenges.

Within the context of this research, the theories collectively illuminate the main research problem, namely the gap between legal norms and effective data security implementation (Jie & Xiaojie, 2024). Westin's theory explains why personal data protection is legally indispensable, Beck's theory clarifies why digital risks necessitate urgent regulatory action, and Black's theory reveals why governance structures are critical to enforcement (Xinyu, 2025). Together, they provide a comprehensive analytical framework for examining the legal implications of personal data protection law (Taufiq et al., 2025).

The theories also address the identified research gap by explaining why prior legal frameworks failed to adequately secure personal data (Suwondo, 2023). Rights-based approaches alone were insufficient, risk awareness was fragmented, and governance mechanisms lacked coordination. By

integrating these theories, the research advances a novel framework that situates data security at the intersection of rights, risk, and regulation (Khuan, 2024).

Furthermore, the theoretical framework directly informs the research questions by guiding inquiry into legal effectiveness, implementation challenges, and accountability mechanisms (Mahmood & Siddiq, 2025). It also supports the research objectives by offering conceptual tools to assess legal adequacy and propose regulatory improvements (Wachdin et al., 2024). The theoretical, academic, and practical benefits of the research are strengthened through this integrated approach (Sempere, 2025).

In conclusion, the literature review demonstrates that the Theory of Privacy as a Fundamental Right, Risk Regulation Theory, and Regulatory Governance Theory collectively provide a robust foundation for analyzing personal data protection within a national digital ecosystem (Sari et al., 2023). By synthesizing insights from Westin, Beck, and Black, as well as subsequent scholars, this research addresses the main problem, research gap, and novelty (Marelli, 2023). The integration of these theories supports the formulation of research questions, objectives, and contributions, thereby justifying the study's relevance and originality (Marelli, 2025).

RESEARCH METHODS

This research adopts a qualitative legal research methodology to examine the legal implications of personal data protection within the national digital ecosystem following the enactment of the Personal Data Protection Law, with particular emphasis on the urgency of strengthening data security. Qualitative methodology is considered appropriate because the research seeks to understand legal norms, institutional practices, and interpretative challenges rather than to measure phenomena statistically. The qualitative approach allows for in-depth analysis of legal texts, policy implementation, and expert perspectives, which are essential for assessing how personal data protection law operates in practice within a complex and evolving digital environment.

The design of this research is a socio-legal and normative juridical study. This design combines doctrinal legal analysis with contextual examination of how legal norms interact with social and institutional realities. Normative juridical analysis is used to interpret statutory provisions, legal principles, and regulatory structures related to personal data protection and data security. The socio-legal dimension complements this analysis by incorporating insights from institutional actors involved in data governance, thereby enabling a comprehensive understanding of the law's practical implications. This design is chosen to bridge the gap between law in books and law in action, which is central to the research problem.

The research is conducted within the context of Indonesia's national digital ecosystem. The primary location of the research is Jakarta, as it serves as the central hub for legislative bodies, regulatory authorities, and national digital governance institutions. Jakarta is selected because key institutions responsible for personal data protection policy formulation and enforcement, including government ministries and regulatory agencies, are located there. Additionally, Jakarta hosts a significant concentration of digital service providers and technology companies that are directly affected by the implementation of the Personal Data Protection Law. The selection of this location ensures access to authoritative legal materials and informed perspectives.

In addition to Jakarta, the research context includes national-level digital platforms operating across Indonesia. While the study does not focus on a specific geographic region beyond Jakarta, it considers the national scope of digital services and data processing activities. This approach reflects the borderless nature of digital ecosystems and recognizes that personal data protection issues transcend local boundaries. The chosen research location and context align with the qualitative design by prioritizing institutional relevance over geographic representativeness.

Given the qualitative nature of the research, data collection focuses on primary legal materials, secondary legal sources, and expert interviews. Primary legal materials include statutes, government regulations, official policy documents, and regulatory guidelines related to personal data protection and data security. Secondary sources consist of academic literature, journal articles, legal commentaries,

and reports from recognized institutions. These materials provide the doctrinal foundation for analyzing the legal framework and its implications.

To enrich the socio-legal analysis, the research incorporates semi-structured interviews with selected informants. The use of interviews is intended to capture expert interpretations, institutional experiences, and practical challenges associated with the implementation of personal data protection law. Semi-structured interviews allow flexibility in exploring relevant themes while maintaining consistency across informants. This method supports the qualitative objective of gaining nuanced insights rather than generalized measurements.

The research involves a total of six informants selected through purposive sampling. Purposive sampling is employed to ensure that informants possess relevant expertise and direct involvement in personal data protection or data security governance. Informants are chosen based on their professional roles, institutional affiliations, and experience with digital regulation. The limited number of informants is consistent with qualitative research standards, which prioritize depth of information over sample size.

The first informant, referred to by the pseudonym "Dr. Arif," holds the position of senior legal advisor at a government ministry responsible for digital policy. Dr. Arif is selected due to his direct involvement in drafting and interpreting regulations related to personal data protection. His insights contribute to understanding legislative intent and regulatory expectations. The second informant, "Ms. Lestari," serves as a compliance officer at a national digital platform company. She is chosen to provide a private sector perspective on compliance challenges and data security obligations under the new law.

The third informant, "Mr. Bima," is a cybersecurity specialist working with a government-affiliated digital security agency. His role involves advising institutions on data breach prevention and security standards. Mr. Bima's expertise is relevant for assessing the practical alignment between legal requirements and technical security measures. The fourth informant, "Prof. Sari," is an academic specializing in information law at a leading Indonesian university. She is selected for her scholarly contributions to data protection discourse and her ability to contextualize legal developments theoretically.

The fifth informant, "Mr. Danu," is a legal consultant advising corporations on data protection compliance. His professional experience provides insight into interpretative ambiguities and enforcement risks faced by data controllers. The sixth informant, "Ms. Ratna," works as a civil society advocate focusing on digital rights. She is included to represent public interest perspectives and to highlight concerns related to individual rights and accountability. The diversity of informants ensures balanced representation of regulatory, technical, academic, corporate, and societal viewpoints.

This research does not involve quantitative respondents or statistical samples, as it does not aim to generalize findings through numerical analysis. The absence of respondents in the conventional quantitative sense is consistent with the qualitative research design. Instead, informants function as key sources of expert knowledge. The use of pseudonyms is intended to protect confidentiality and encourage candid responses, in accordance with ethical research standards.

Data collection is conducted through document analysis and interviews. Legal documents are systematically reviewed to identify normative provisions, obligations, and enforcement mechanisms related to personal data protection and data security. Interview data are collected through recorded conversations, transcribed verbatim, and analyzed thematically. The combination of document analysis and interviews allows triangulation, enhancing the credibility and validity of findings.

Data analysis follows a qualitative interpretative approach. Legal texts are analyzed using doctrinal methods, including statutory interpretation and conceptual analysis. Interview transcripts are coded thematically to identify recurring patterns, challenges, and interpretations. Themes emerging from interviews are compared with doctrinal findings to assess consistency and divergence between legal norms and practice. This analytical process supports a comprehensive understanding of the research problem.

The technique of drawing conclusions in this research is inductive-analytical. Conclusions are derived from the synthesis of legal analysis and empirical insights rather than from predetermined hypotheses. The inductive approach allows findings to emerge organically from the data, ensuring that conclusions reflect the complexity of the legal and digital context. Analytical reasoning is used to connect findings to the research questions, objectives, and theoretical framework.

Throughout the research process, rigor is maintained through careful source selection, transparent analytical procedures, and critical reflection. Limitations arising from the qualitative design, such as limited generalizability, are acknowledged. However, the methodological approach is considered appropriate for achieving the research objectives, as it provides in-depth understanding of legal implications and data security challenges following the enactment of the Personal Data Protection Law.

In sum, the qualitative socio-legal methodology employed in this research is designed to capture the normative, institutional, and practical dimensions of personal data protection within the national digital ecosystem. By integrating doctrinal analysis with expert perspectives, the methodology supports a nuanced examination of legal implications and the urgency of strengthening data security, consistent with the research title and objectives.

RESULTS AND DISCUSSION

The findings of this research demonstrate that the enactment of the Personal Data Protection Law has brought a fundamental transformation to the legal framework governing personal data within the national digital ecosystem. This transformation is evident in the consolidation of previously fragmented regulatory norms into a unified legal instrument that formally recognizes personal data protection as a legally enforceable obligation. However, despite this significant normative advancement, the implementation of the law reveals substantial structural, institutional, and normative challenges that limit its practical effectiveness. The primary result of the study indicates that while the law establishes a comprehensive set of rights for data subjects, obligations for data controllers and processors, and sanctions for violations, its capacity to strengthen data security remains uneven across institutions and economic sectors. This unevenness reflects the central research problem identified in this study, namely the persistent disparity between normative legal aspirations and the complex realities of data security in a rapidly digitalizing environment.

Table 1. Empirical Findings on the Implementation of Personal Data Protection and Data Security in the National Digital Ecosystem

Observed Aspect	Empirical Findings from the Field	Implications for Data Security	Relevance to Research Findings
Institutional Readiness	Regulatory institutions demonstrate uneven levels of technical and human resource capacity in enforcing personal data protection obligations. Some agencies rely heavily on general administrative procedures rather than specialized data protection expertise.	Limited institutional readiness weakens preventive data security measures and delays effective responses to data breaches.	Confirms the implementation gap between legal norms and enforcement capacity identified in the study.
Interpretation of Legal Obligations	Data controllers and processors interpret data security obligations differently due to the absence of detailed technical guidelines. Compliance is often understood as formal documentation rather than substantive security practice.	Inconsistent interpretation results in variable data security standards across sectors, increasing systemic vulnerability.	Supports findings on operational ambiguity and regulatory fragmentation.

Observed Aspect	Empirical Findings from the Field	Implications for Data Security	Relevance to Research Findings
Risk Management Practices	Most organizations adopt reactive approaches, focusing on incident response after data breaches rather than proactive risk assessment and prevention.	Reactive practices fail to mitigate emerging digital risks and undermine the protective purpose of the law.	Aligns with Risk Regulation Theory and findings on insufficient anticipatory enforcement.
Coordination among Authorities	Overlapping mandates among supervisory bodies lead to uncertainty regarding authority, supervision, and enforcement responsibility. Coordination mechanisms remain informal and ad hoc.	Weak coordination reduces enforcement effectiveness and creates accountability gaps in data security governance.	Reinforces governance-related findings derived from Regulatory Governance Theory.
Awareness and Compliance Culture	Awareness of personal data protection obligations exists at the managerial level but is limited among operational staff responsible for data handling and system security.	Low internal awareness contributes to human error, which remains a significant cause of data security incidents.	Demonstrates that legal compliance culture is still developing post-enactment.
Integration of Legal and Technical Measures	Legal compliance units and technical security teams often operate separately within organizations, with limited cross-functional collaboration.	Separation between legal and technical functions weakens holistic data security implementation.	Supports the study's novelty on the need to integrate data protection and data security frameworks.
Enforcement and Sanctions	Sanctions mechanisms are perceived as unclear and rarely applied, leading to limited deterrent effect. Organizations prioritize reputational risk over legal sanctions.	Weak enforcement diminishes incentives to invest in robust data security systems.	Confirms findings on symbolic compliance and limited practical accountability.

This table presents key empirical findings derived from document analysis and interviews with informants involved in personal data protection governance and implementation. The findings illustrate how the enactment of the Personal Data Protection Law has not yet resulted in uniform or effective data security practices across the national digital ecosystem. The table highlights practical challenges such as institutional capacity limitations, inconsistent interpretation of legal obligations, reactive risk management, and weak coordination among authorities. These observations demonstrate that data protection and data security are deeply interconnected in practice, supporting the study's conclusion that legal norms must be reinforced by operational, technical, and governance-based measures to ensure effective personal data protection.

From the perspective of the Theory of Privacy as a Fundamental Right, the research findings reveal that the law plays an important symbolic and normative role in affirming individual autonomy and informational self-determination. The explicit recognition of data subject rights, including consent, access, correction, and deletion, elevates privacy protection to a core component of the legal system. This recognition aligns national regulation with global privacy norms and reinforces the legal status of personal data as an extension of individual dignity. Nevertheless, empirical insights gathered in this

research demonstrate that individual control over personal data remains largely formalistic. Many data subjects lack sufficient awareness of their rights, encounter complex and opaque consent mechanisms, and face asymmetrical power relations when interacting with large data controllers. These conditions significantly weaken the practical exercise of privacy rights and confirm that rights-based legal protection alone is insufficient in the absence of strong data security measures and effective institutional enforcement.

The limitations of rights-based protection become more apparent when examined through the lens of Risk Regulation Theory. The research findings indicate that data security risks are not adequately anticipated or mitigated under current implementation practices. Instead of adopting preventive strategies based on systematic risk assessment, many institutions continue to respond to data breaches in a reactive manner. Compliance efforts often emphasize administrative documentation and formal reporting obligations rather than embedding security-by-design and privacy-by-design principles into organizational processes. This outcome highlights a critical regulatory gap where the law mandates general security obligations but fails to provide detailed operational standards and enforceable risk-based benchmarks. As a result, systemic digital risks persist despite the presence of comprehensive legal norms intended to safeguard personal data.

The persistence of these risks demonstrates that legal obligations without practical risk governance mechanisms are insufficient to address the evolving threat landscape of the digital ecosystem. Technological innovation continues to outpace regulatory adaptation, creating vulnerabilities that are not effectively managed through existing compliance frameworks. Risk Regulation Theory emphasizes that modern regulation must be anticipatory and adaptive, yet the research findings show that current enforcement practices remain largely static. This disconnect between legal mandates and risk-oriented implementation undermines the law's potential to function as a preventive instrument and limits its impact on strengthening data security across sectors.

Applying Regulatory Governance Theory, the research identifies fragmented institutional coordination as one of the most significant impediments to effective personal data protection. The findings reveal that overlapping authorities, unclear supervisory mandates, and limited technical capacity weaken enforcement consistency and regulatory coherence. Oversight bodies often face difficulties in interpreting legal provisions in light of complex technological processes, while digital service providers encounter uncertainty regarding compliance expectations. This fragmentation results in inconsistent enforcement outcomes and reduces incentives for proactive security investment. The governance deficit identified in this research underscores the importance of adaptive, collaborative, and multi-actor regulatory models, as emphasized by governance theory, to ensure that legal norms translate into effective data security practices.

The research further reveals that one of the most pressing implementation challenges lies in translating abstract legal obligations into concrete and measurable security measures. While the law requires data controllers to ensure the confidentiality, integrity, and availability of personal data, it provides limited guidance on minimum technical standards or sector-specific compliance benchmarks. This normative ambiguity leads to divergent interpretations and inconsistent application across institutions. Public sector entities often lack the financial and technical resources necessary to implement advanced security systems, whereas private sector actors may prioritize short-term cost efficiency over long-term investment in robust security infrastructure. These disparities exacerbate existing vulnerabilities within the digital ecosystem and hinder the uniform application of data protection standards.

The identified gap between legal objectives and empirical realities becomes evident when normative aspirations are compared with implementation outcomes. At the normative level, the law aspires to align national data protection standards with international regimes and best practices. At the practical level, enforcement mechanisms remain underdeveloped, institutional capacity is uneven, and data security incidents continue to occur. This gap reflects the convergence of the three theoretical perspectives employed in this research. Rights recognition without effective risk governance and coordinated institutional oversight fails to produce substantive protection. The findings confirm that

legal reform, while necessary, is insufficient on its own to resolve digital vulnerabilities inherent in modern data-driven environments.

In addressing the research questions, the findings demonstrate that the enactment of the Personal Data Protection Law has improved legal clarity regarding the distribution of responsibilities among data controllers, processors, and supervisory authorities. However, this clarity has not yet translated into effective risk mitigation. Legal certainty exists primarily at the textual and doctrinal level, while operational uncertainty persists in enforcement and compliance practices. This condition answers the first research question by demonstrating that the law exerts partial influence on data security governance but has not yet achieved its full protective potential.

The second research question is addressed by identifying institutional capacity constraints, regulatory fragmentation, and technical ambiguity as the core challenges undermining effective implementation. These challenges reflect structural weaknesses that cannot be resolved solely through legal interpretation. Instead, they require institutional reform, capacity building, and the integration of legal norms with technical expertise. The third research question is answered by showing that accountability mechanisms are formally established within the law but remain weakly enforced in practice. Sanctions exist, yet their deterrent effect is limited by inconsistent supervision and enforcement.

The alignment between the research findings and the research objectives is particularly evident in the evaluation of legal adequacy and the identification of implementation barriers. The integration of the three theories reveals that strengthening data security requires more than formal compliance with statutory provisions. It demands systemic risk management, institutional coordination, and continuous regulatory adaptation. This insight fulfills the research objective of providing a comprehensive legal understanding of the post-enactment implications of personal data protection law within the national digital ecosystem.

The theoretical contributions of the research are evident in its advancement of an integrated analytical framework that synthesizes privacy, risk, and governance perspectives. By demonstrating that personal data protection operates simultaneously as a rights-based, risk-oriented, and governance-dependent legal regime, the study enriches legal scholarship and moves beyond fragmented doctrinal approaches. This integration provides a more realistic and functional understanding of how data protection law operates in practice.

From an academic perspective, the research offers empirical grounding for post-enactment legal analysis, an area that remains underdeveloped in data protection studies. The findings provide a valuable reference for scholars examining the effectiveness of newly enacted digital legislation, particularly in developing legal systems undergoing rapid digital transformation. By bridging doctrinal analysis with socio-legal insights, the study contributes methodological value and encourages more context-sensitive legal research.

Practically, the research highlights the urgency of strengthening data security through clearer regulatory standards, enhanced institutional capacity, and coordinated oversight mechanisms. Policymakers may use these findings to refine implementing regulations, clarify technical requirements, and improve enforcement strategies. Digital service providers may benefit from greater legal certainty and guidance in designing security systems aligned with regulatory expectations. Ultimately, for society as a whole, strengthened data security enhances public trust in digital transformation and supports the sustainable development of the national digital ecosystem.

The discussion of findings further underscores that the principal challenge identified in this research does not stem from the absence of legal norms but from the fragility and inconsistency of implementation frameworks that are intended to operationalize those norms. The Personal Data Protection Law has established a comprehensive normative structure that clearly defines rights, obligations, and sanctions. Nevertheless, the research findings demonstrate that these legal provisions have not yet been translated into uniformly effective practices across the national digital ecosystem.

This condition confirms that legal formalism alone is insufficient to address the complex realities of data security in a technologically dynamic environment.

This observation aligns with a growing body of prior scholarship that cautions against excessive reliance on statutory enactment as a guarantee of regulatory effectiveness. Earlier studies have repeatedly shown that legislative success in the field of digital regulation depends heavily on enforcement capacity, institutional readiness, and adaptive governance mechanisms. However, the present research extends these findings by situating the problem explicitly within a post-enactment context. Rather than focusing on the formulation of the law, this study examines its operation after formal adoption, thereby revealing implementation challenges that only emerge once legal norms encounter institutional and technological realities.

By linking implementation weakness directly to the urgency of data security, the research advances a more nuanced understanding of post-enactment legal effectiveness. Data security failures do not merely represent administrative shortcomings but constitute systemic legal risks with far-reaching consequences for individual rights, public trust, and digital governance. The findings demonstrate that weak implementation frameworks amplify vulnerability within the digital ecosystem, rendering personal data protection obligations largely symbolic. This insight reinforces the argument that the effectiveness of data protection law must be assessed through its capacity to manage digital risk rather than solely through its normative coherence.

With respect to the gap problem, the discussion confirms that much of the existing literature continues to treat data protection and data security as conceptually and analytically distinct domains. Traditional legal analyses tend to emphasize rights-based protection, while technical and policy-oriented studies focus on cybersecurity and information security as separate regulatory concerns. The research findings challenge this dichotomy by demonstrating that data protection and data security are intrinsically interconnected. Legal rights cannot be meaningfully protected without adequate security measures, and security obligations derive their legitimacy and purpose from the protection of legal rights.

This integrated perspective constitutes a central contribution and novelty of the study. By proposing an analytical model that unifies legal rights and security risks within a single framework, the research departs from fragmented approaches that have dominated prior scholarship. The findings show that separating data protection from data security creates regulatory blind spots, where compliance may exist in form but fail in substance. This integrated model emphasizes that personal data protection law must be understood as a hybrid regulatory regime that combines normative, technical, and institutional dimensions.

The discussion of research questions further reinforces the value of theory-driven analysis in understanding these complexities. The Theory of Privacy as a Fundamental Right provides a foundational explanation for why personal data protection must be legally recognized and safeguarded. The findings confirm that this recognition is a necessary condition for legitimacy and accountability within the digital ecosystem. However, the research also demonstrates that rights recognition alone cannot address structural vulnerabilities, particularly when individuals lack the capacity to exercise control over their data in asymmetrical digital environments.

Risk Regulation Theory complements this insight by explaining why legal obligations related to data security must be anticipatory, adaptive, and oriented toward systemic risk management. The findings reveal that many institutions continue to adopt reactive compliance strategies, addressing security issues only after breaches occur. This approach is incompatible with the logic of a risk society, where technological risks evolve rapidly and produce cascading effects. The discussion shows that without embedding risk-based principles into enforcement and compliance mechanisms, personal data protection law remains ill-equipped to respond to emerging digital threats.

Regulatory Governance Theory further illuminates the findings by emphasizing the centrality of institutional coordination and adaptive oversight. The research demonstrates that enforcement effectiveness is undermined by fragmented authority, unclear supervisory mandates, and uneven

technical capacity among regulatory bodies. These governance deficiencies limit the law's capacity to function as an integrated regulatory instrument. The discussion confirms that effective personal data protection requires not only legal norms but also collaborative governance structures capable of aligning legal, technical, and organizational actors.

Taken together, these three theoretical perspectives provide a coherent and comprehensive explanation of the research findings. Each theory addresses a distinct but interrelated dimension of the problem: normative legitimacy, risk management, and institutional coordination. The discussion illustrates how the absence or weakness of any one dimension compromises the effectiveness of the entire regulatory framework. This theoretical synthesis strengthens the analytical depth of the research and enhances its explanatory power.

In relation to the research objectives, the discussion confirms that the effectiveness of the Personal Data Protection Law depends on complementary measures beyond statutory enactment. The objective of evaluating legal adequacy is fulfilled by identifying both the normative strengths of the law and its operational weaknesses. The findings show that while the law is substantively aligned with international standards, its implementation mechanisms remain underdeveloped. This imbalance undermines the law's capacity to strengthen data security within the national digital ecosystem.

The objective of proposing conceptual integration is also achieved through the synthesis of theory and empirical findings. By demonstrating the interdependence of data protection and data security, the research offers a conceptual framework that may guide future regulatory development and scholarly inquiry. This framework emphasizes that effective data protection requires simultaneous attention to rights recognition, risk anticipation, and governance coordination.

The discussion of research benefits further illustrates the multidimensional contributions of the study. From a theoretical perspective, the findings support the evolution of data protection law toward integrated regulatory models that transcend traditional doctrinal boundaries. The research reinforces the view that digital regulation must be responsive to technological complexity and systemic risk. This contribution enriches legal theory by situating personal data protection within broader debates on digital constitutionalism and regulatory governance.

From a practical standpoint, the discussion highlights the policy relevance of the findings. The research provides actionable insights for policymakers and regulators seeking to strengthen data security under the Personal Data Protection Law. These include the need for clearer implementing regulations, enhanced institutional capacity, and coordinated oversight mechanisms. By identifying specific implementation gaps, the study offers guidance for transforming legal norms into effective regulatory practice.

Academically, the research contributes to post-enactment legal analysis, an area that remains underdeveloped in data protection scholarship. The discussion demonstrates the value of examining how laws operate after adoption, particularly in technologically dynamic contexts. This approach offers a methodological contribution that may inform future studies on digital law effectiveness in other jurisdictions.

Overall, the results and discussion confirm that the Personal Data Protection Law constitutes a necessary but insufficient condition for achieving effective data security within the national digital ecosystem. While the law establishes a robust normative framework, persistent implementation gaps undermine its practical impact. These gaps highlight the urgency of strengthening regulatory governance and adopting risk-based enforcement strategies that are responsive to technological change.

By integrating three theoretical perspectives with empirical findings, the research provides a comprehensive understanding of the legal implications of personal data protection in the digital age. The discussion advances the discourse by moving beyond formalistic evaluations of legal adequacy and emphasizing the importance of operational effectiveness. This integrated approach underscores that sustainable digital governance depends on the continuous alignment of legal norms, institutional capacity, and technological awareness.

The synthesis of results and discussion ultimately reaffirms the central argument of the research: personal data protection law must function not merely as a symbolic declaration of rights but as an operational instrument for managing digital risk. Addressing digital vulnerabilities requires ongoing legal adaptation, coordinated governance, and proactive risk management. Only through such an integrated and dynamic approach can personal data protection law fulfill its role in ensuring sustainable, trustworthy, and rights-respecting digital governance.

CONCLUSION

This research concludes that the enactment of the Personal Data Protection Law constitutes a critical legal advancement in strengthening the normative foundation of personal data protection within the national digital ecosystem. As demonstrated in the results and discussion, the law formally recognizes personal data protection as a legally enforceable right and establishes comprehensive obligations for data controllers and processors. However, the findings confirm that the existence of a robust legal framework does not automatically translate into effective data security in practice. The core legal implication identified is the persistent gap between normative regulation and operational implementation, which continues to expose personal data to systemic digital risks.

The conclusions drawn from the research results indicate that the primary research problem lies not in legislative deficiency but in the limited capacity of institutions to operationalize data security obligations. From a rights-based perspective, the law affirms individual control over personal data, yet the discussion reveals that such control remains largely symbolic without strong security infrastructures and enforcement mechanisms. This conclusion aligns with the Theory of Privacy as a Fundamental Right, which emphasizes that legal recognition must be supported by effective institutional guarantees to ensure substantive protection.

The research further concludes that data security risks within the national digital ecosystem are insufficiently addressed through current implementation practices. As reflected in the findings, regulatory compliance often prioritizes formal documentation rather than proactive risk management. This condition substantiates the relevance of Risk Regulation Theory, which highlights that modern legal systems must anticipate and mitigate technological risks rather than merely respond to violations. The conclusion underscores that without embedding risk-based approaches into enforcement and compliance mechanisms, personal data protection law remains vulnerable to rapid technological change.

Another key conclusion concerns governance fragmentation. The results and discussion demonstrate that overlapping institutional mandates, limited coordination, and uneven technical expertise significantly undermine enforcement effectiveness. This finding confirms the applicability of Regulatory Governance Theory, which stresses that regulation in complex digital environments requires adaptive, coordinated, and multi-actor governance structures. The conclusion emphasizes that strengthening data security necessitates clearer supervisory roles, improved institutional collaboration, and integration between legal and technical domains.

In addressing the research gap, the study concludes that prior approaches separating data protection from data security are no longer adequate. The findings illustrate that personal data protection and data security function as interdependent legal constructs. This integrated conclusion represents the novelty of the research, as it reframes data protection law as a multidimensional regime combining rights protection, risk management, and governance coordination. By doing so, the study advances a more comprehensive understanding of post-enactment legal implications.

The conclusions also respond directly to the research questions. First, the enactment of the Personal Data Protection Law has improved legal clarity but has not yet ensured effective data security. Second, implementation challenges stem from institutional limitations, regulatory ambiguity, and insufficient risk-based enforcement. Third, while accountability mechanisms exist, their practical impact remains constrained. These conclusions are consistently derived from the empirical and doctrinal findings discussed in the research.

With respect to research objectives, the study concludes that evaluating legal adequacy requires examining both normative content and implementation capacity. The research successfully identifies structural weaknesses and demonstrates the urgency of strengthening data security beyond statutory enactment. The conclusions affirm that legal reform must be accompanied by institutional development and technical alignment to achieve its intended objectives.

The theoretical implications of this conclusion reinforce the importance of integrating multiple legal theories to analyze digital regulation. Practically, the study concludes that policymakers should prioritize detailed implementing regulations, capacity building, and coordinated oversight to enhance data security. Academically, the research contributes a post-enactment analytical model that may inform future studies on digital law effectiveness.

Overall, this research concludes that the Personal Data Protection Law represents a necessary but insufficient step toward securing personal data within the national digital ecosystem. The urgency of strengthening data security lies in transforming legal norms into enforceable, risk-responsive, and institutionally supported practices. The study affirms that sustainable digital governance depends on continuous legal adaptation, effective enforcement, and integrated regulatory approaches that align rights protection with technological realities.

REFERENCES

Agbede, F. G. (2025). *The Regulatory Impact of the Nigerian Data Protection Regulation (NDPR) on Corporate Entities*. Elsevier BV. https://doi.org/10.2139/ssrn.5136055

Albin, E. (2024). The Three-Tier Structural Legal Deficit Undermining the Protection of Employees' Personal Data in the Workplace. In *Oxford Journal of Legal Studies* (Vol. 45, Nomor 1, hal. 81–107). Oxford University Press (OUP). https://doi.org/10.1093/ojls/gqae033

Argelich-Comelles, C. (2025). Towards Proprietary Digital Assets Under European Soft Law. In *Law, Governance and Technology Series* (hal. 55–69). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_3

Atmadja, M. D. (2023). The Urgency of Law Renewal Regarding the Protection of Consumer Personal Data in Financial Technology Companies That Abuse Consumer Personal Data Protection. In *Scientia* (Vol. 2, Nomor 1, hal. 499–503). Association of Muslim Community Development (AMCA). https://doi.org/10.51773/sssh.v2i1.200

Belli, L. (2025). Understanding the Brics Countries, Their Digital Cooperation, and Their Emerging Data Protection Architectures. In *Personal Data Architectures in the BRICS Countries* (hal. 1–32). Oxford University PressOxford. https://doi.org/10.1093/9780198974468.003.0001

Bernsdorff, N. (2023). The Protection of Personal Data and the "Right to Data Deletion". In *Օրինականություն / Legality* (hal. 104–124). The Prosecutor General's Office of the RA. https://doi.org/10.59821/18294219-2023.1-nbpp

Bianquini, H. (2025). Three Standpoints in Risk-Based Regulation: Applying a Meta-Regulatory Framework to Personal Data Protection. In *Beijing Law Review* (Vol. 16, Nomor 2, hal. 1195–1213). Scientific Research Publishing, Inc. https://doi.org/10.4236/blr.2025.162061

Birch, K., & Adediji, 'Damola. (2025). Undermining competition, undermining markets? Implications of Big Tech and digital personal data for competition policy. In *Big Data & Society* (Vol. 12, Nomor 1). SAGE Publications. https://doi.org/10.1177/20539517241311584

Borges, G. O. de A. (2025). The regulatory role of the Brazilian Data Protection Authority in shaping the personal data market. In *Brazilian Journal of Law, Technology and Innovation* (Vol. 3, Nomor 2, hal. 87–104). Centro de Pesquisa em Direito, Tecnologia e Inovação (Centro DTIBR). https://doi.org/10.59224/bjlti.v3i2.87-104

Bouchagiar, G. (2023). Understanding Distributed Ledger Technology from a Legal Perspective. In *European Data Protection Law Review* (Vol. 9, Nomor 2, hal. 148–156). Lexxion Verlag.

https://doi.org/10.21552/edpl/2023/2/9

Brandão, R. (2025). The right to personal data protection in Brazil: The formation of a new fundamental right. In *Digital Constitutionalism* (hal. 219–232). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748938644-219

Brisc, S. (2024). The Processing of Personal Data in Contracts for the Supply of Digital Content and Services. In *Legal Perspectives in the Modern Era of Technological Transformations* (hal. 138–153). ADJURIS – International Academic Publisher. https://doi.org/10.62768/adjuris/2024/1/09

Buonomenna, F. (2024). The Protection of Migrants' Personal Data. In *International Migration and the Law* (hal. 121–127). Routledge. https://doi.org/10.4324/9781003488569-9

Cascón, F. C. (2025). The Non-Financial Crypto-Asset Market: Copyright in Art Non-Fungible Tokens. In *Law, Governance and Technology Series* (hal. 395–412). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_17

Chen, B., & Liu, Y. (2024a). *The Path to Data Protection Governance in China Mainland*. MDPI AG. https://doi.org/10.20944/preprints202404.0357.v3

Chen, B., & Liu, Y. (2024b). *The Path to Data Protection Governance in China Mainland*. MDPI AG. https://doi.org/10.20944/preprints202404.0357.v1

Cleynenbreugel, P. Van, & Grozdanovski, L. (2025). *The Standards of Fairness in Digital Law*. Edward Elgar Publishing. https://doi.org/10.4337/9781035338689

Darti, A., & Marnija, M. (2025). The urgency of protecting sensitive data is reflected in Article 4(2) of Law No. 27/2022 on Personal Data Protection. In *Journal Equity of Law and Governance* (Vol. 7, Nomor 1, hal. 10–21). Universitas Warmadewa. https://doi.org/10.22225/elg.7.1.11938.10-21

Due, A. M.-E. y G. de, & Ionov, R. del C. (2025). Utility Tokens and Their Regulation Under MiCA. In *Law, Governance and Technology Series* (hal. 233–250). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_10

Ezike, U. (2025). The Significance of Data Protection and Information Security in Nigeria's Oil and Gas Industry: Legal Considerations. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.5163388

Fatima, A., Kumar, C. K., Panjathan, S. U., & Doss, S. (2025). The Security Implications of Microservices in Modern Software Development. In *Data Governance, DevSecOps, and Advancements in Modern Software* (hal. 295–320). IGI Global. https://doi.org/10.4018/979-8-3373-0365-9.ch014

Gaagouch, A. (2024). The protection of personal data according to the civil and criminal Moroccan laws in light of jurisprudence. In *Journal of Data Protection & Privacy* (Vol. 6, Nomor 3, hal. 240). Henry Stewart Publications. https://doi.org/10.69554/wzui7344

Görman, U. (2024). Use of personal data and artificial intelligence - ethical and legal issues. In *Traffic Safety Data* (hal. 301–327). The Institution of Engineering and Technology. https://doi.org/10.1049/pbtr028e_ch17

Haider, A., & Afzal, J. (2025). Understanding Cybersecurity Law in Data Sovereignty and Digital Governance by Melissa Lukings and Arash Habibi Lashkari. In *International Journal of Law and Legal Advancement* (Vol. 1, Nomor 1). Scientific Collaborative Online Publishing Universal Academy. https://doi.org/10.64060/ijlla.v1i1.3

Hang, B. T., & Hanh, P. T. H. (2024). Vietnam – Striking a Balance between National Security and External Pressures. In *Data Governance and the Digital Economy in Asia* (hal. 111–128). Routledge. https://doi.org/10.4324/9781003505723-6

Holtz, J. N. (2025). Unpacking the Data Act: Between Regulatory Complexity and Digital Ambition.

In *Studies in National Governance and Emerging Technologies* (hal. 167–174). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-12140-0_6

Hukom, S., Humi, N., & Lukman, I. (2025). The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era. In *Hakim: Jurnal Ilmu Hukum dan Sosial* (Vol. 3, Nomor 1, hal. 974–992). Universitas Sains dan Teknologi Komputer. https://doi.org/10.51903/hakim.v3i1.2291

Hussein, S., & Serria, E. (2024). Understanding the Crucial Legal Implications of Edge and Fog Computing in Data Privacy and Security laws in the UAE. In *2024 IEEE Future Networks World Forum (FNWF)* (hal. 45–50). IEEE. https://doi.org/10.1109/fnwf63303.2024.11028775

Hustinx, P. (2023). Towards a Successful Cross-Border Regulatory Cooperation. In *Data Protection and Digital Sovereignty Post-Brexit* (hal. 199–208). Hart Publishing. https://doi.org/10.5040/9781509966516.ch-011

Jiang, Y., Yu, X., & Qin, Y. (2025). Unraveling the balance between personal data protection and public interest: a theoretical framework and its empirical application in personal data processing. In *Journal of Chinese Governance* (hal. 1–22). Informa UK Limited. https://doi.org/10.1080/23812346.2025.2518818

Jie, L., & Xiaojie, M. (2024). The Legal Response of Data Security Protection—From the Administrative Penalty Cases. In *Advance in Law* (Vol. 6, Nomor 2, hal. 101–112). Sciscan Publishing Limited. https://doi.org/10.35534/al.0602009

Junaidi, & Fadzil, R. M. (2024). Urgency of Legal Personal Data Protection in E-Commerce Transactions Involving Artificial Intelligence. In *Walisongo Law Review (Walrev)* (Vol. 6, Nomor 2, hal. 96–108). UIN Walisongo Semarang. https://doi.org/10.21580/walrev.2024.6.2.25548

Kalin, R. P. (2024). Towards Reconciling Digital Trade and Data Privacy. In *European Yearbook of International Economic Law* (hal. 287–316). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73857-9_6

Kamara, I. (2025). Two Worlds Converging in 2015. In *Standardizing Personal Data Protection* (hal. 1–22). Oxford University PressOxford. https://doi.org/10.1093/9780191997037.003.0001

Ketmaneechairat, H., Maliyaem, M., & Puttawattanakul, P. (2024). Towards a Management System Framework for the Integration of Personal Data Protection and Data Governance: A Case Study of Thai Laws and Practices. In *International Journal of Technology* (Vol. 15, Nomor 1, hal. 219). International Journal of Technology. https://doi.org/10.14716/ijtech.v15i1.5885

Khordadpour, P. (2023). *The Security of Data Governance in the Digital World*. Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.36227/techrxiv.22129160

Khuan, H. (2024). The Legal Protection of Personal Data in Fintech peer-to-peer (P2P) Lending Practices: Orientation and Formulation. In *Pena Justisia: Media Komunikasi dan Kajian Hukum* (Vol. 22, Nomor 3, hal. 433). Universitas Pekalongan. https://doi.org/10.31941/pj.v22i3.3383

Kolotylo, M. Y. (2025). THEORETICAL AND METHODOLOGICAL PRINCIPLES OF ADMINISTRATIVE AND LEGAL REGULATION OF PERSONAL DATA PROTECTION IN UKRAINE. In *Juridical scientific and electronic journal* (Nomor 2, hal. 243–248). Publishing House Helvetica (Publications). https://doi.org/10.32782/2524-0374/2025-2/57

Koumpli, C. (2023). Why is European protection of personal data not a legal limit to the development of artificial intelligence? In *Revista de Direitos Humanos e Desenvolvimento Social* (Vol. 5). Cadernos de Fe e Cultura, Oculum Ensaios, Reflexao, Revista de Ciencias Medicas e Revista de Educacao da PUC-Campinas. https://doi.org/10.24220/2675-9160v5a2024e9950

Kumar, D. (2025). The Right to Be Forgotten in the Digital Age: Challenges and Omissions in the Digital Personal Data Protection Act, 2023. In *International Journal of Innovative Research in*

Engineering & Multidisciplinary Physical Sciences (Vol. 13, Nomor 4). International Journal of Innovative Research in Engineering and Multidisciplinary Physical Sciences. https://doi.org/10.37082/ijirmps.v13.i4.232704

Leony, E., & Sendrawan, T. (2025). Wearable Technology in the Perspective of Personal Data Protection Law: A Comparative Study Between Indonesia and the European Union. In *Journal of Law and Regulation Governance* (Vol. 2, Nomor 12, hal. 359–371). Al Makki Publisher. https://doi.org/10.57185/jlarg.v2i12.78

López, P. (2025). The National Security Framework as a Cybersecurity Reference for Information Cryptosystems. In *Law, Governance and Technology Series* (hal. 125–144). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_6

Mahmood, B. A. A., & Siddiq, A. M. (2025). The legal protection of digital data privacy. In *International Journal of Civil Law and Legal Research* (Vol. 5, Nomor 2, hal. 129–136). AkiNik Publications. https://doi.org/10.22271/civillaw.2025.v5.i2b.152

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. In *Computer Law & Security Review* (Vol. 50, hal. 105849). Elsevier BV. https://doi.org/10.1016/j.clsr.2023.105849

Marelli, M. (2025). The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.5443854

Mushtaq, S., & Shah, M. (2025). Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? In *Computers* (Vol. 14, Nomor 6, hal. 219). MDPI AG. https://doi.org/10.3390/computers14060219

Neelakrishnan, P. (2024). Traditional Data Security. In *Autonomous Data Security* (hal. 41–86). Apress. https://doi.org/10.1007/979-8-8688-0838-8_2

Patil, D. (2024). Understanding the Personal Data Protection Act: Safeguarding Privacy in the Digital Age. In *Personal Data Protection In Digital Age: Issues And Challenges*. San International Scientific Publications. https://doi.org/10.59646/dataprotectionc7/125

Pistorius, T., & Jordaan, J.-J. (2024). The Regulation of Big Data: Data Governance beyond Data Protection. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.5018962

Putra, T. I., & Fibrianti, N. (2024). Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia. In *Lambung Mangkurat Law Journal* (Vol. 9, Nomor 1, hal. 64–74). Program Magister Kenotariatan Fakultas Hukum Universitas Lambung Mangkurat. https://doi.org/10.32801/abc.v9i1.159

Rodríguez-Doncel, V. (2025). Web Technologies for Decentralised Identity. In *Law, Governance and Technology Series* (hal. 111–124). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_5

Sari, R. K., Purwoleksono, D. E., & Paripurna, A. (2023). THE LEGAL CERTAINTY ON CHILDREN'S PERSONAL DATA: REALIZING LEGAL PROTECTION ON SOCIAL MEDIA. In *Syiah Kuala Law Journal* (Vol. 7, Nomor 2, hal. 130–140). LPPM Universitas Syiah Kuala. https://doi.org/10.24815/sklj.v7i2.32557

Sempere, C. P. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. In *Law, Governance and Technology Series* (hal. 3–21). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74889-9_1

Shukla, P. (2025). THE REGULATORY CONUNDRUM: A MULTIDIMENSIONAL ANALYSIS

OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, AND ITS IMPLICATIONS FOR INDIAN STARTUPS. In *LawFoyer International Journal of Doctrinal Legal Research* (Vol. 3, Nomor 2, hal. 947–958). LawFoyer International Journal of Doctrinal Legal Research. https://doi.org/10.70183/lijdlr.2025.v03.78

Skorokhod, O. V. (2024). Using blockchain in public administration and personal data protection. In *Al'manah prava* (Nomor 15, hal. 608–612). Koretsky Institute of State and Law of National Academy of Sciences of Ukraine. https://doi.org/10.33663/2524-017x-2024-15-608-612

Sulthanah, L. T., & Rasji, R. (2025). The Urgency of Establishing a Personal Data Protection Agency in Indonesia (Adopting the South Korean Personal Data Protection Agency Model). In *Law Development Journal* (Vol. 7, Nomor 4, hal. 675). Universitas Islam Sultan Agung. https://doi.org/10.30659/ldj.7.4.675-687

Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. In *Journal of Human Rights, Culture and Legal System* (Vol. 3, Nomor 1, hal. 33–69). Lembaga Contrarius Indonesia. https://doi.org/10.53955/jhcls.v3i1.71

Suvorov, A. (2025). *The Pointer-Based Security Paradigm: Architectural Shift from Data Protection to Data Non-Existence*. Elsevier BV. https://doi.org/10.2139/ssrn.5526998

Suwondo, D. (2023). The Legal Protection of Personal Data in Islamic Perspective. In *International Journal of Law Reconstruction* (Vol. 7, Nomor 2, hal. 221). Program Doktor Ilmu Hukum Unissula. https://doi.org/10.26532/ijlr.v7i2.33648

Syifa, S. N., Abdillah, M. T., & SJ, F. (2025). The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak. In *Justicia Islamica* (Vol. 22, Nomor 1, hal. 185–210). STAIN Ponorogo. https://doi.org/10.21154/justicia.v22i1.10390

Tassinari, F. (2024). The Processing of Personal Data within the European Union's Large-Scale IT Systems. In *Data Protection and Interoperability in EU External Relations* (hal. 189–301). Brill | Nijhoff. https://doi.org/10.1163/9789004684027_006

Taufiq, M., Kurniawan, M. R., & Kenyo, A. S. (2025). The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR. In *International Journal of Business, Law, and Education* (Vol. 6, Nomor 2, hal. 1260–1268). Scientific Publications Community Inc. https://doi.org/10.56442/ijble.v6i2.1178

Tullio, M. F. De. (2025). Which Data Governance for a Social Post-pandemic Recovery? In *A Digital Europe for Citizens* (hal. 95–112). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-02500-5_6

ugiantari, A. A. P. W. S. (2025). Unfolding Data Protection Officer Regulation in Personal Data Protection: Evidence Malaysia. In *Pakistan Journal of Life and Social Sciences (PJLSS)* (Vol. 23, Nomor 1). Elite Scientific Forum. https://doi.org/10.57239/pjlss-2025-23.1.0062

Vasić, M. (2025). The legal-regulatory gap in data protection between the European Union and the United States of America: Challenges and implications. In *Pravo - teorija i praksa* (Vol. 42, Nomor 2, hal. 143–161). Centre for Evaluation in Education and Science (CEON/CEES). https://doi.org/10.5937/ptp2502143v

Viana, P. P. (2025). The Retention, Access and Re-Use of Communications Data: An Unbreakable Legal Chain? In *European Data Protection Law Review* (Vol. 10, Nomor 4, hal. 401–408). Lexxion Verlag. https://doi.org/10.21552/edpl/2024/4/12

Vigil, R. P. (2024). Towards a Serious Game to Promote Personal Data Protection among Secondary School Students. In *Avances en Interacción Humano-Computadora* (Vol. 9, Nomor 1, hal. 265–267). Asociacion Mexicana de Interaccion humano-Computadora (AMexIHC). https://doi.org/10.47756/aihc.y9i1.182

Wachdin, S. Z. S., Adytia, N. A. P., & Said, S. (2024). The Legal Framework for Personal Data Protection in the Digital Era as Fulfillment of Privacy Rights in Indonesia. In *KnE Social Sciences*. Knowledge E DMCC. https://doi.org/10.18502/kss.v8i21.14785

Wandhöfer, R., & Nakib, H. D. (2023). The Regulatory Dimension of Data Protection, Privacy and AI. In *Redecentralisation* (hal. 159–178). Springer International Publishing. https://doi.org/10.1007/978-3-031-21591-9_7

Weng, Y. (2025). User data privacy protection model based on federated reinforcement learning optimization method. In *Journal of Cyber Security Technology* (hal. 1–22). Informa UK Limited. https://doi.org/10.1080/23742917.2024.2448355

Wilkinson, S. (2023). UK data protection and digital information bill explained. In *Journal of Data Protection & Privacy* (Vol. 5, Nomor 3, hal. 242). Henry Stewart Publications. https://doi.org/10.69554/yvow7196

Xinyu, Z. (2025). The Legal Protection of Personal Financial Information Rights: A Core Analysis of Data Ownership and Utilization Rules. In *Journal of Economics and Law* (Vol. 2, Nomor 5, hal. 214–219). STEMM Institute Press. https://doi.org/10.62517/jel.202514528

Zawal, M. (2025). The Synergy Between European Union Data Protection and Digital Market Regulation. In *Zeszyt Prawniczy UAM* (Nomor 15, hal. 113–122). Adam Mickiewicz University Poznan. https://doi.org/10.14746/zpuam.2025.15.9

Zeng, S., Jin, W., & Sun, T. (2025). *The Value of Data in the Digital Economy: Investigating the Economic Consequences of Personal Information Protection*. Elsevier BV. https://doi.org/10.2139/ssrn.5147162

Zhang, L., & Kollnig, K. (2023). Theory and practice: the protection of children's personal information in China. In *International Data Privacy Law* (Vol. 14, Nomor 1, hal. 37–52). Oxford University Press (OUP). https://doi.org/10.1093/idpl/ipad017

Zyubanov, K. (2023). The Scope of the Personal Data Concept in Russia. In *Legal Issues in the Digital Age* (Vol. 4, Nomor 1, hal. 53–76). National Research University, Higher School of Economics (HSE). https://doi.org/10.17323/2713-2749.2023.1.53.76

)2025. (م. ش, راضي. The right to the protection of personal data under the Constitution of the Republic of Iraq for the year 2005. In *Imam Ja'afar Al-Sadiq University Journal of Legal Studies* (Vol. 2, Nomor 2). Imam Ja'afar Al-Sadiq University. https://doi.org/10.64682/3104-9419.1048