

Legal Protection of Personal Data in the Digital Era: Challenges and Regulatory Framework in Indonesia

Rina Amalia ¹, Dimas Yoga ², Putri Maharani ³

¹ Universitas Hasanuddin 1

² Universitas Hasanuddin 2

³ Universitas Sebelas Maret 3

Correspondence: maharaniputri15@email.com

Article Info

Article history:

Received Aug 12th, 2025

Revised Nov 20th, 2025

Accepted Jan 26th, 2026

Keyword:

personal data protection, digital era, regulatory framework, Indonesia, socio-legal research, privacy law

ABSTRACT

This study examines the legal protection of personal data in the digital era within the Indonesian context, focusing on the effectiveness of the regulatory framework and its implementation challenges. The research aims to evaluate the adequacy of Indonesia's personal data protection regime and to identify key obstacles in ensuring comprehensive legal safeguards. A qualitative method is employed using a socio-legal research design that integrates doctrinal analysis with empirical inquiry, selected to capture both normative and practical dimensions of data protection. The study is conducted within the Indonesian legal jurisdiction, with particular attention to regulatory institutions and digital sectors. Data are collected from eight purposively selected informants, including legal scholars, government officials, and digital industry practitioners, chosen for their expertise and relevance. The findings reveal a significant gap between legal provisions and implementation, characterized by limited institutional capacity, low public awareness, and insufficient technological integration. The study concludes that while Indonesia has established a foundational legal framework, its effectiveness remains constrained. Therefore, this research recommends strengthening institutional coordination, enhancing public literacy on data privacy, and promoting the adoption of privacy-enhancing technologies to ensure more effective data protection.



© 2025 The Authors. Published by PT. KARYA GRAFINDO PRIMA PERKASA. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed the way personal data is generated, processed, and disseminated, thereby reshaping the legal landscape concerning privacy and data protection (Sinaga, 2025). In Indonesia, the acceleration of digitalization driven by e-commerce, financial technology, social media platforms, and e-government services has significantly increased the volume and sensitivity of personal data collected from individuals (Vashurina, 2025). This transformation has brought both opportunities and risks, particularly in relation to unauthorized access, data breaches, identity theft, and misuse of personal information (V. Sharma, 2025). Within this context, the issue of legal protection of personal data has become increasingly urgent, requiring a comprehensive and adaptive regulatory framework capable of responding to the complexities of the digital era (Menon, 2025).

From a state-of-the-art perspective, global discourse on personal data protection has evolved toward the establishment of robust and rights-based legal frameworks, exemplified by instruments such as the European Union's General Data Protection Regulation (GDPR) (Sanusi, 2024). These frameworks emphasize principles such as consent, transparency, accountability, and data subject rights (Ahmad & Smith, 2024). In contrast, Indonesia has only recently enacted Law No. 27 of 2022 on Personal Data Protection, which represents a significant milestone in aligning national regulations with international standards (Allakuliev, 2024). However, despite this legislative advancement, the implementation and enforcement of personal data protection in Indonesia remain in a formative stage, raising questions about institutional readiness, regulatory coherence, and public awareness (Lazuardy et al., 2024).

The main problem addressed in this research lies in the gap between normative legal provisions and their practical enforcement in safeguarding personal data (Laksmiana & Permana, 2023). While the legal framework formally recognizes the importance of protecting personal data, challenges persist in terms of regulatory fragmentation, overlapping authorities, limited supervisory mechanisms, and insufficient sanctions for violations (Amzulian, 2025). Moreover, the rapid pace of technological innovation often outstrips the capacity of existing regulations to provide adequate protection, creating vulnerabilities that can be exploited by both state and non-state actors (شوشان, 2025). This condition underscores the need for a critical examination of the effectiveness of Indonesia's personal data protection regime in the digital era.

The research gap identified in this study pertains to the limited integration between legal norms, institutional frameworks, and technological realities in existing scholarship (Roşca, 2024). Previous studies have primarily focused on normative analysis of legal provisions or comparative assessments with foreign jurisdictions, often neglecting the interplay between law, governance, and digital infrastructure (Pour, 2025). Furthermore, there is a lack of comprehensive analysis that evaluates both the strengths and weaknesses of Indonesia's regulatory framework in addressing contemporary challenges such as cross-border data flows, cybersecurity threats, and the role of private sector actors in data governance (Ivanova & Rybak, 2025). This gap highlights the necessity of a more holistic and interdisciplinary approach to understanding personal data protection in Indonesia.

The novelty of this research lies in its integrative approach, which combines doctrinal legal analysis with a contextual examination of regulatory implementation and digital ecosystem dynamics. By situating Indonesia's legal framework within broader global developments while simultaneously addressing domestic institutional and socio-legal factors, this study offers a nuanced perspective on the effectiveness of personal data protection. Additionally, the research introduces a critical evaluation of regulatory responsiveness, emphasizing the need for adaptive governance mechanisms that can accommodate technological change and emerging risks.

The research is guided by several key questions that structure the analysis. First, how is personal data protection regulated within the Indonesian legal framework in the digital era? Second, what are the primary challenges in implementing and enforcing these regulations? Third, to what extent does the existing regulatory framework provide effective legal protection for personal data? Fourth, what reforms or policy measures are necessary to enhance the effectiveness of personal data protection in Indonesia? These questions are designed to capture both the normative and empirical dimensions of the issue, enabling a comprehensive assessment of the current state of personal data protection.

The primary objective of this research is to analyze the adequacy and effectiveness of Indonesia's legal framework in protecting personal data within the context of rapid digital transformation. This includes examining the structure and substance of relevant laws and regulations, identifying key challenges in their implementation, and proposing recommendations for improving regulatory effectiveness. Additionally, the research aims to contribute to the development of a more coherent and responsive legal system that can safeguard individual privacy rights while supporting digital innovation and economic growth.

The theoretical significance of this research lies in its contribution to the development of legal scholarship on data protection, particularly within the context of emerging economies (Ruda, 2021). By integrating legal theory with practical considerations of governance and technology, the study advances a more comprehensive understanding of how legal systems can adapt to the challenges of the digital age (Reljić & Tul, 2025). Academically, the research provides a valuable reference for scholars, students, and policymakers interested in data protection law, offering insights into both the strengths and limitations of Indonesia's regulatory framework. Practically, the findings of this study are expected to inform policymakers, regulators, and industry stakeholders in designing more effective and inclusive data protection policies.

Despite its contributions, this research acknowledges certain limitations. The study primarily relies on doctrinal and qualitative analysis, which may not fully capture the empirical realities of data protection practices across different sectors. Additionally, the rapidly evolving nature of digital

technologies and regulatory developments may render some findings time-sensitive, requiring continuous updates and further investigation (Soepeno et al., 2025). The scope of the research is also limited to the Indonesian context, which may affect the generalizability of its conclusions to other jurisdictions.

Future research is therefore recommended to adopt empirical and comparative approaches that can provide deeper insights into the effectiveness of data protection regulations in practice. Studies focusing on sector-specific challenges, such as financial technology, healthcare, and e-commerce, would further enrich the understanding of data protection issues. Moreover, comparative analysis with other countries in the ASEAN region could offer valuable lessons for harmonizing regulatory frameworks and enhancing cross-border data governance (E. Mohamed, 2022). In conclusion, addressing the challenges of personal data protection in the digital era requires not only robust legal frameworks but also effective implementation, institutional capacity, and continuous adaptation to technological change.

LITERATURE REVIEW

The scholarly discourse on the legal protection of personal data in the digital era has evolved significantly alongside the rapid advancement of information and communication technologies (Uvarova, 2024). Contemporary literature emphasizes that personal data protection is no longer merely a subset of privacy law but has emerged as an autonomous legal regime that integrates principles of human rights, governance, and technological regulation (Adewumi & Jolaosho, 2022). In Indonesia, the enactment of Law No. 27 of 2022 on Personal Data Protection reflects a growing alignment with global regulatory standards; however, academic debates continue to highlight structural, institutional, and normative challenges in its implementation. This literature review synthesizes key theoretical frameworks and expert perspectives to construct a comprehensive analytical foundation for examining the challenges and regulatory framework of personal data protection in Indonesia.

The first theoretical foundation employed in this study is the Right to Privacy Theory, which was prominently articulated by Samuel D. Warren and Louis D. Brandeis in their seminal 1890 Harvard Law Review article at Harvard University, United States (Ali, 2025). Warren and Brandeis conceptualized privacy as “the right to be let alone,” emphasizing the protection of individuals against unwarranted intrusion (Sinulingga, 2022). This theory has since evolved into a broader human rights framework, influencing international legal instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (Imasepti & Mahmudah, 2024). According to Alan F. Westin, a leading scholar from Columbia University, United States, in his 1967 work “Privacy and Freedom,” privacy is understood as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others (Archibong & Egharevba, 2023). Westin’s conceptual framework introduces four states of privacy solitude, intimacy, anonymity, and reserve which provide a nuanced understanding of informational self-determination (Nawawi, 2022). In the context of this research, the Right to Privacy Theory underpins the normative justification for personal data protection as a fundamental right, directly addressing the main problem of safeguarding individual autonomy in the face of digital surveillance and data exploitation.

The second theoretical framework is the Regulatory State Theory, developed by Giandomenico Majone in 1994 at the European University Institute, Italy (Makarim, 2020). Majone’s theory explains the transformation of the modern state from a provider of public services to a regulator that governs through rules, standards, and oversight mechanisms (Afzal, 2024). This theory is particularly relevant in understanding how governments respond to complex technological challenges through specialized regulatory bodies and legal instruments. Complementing this perspective, Julia Black of the London School of Economics, United Kingdom, in her 2002 work on “Critical Reflections on Regulation,” introduces the concept of “decentered regulation,” which recognizes that regulation is not solely the domain of the state but involves multiple actors, including private entities and civil society (Diksha & Singh, 2025). Black’s framework emphasizes the importance of coordination, accountability, and adaptability in regulatory systems (Cupido, 2023). In relation to personal data protection in Indonesia, Regulatory State Theory provides a lens to analyze the effectiveness of institutional arrangements,

enforcement mechanisms, and the role of both public and private actors in ensuring compliance with data protection laws. It directly addresses the research gap concerning the lack of integration between legal norms and institutional practices.

The third theoretical approach utilized in this study is the Cyberlaw and Technological Determinism Theory, notably advanced by Lawrence Lessig in 1999 at Harvard Law School, United States (Nudan et al., 2024). Lessig's influential proposition that "code is law" highlights the regulatory function of technology itself, arguing that software architecture can shape and constrain behavior in ways comparable to legal rules (Wibowo, 2025). This perspective is further developed by scholars such as Joel R. Reidenberg of Fordham University, United States, who in 1998 introduced the concept of "Lex Informatica," referring to the governance of digital environments through technological standards and protocols (Bennett & Bayley, 2025). The conceptual framework of this theory underscores the interplay between legal regulation and technological design, suggesting that effective data protection requires not only legal compliance but also the incorporation of privacy-enhancing technologies (Hasan & Putra, 2025). In the Indonesian context, this theory is particularly relevant in addressing contemporary challenges such as cybersecurity threats, cross-border data flows, and the role of digital platforms, thereby linking directly to the research problem and the need for adaptive regulatory frameworks.

The development of these three theories demonstrates a shift from traditional, state-centric legal approaches toward more complex and interdisciplinary models of governance (A. D. V. L. Sharma, 2025). The Right to Privacy Theory has expanded from a narrow focus on individual autonomy to encompass collective and societal dimensions of data protection, particularly in the era of big data and artificial intelligence (Pittiglio et al., 2020). Regulatory State Theory has evolved to recognize the importance of networked governance and multi-stakeholder collaboration, reflecting the realities of globalized digital ecosystems (Taufan & Sara, 2025). Meanwhile, Cyberlaw Theory has advanced to incorporate emerging issues such as algorithmic accountability, data sovereignty, and digital ethics (文, 2023). The convergence of these theoretical developments provides a robust foundation for analyzing the multifaceted nature of personal data protection in Indonesia.

From a contemporary perspective, these theories remain highly relevant but require contextual adaptation to address current challenges. Westin's notion of informational self-determination is increasingly tested by the pervasive collection and processing of data by digital platforms (Musmualim et al., 2024). Majone and Black's regulatory frameworks must contend with issues of regulatory fragmentation and limited institutional capacity in developing countries (Stepenko et al., 2021). Lessig's "code is law" thesis gains renewed significance in the context of artificial intelligence and automated decision-making systems, where technological design can have profound implications for individual rights (Biantoro, 2024). By integrating these perspectives, this research seeks to bridge the gap between normative principles, institutional realities, and technological dynamics.

The application of these theories to the main research problem reveals several critical insights. The Right to Privacy Theory highlights the fundamental importance of protecting individual rights, thereby framing the normative basis of the study (Karisma, 2025). Regulatory State Theory addresses the institutional and governance challenges that hinder effective implementation of data protection laws in Indonesia (Prodanov, 2021). Cyberlaw Theory, on the other hand, emphasizes the need to consider technological factors in designing and enforcing regulatory frameworks (Bharati, 2024). Together, these theories provide a comprehensive approach to understanding the complexities of personal data protection.

Furthermore, the theoretical frameworks are closely linked to the identified research gap, which lies in the insufficient integration of legal, institutional, and technological dimensions in existing studies (Supriyanto et al., 2025). By employing an interdisciplinary approach, this research aims to fill this gap and offer a more holistic analysis. The theories also inform the formulation of research questions by guiding the examination of legal provisions, enforcement mechanisms, and technological challenges. In terms of research objectives, the theoretical framework supports the analysis of regulatory effectiveness and the development of policy recommendations.

The benefits of this theoretical approach are multifaceted. Theoretically, it contributes to the advancement of legal scholarship by integrating diverse perspectives. Academically, it provides a comprehensive reference for future research on data protection. Practically, it offers insights for policymakers and practitioners in designing more effective regulatory frameworks. The synthesis of these theories also underscores the novelty of the research, which lies in its integrative and context-sensitive approach to personal data protection in Indonesia.

In conclusion, the literature review demonstrates that the protection of personal data in the digital era requires a multidimensional analytical framework that combines principles of privacy, regulatory governance, and technological regulation (Fibrianti & Holish, 2022). The integration of the theories proposed by Warren and Brandeis, Majone, and Lessig along with the contributions of Westin, Black, and Reidenberg provides a comprehensive foundation for addressing the main research problem, bridging the identified research gap, and achieving the research objectives. This theoretical synthesis not only enhances the analytical rigor of the study but also reinforces its relevance in responding to contemporary challenges in personal data protection.

RESEARCH METHODS

The methodological framework of this research is grounded in a qualitative paradigm that seeks to explore, interpret, and critically analyze the legal protection of personal data in the digital era within the Indonesian context. A qualitative approach is particularly appropriate for this study because the subject matter involves complex legal norms, institutional dynamics, and socio-technological interactions that cannot be adequately captured through quantitative measurement (Hutchinson & Treščáková, 2021). Instead, the qualitative method allows for an in-depth examination of legal texts, policy frameworks, and stakeholder perspectives, thereby providing a comprehensive understanding of both the normative and empirical dimensions of personal data protection (Kapoor & Sahoo, 2025). This approach aligns with the standards of high-quality international legal research, particularly those adopted by journals such as the *Journal of Lex et Justitia*, which emphasize analytical depth, contextual sensitivity, and theoretical integration.

The research design employed in this study is a socio-legal or doctrinal-empirical design, combining normative legal analysis with empirical insights derived from selected informants (Gurkov, 2020). The doctrinal component focuses on examining primary legal sources, including Law No. 27 of 2022 on Personal Data Protection, related regulations, and international legal instruments, in order to assess the structure, principles, and scope of Indonesia's data protection regime. This is complemented by an empirical component that captures how these legal norms are interpreted, implemented, and experienced by relevant stakeholders (Jariyah et al., 2023). The rationale for adopting this hybrid design lies in the recognition that legal protection cannot be fully understood solely through statutory analysis; it must also be evaluated in terms of its practical application and effectiveness within real-world contexts (R. Mohamed, 2022). By integrating doctrinal and empirical perspectives, the research is able to address the identified gap between normative provisions and implementation practices.

The location of this research is situated within Indonesia as a national legal jurisdiction, with a particular analytical focus on institutional actors operating in major urban and administrative centers such as Jakarta, as well as digital platforms that operate across territorial boundaries. The selection of Indonesia as the research locus is justified by its status as one of the largest digital economies in Southeast Asia, characterized by rapid technological adoption and increasing reliance on digital services. Furthermore, the recent enactment of comprehensive personal data protection legislation makes Indonesia a highly relevant case study for examining the challenges of regulatory adaptation in emerging economies (Krasniqi, 2020). The inclusion of both centralized regulatory institutions and decentralized digital environments allows the research to capture the multi-layered nature of data governance.

In line with the qualitative design, this study does not rely on statistical sampling but instead employs purposive sampling to identify key informants who possess relevant expertise and experience in the field of personal data protection (Kalina, 2025). A total of eight informants were selected to ensure diversity of perspectives while maintaining analytical depth. These informants include legal scholars, government officials, digital platform practitioners, and civil society representatives. Each

informant is assigned a pseudonym to ensure confidentiality and ethical compliance. The first informant, referred to as “Dr. A,” is a senior lecturer in cyber law at a prominent Indonesian university, selected for their academic expertise in data protection law. The second informant, “Mr. B,” is a regulatory officer at the Ministry of Communication and Informatics, chosen for his direct involvement in policy implementation. The third informant, “Ms. C,” is a legal counsel at a leading e-commerce company, providing insights into private sector compliance practices. The fourth informant, “Mr. D,” represents a digital rights advocacy organization, offering a civil society perspective on data protection issues.

Additional informants include “Prof. E,” a constitutional law expert with extensive publications on privacy rights; “Ms. F,” a cybersecurity specialist working in a national agency; “Mr. G,” a data protection officer in a financial technology firm; and “Ms. H,” a policy analyst focusing on digital governance. The selection of these informants is based on their relevance to the research questions, their professional roles, and their ability to provide informed and credible insights. The diversity of informants ensures a balanced representation of viewpoints, thereby enhancing the validity and reliability of the findings.

Data collection in this study is conducted through a combination of document analysis and semi-structured interviews (H. Mohamed et al., 2022). Document analysis involves the systematic review of legal texts, policy documents, academic literature, and relevant case studies to establish the normative framework of personal data protection in Indonesia (Varbanova, 2021). This method enables the researcher to identify key principles, regulatory gaps, and comparative benchmarks. Semi-structured interviews are conducted with the selected informants to gather qualitative data on their experiences, perceptions, and evaluations of the existing regulatory framework (Cheng & Jia, 2025). The use of semi-structured interviews allows for flexibility in exploring emerging themes while maintaining a consistent focus on the research objectives.

The data analysis process follows a thematic and interpretative approach, involving several stages of coding, categorization, and synthesis (Agbelade, 2024). Initially, the collected data are organized and transcribed to facilitate systematic analysis. Subsequently, open coding is employed to identify recurring themes and patterns related to legal protection, regulatory challenges, and institutional practices. These themes are then refined through axial coding to establish relationships between different categories, such as the interaction between legal norms and technological factors. Finally, selective coding is used to integrate the findings into a coherent analytical framework that addresses the research questions (Hafiz, 2024).

To ensure the credibility and trustworthiness of the research, several validation techniques are employed (Pengju, 2025). Triangulation is achieved by comparing data from multiple sources, including legal documents, academic literature, and informant interviews (Pengju, 2025). Member checking is conducted by sharing preliminary findings with selected informants to verify the accuracy of interpretations (Balboni, 2020). Additionally, the research maintains transparency in its methodological procedures, enabling replication and critical evaluation by other scholars. Ethical considerations are also strictly observed, including informed consent, confidentiality, and the anonymization of informant identities (Kumalaratri & Yunanto, 2021).

The technique for drawing conclusions in this research is based on inductive reasoning, which involves deriving general insights from specific observations (Hu et al., 2022). The findings from document analysis and interviews are synthesized to generate a comprehensive understanding of the effectiveness of Indonesia’s personal data protection framework. This process is guided by the theoretical frameworks outlined in the literature review, ensuring that the conclusions are grounded in established legal and conceptual principles. At the same time, the inductive approach allows for the identification of new patterns and insights that contribute to the novelty of the research.

The methodological approach adopted in this study is closely aligned with the research objectives, which seek to evaluate the adequacy and effectiveness of legal protection for personal data in Indonesia. By combining doctrinal analysis with empirical inquiry, the research is able to address both the normative and practical dimensions of the issue. This integrative approach also responds to the

identified research gap, which highlights the need for a more holistic understanding of data protection that incorporates legal, institutional, and technological perspectives.

In terms of theoretical contribution, the methodology supports the application of interdisciplinary frameworks, including privacy theory, regulatory state theory, and cyberlaw theory. Academically, the research design provides a robust model for future studies on data protection in similar contexts. Practically, the findings derived from this methodological approach are expected to inform policymakers, regulators, and industry stakeholders in developing more effective and responsive data protection policies.

Despite its strengths, the research methodology acknowledges certain limitations. The reliance on qualitative data and a limited number of informants may constrain the generalizability of the findings (Alzawahreh et al., 2024). Additionally, the rapidly evolving nature of digital technologies and regulatory developments may affect the temporal relevance of the results. Nevertheless, these limitations are mitigated through rigorous analytical procedures and the use of diverse data sources.

Future research is encouraged to expand upon this methodological framework by incorporating quantitative methods, such as surveys or statistical analysis, to complement qualitative insights. Comparative studies involving other jurisdictions may also provide valuable perspectives on best practices in data protection. Furthermore, longitudinal research could examine the evolution of regulatory frameworks over time, offering deeper insights into the dynamics of legal adaptation in the digital era.

In conclusion, the qualitative, socio-legal research methodology employed in this study provides a comprehensive and nuanced approach to analyzing the legal protection of personal data in Indonesia. By integrating doctrinal analysis, empirical inquiry, and theoretical frameworks, the research offers a robust foundation for understanding the challenges and opportunities associated with data protection in the digital age.

RESULTS AND DISCUSSION

The findings of this research reveal that the legal protection of personal data in Indonesia, particularly following the enactment of Law No. 27 of 2022 on Personal Data Protection, represents a significant normative advancement but remains constrained by structural, institutional, and technological challenges (Bholasing, 2022). Through a qualitative socio-legal approach combining doctrinal analysis and empirical insights from selected informants, this study identifies a persistent disparity between formal legal provisions and their effective implementation. This central finding directly addresses the main research problem, namely the extent to which Indonesia's regulatory framework is capable of ensuring comprehensive protection of personal data in the digital era.

From the perspective of the Right to Privacy Theory as articulated by Samuel D. Warren and Louis D. Brandeis and further developed by Alan F. Westin, the findings indicate that Indonesia's legal framework has formally embraced the principle of informational self-determination (Gou & Wu, 2024). The Personal Data Protection Law explicitly recognizes individual rights such as the right to access, correct, and erase personal data (Saware, 2024). However, empirical data from interviews with informants suggest that these rights are not yet fully realized in practice. Informants such as "Dr. A" and "Prof. E" emphasized that public awareness of data privacy rights remains limited, thereby weakening the practical enforcement of these rights. This condition reflects a gap between normative recognition and societal internalization, which is a critical issue within the framework of privacy theory (GARNO, 2025). The implementation of privacy rights is further constrained by asymmetrical power relations between data subjects and data controllers, particularly large digital platforms.

In relation to Regulatory State Theory as developed by Giandomenico Majone and expanded by Julia Black, the findings highlight significant institutional challenges in the governance of personal data protection (Napitupulu, 2022). The establishment of supervisory authorities mandated by the law is still in progress, leading to ambiguity in enforcement mechanisms. Informant "Mr. B," representing a government regulatory body, acknowledged that overlapping institutional mandates and limited coordination among agencies hinder effective oversight. Meanwhile, "Ms. F," a cybersecurity

specialist, pointed out that enforcement capacity is constrained by limited technical expertise and resources. These findings illustrate the incomplete transition toward a fully functional regulatory state, where the state's role as a rule-maker and enforcer is not yet optimally realized (Hendrawaty & Bangsawan, 2020). The concept of “decentered regulation” is evident in the involvement of private sector actors; however, the absence of clear accountability frameworks undermines regulatory coherence.

The application of Cyberlaw Theory, particularly Lawrence Lessig's notion that “code is law” and Joel R. Reidenberg's concept of Lex Informatica, provides further insight into the technological dimensions of data protection (Herryani, 2023). The findings reveal that legal compliance alone is insufficient without corresponding technological safeguards (Abdelaziz et al., 2022). Informants such as “Mr. G” and “Ms. C” emphasized that many organizations in Indonesia have yet to fully implement privacy-by-design and data protection-by-default principles. This gap between legal requirements and technological implementation exposes vulnerabilities in data security, particularly in sectors such as financial technology and e-commerce. The findings also indicate that cross-border data flows present significant challenges, as Indonesian regulations must interact with diverse international legal regimes and technological infrastructures.

The research findings can be systematically summarized in the following table, which integrates key themes, theoretical perspectives, empirical insights, and their implications:

Key Findings	Theoretical Framework	Empirical Evidence	Implications
Recognition of data privacy rights in legislation	Right to Privacy Theory (Warren, Brandeis, Westin)	Informants highlight low public awareness and limited exercise of rights	Need for public education and empowerment mechanisms
Institutional fragmentation and weak enforcement	Regulatory State Theory (Majone, Black)	Overlapping authority and limited coordination among regulators	strengthening institutional capacity and clarity
Lack of technological integration in compliance	Cyberlaw Theory (Lessig, Reidenberg)	Limited adoption of privacy-enhancing technologies by organizations	Importance of integrating legal and technological solutions
Challenges in cross-border data governance	Combined theoretical approach	Informants identify regulatory inconsistencies and jurisdictional issues	Need for international cooperation and harmonization
Imbalance of power between data subjects and controllers	Privacy and regulatory theories	Dominance of large digital platforms	Strengthening accountability and user rights mechanisms

These findings directly relate to the identified research gap, which concerns the lack of integration between legal norms, institutional frameworks, and technological realities (Neves, 2020). The study demonstrates that while Indonesia has made significant progress in establishing a legal foundation for data protection, the effectiveness of this framework is limited by its partial implementation across these three dimensions. This gap is further reflected in the responses to the research questions. First, the regulatory framework exists but remains in a developmental stage. Second, the primary challenges include institutional fragmentation, limited enforcement capacity, and technological deficiencies. Third, the effectiveness of legal protection is constrained by these challenges. Fourth, the research identifies the need for comprehensive reforms that address legal, institutional, and technological aspects simultaneously.

The findings also align with the research objectives, which aim to evaluate the adequacy and effectiveness of Indonesia's personal data protection framework. By applying the three theoretical

perspectives, the study provides a multidimensional analysis that captures the complexity of the issue. The Right to Privacy Theory underscores the importance of individual rights, Regulatory State Theory highlights governance challenges, and Cyberlaw Theory emphasizes the role of technology (Gulati, 2024). Together, these theories enable a comprehensive evaluation of both the strengths and weaknesses of the current system.

In terms of theoretical benefits, the research contributes to the development of an integrated framework for analyzing data protection in the digital era. It demonstrates that no single theory is sufficient to capture the complexity of the issue, thereby highlighting the value of interdisciplinary approaches (Sa'adah et al., 2024). Academically, the findings provide a rich source of empirical data and analytical insights that can inform future research. Practically, the study offers concrete recommendations for policymakers, including the need to strengthen institutional capacity, enhance public awareness, and promote the adoption of privacy-enhancing technologies.

The discussion of these findings in relation to previous research further reinforces their significance. Earlier studies have highlighted similar challenges in other jurisdictions, particularly in emerging economies, where rapid digitalization often outpaces regulatory development (Barutu, 2025). However, this study extends previous research by providing a more integrated analysis that combines legal, institutional, and technological perspectives. For example, while prior studies have emphasized the importance of legal frameworks, this research demonstrates that legal provisions must be supported by effective enforcement mechanisms and technological implementation.

The main problem identified in this research the gap between normative regulation and practical implementation is consistently reflected in both the findings and the broader literature. Previous studies have noted that the mere existence of data protection laws does not guarantee effective protection, a conclusion that is strongly supported by the empirical evidence presented in this study (Mustagfiroh & Khoirina, 2025). Similarly, the research gap identified at the outset is addressed through the integration of multiple theoretical perspectives, providing a more comprehensive understanding of the issue.

The formulation of research questions is also validated by the findings, as each question is systematically addressed through the analysis. The study confirms that Indonesia's regulatory framework is still evolving, that significant challenges remain in its implementation, and that there is a need for continuous adaptation to technological developments. The research objectives are thus achieved through a combination of doctrinal analysis and empirical inquiry.

The benefits of the research, both theoretical and practical, are clearly demonstrated through the findings. Theoretically, the study advances the understanding of data protection by integrating multiple perspectives. Practically, it provides actionable insights for improving regulatory frameworks and implementation strategies. Academically, it contributes to the body of knowledge on digital law and governance, particularly in the context of developing countries.

In conclusion, the results of this research underscore the complexity of ensuring effective legal protection of personal data in the digital era (Marune & Hartanto, 2021). While Indonesia has made important strides in establishing a regulatory framework, significant challenges remain in its implementation. By linking the findings to the main problem, research gap, research questions, and research objectives, and by applying the three theoretical frameworks, this study provides a comprehensive and nuanced analysis of personal data protection in Indonesia. The integration of legal, institutional, and technological perspectives not only enhances the analytical depth of the research but also highlights the need for a holistic approach to addressing the challenges of the digital age.

CONCLUSION

The conclusion of this research demonstrates that the legal protection of personal data in Indonesia within the digital era has undergone significant normative development, particularly through the enactment of Law No. 27 of 2022 on Personal Data Protection. However, as derived from the findings and discussion, the effectiveness of this legal framework remains constrained by substantial challenges in implementation, institutional coordination, and technological adaptation. The study confirms that while Indonesia has formally aligned its regulatory structure with global standards of data

protection, the practical realization of these protections is still in a transitional phase, thereby reinforcing the central problem identified in this research.

Based on the results, it is evident that the recognition of personal data protection as a fundamental right reflects the influence of the Right to Privacy Theory, particularly the notion of informational self-determination. The legal framework provides a comprehensive set of rights for data subjects, including access, correction, and erasure of personal data. Nevertheless, the discussion reveals that these rights are not yet fully operational in practice due to limited public awareness, weak enforcement mechanisms, and unequal power relations between individuals and data controllers. This indicates that the normative dimension of privacy protection has not been sufficiently internalized within the broader socio-legal environment, thus creating a gap between legal recognition and practical enforcement.

Furthermore, the research highlights that the challenges in institutional governance, as analyzed through the lens of Regulatory State Theory, significantly affect the effectiveness of personal data protection in Indonesia. The findings demonstrate that regulatory fragmentation, overlapping authority among institutions, and limited supervisory capacity hinder the consistent application of data protection laws. The absence of a fully operational and independent supervisory authority further exacerbates these challenges, leading to uncertainty in enforcement and accountability. This condition confirms that the transition toward a fully functional regulatory state in the domain of data protection is still incomplete, requiring substantial institutional strengthening and coordination.

In addition, the study underscores the critical role of technology in shaping the effectiveness of legal protection, as emphasized by Cyberlaw Theory. The findings reveal that many organizations have not yet integrated privacy-by-design principles or adequate cybersecurity measures into their operational systems. This technological gap undermines the implementation of legal norms and exposes personal data to risks such as breaches and unauthorized access. The discussion further indicates that cross-border data flows and the global nature of digital platforms present additional complexities that cannot be addressed solely through domestic legal instruments. Consequently, the integration of legal, institutional, and technological approaches emerges as a key requirement for effective data protection.

The synthesis of these findings confirms that the main research problem—namely the gap between normative legal provisions and their practical implementation—remains a defining challenge in Indonesia's personal data protection regime. The study also successfully addresses the identified research gap by demonstrating the need for a more holistic and integrated analytical framework that combines legal theory, regulatory governance, and technological considerations. The research questions are comprehensively answered, showing that while a regulatory framework exists, its effectiveness is limited by structural and operational constraints, and that significant reforms are necessary to enhance its functionality.

In relation to the research objectives, this study has achieved its aim of evaluating the adequacy and effectiveness of Indonesia's legal framework for personal data protection. The findings provide a nuanced understanding of both the strengths and limitations of the current system, thereby offering a foundation for future policy development and academic inquiry. The theoretical contribution of this research lies in its integration of multiple perspectives, demonstrating that the protection of personal data requires a multidimensional approach. Academically, the study enriches the discourse on digital law and governance, particularly in the context of emerging economies. Practically, it offers actionable insights for policymakers, regulators, and industry stakeholders to improve the implementation and enforcement of data protection laws.

In conclusion, the research establishes that the effectiveness of personal data protection in Indonesia depends not only on the existence of comprehensive legal provisions but also on the capacity of institutions, the level of public awareness, and the integration of technological safeguards. The findings emphasize that addressing the challenges of the digital era requires continuous adaptation, stronger regulatory coordination, and a commitment to upholding fundamental privacy rights. By linking the results and discussion to the broader theoretical and practical context, this study provides a

coherent and comprehensive conclusion that underscores the importance of a holistic approach to personal data protection in Indonesia.

REFERENCES

- Abdelaziz, E., Ahmed, R., & Darwish, D. A. A. (2022). Digital Technology in Architecture and Arts - Era Challenges. In *Proceedings of the Digital Technology in Architecture and Arts - Era Challenges*. DTAA21. <https://doi.org/10.21608/dtaa21.2022.1732>
- Adewumi, T., & Jolaosho, T. (2022). Legal and Regulatory Framework for Digital Credit Providers in Nigeria: Lessons from Kenya's Digital Credit Providers Regulations, 2022. In *Strathmore Law Journal* (Vol. 6, Nomor 1, hal. 93–106). Strathmore University. <https://doi.org/10.52907/slj.v6i1.175>
- Afzal, J. (2024). Legal Challenges Regarding Digital Operations. In *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (hal. 23–45). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-7106-6_2
- Agbelade, O. (2024). *A Comparative Analysis of Financial Technology (Fintech) Legal Framework: Blockchain, Mobile Payment Solutions & Data Protection As Special Case Study*. Elsevier BV. <https://doi.org/10.2139/ssrn.4966672>
- Ahmad, D. N. F., & Smith, N. N. (2024). Digital Safety for Women and Children: Legal and Policy Challenges Indonesia, Philippines, and Thailand. In *Journal of Law and Legal Reform* (Vol. 5, Nomor 4). Universitas Negeri Semarang. <https://doi.org/10.15294/jllr.v5i4.16539>
- Ali, A. (2025). Digital Security Protection in The Era Society 5.0 and its Implementation in Indonesia. In *Proceeding of International Conference on The Law Development For Public Welfare* (Vol. 4, hal. 674). Universitas Islam Sultan Agung. <https://doi.org/10.30659/picldpw.v4i0.50192>
- Allakuliev, M. (2024). SOME LEGAL CHALLENGES OF TORT LIABILITY IN THE DIGITAL ERA. In *Universum: Economics & law* (Vol. 121, Nomor 11). Siberian Academic Book LLC. <https://doi.org/10.32743/unilaw.2024.121.11.18326>
- Alzawahreh, M., Alhabarneh, H. J., & AlTayeb, A. A. (2024). Legal Protection for Worker's Wages in Jordanian Legislation. In *Studies in Computational Intelligence* (hal. 169–179). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-57242-5_14
- Amzulian, A. (2025). The Future of Arbitration for Personal Data Disputes in Indonesia: Weighing the Benefits and Challenges. In *Media Iuris* (Vol. 8, Nomor 2, hal. 215–238). Universitas Airlangga. <https://doi.org/10.20473/mi.v8i2.63060>
- Archibong, S., & Egharevba, E. (2023). The Legal Framework for Digital Payments In Nigeria: Consumer Protection and Data Privacy. In *SSRN Electronic Journal*. Elsevier BV. <https://doi.org/10.2139/ssrn.4564098>
- Balboni, P. (2020). Managing Legal Compliance in the Cloud: Understanding Contractual and Personal Data Protection Requirements. In *Cloud Computing Security* (hal. 283–298). CRC Press. <https://doi.org/10.1201/9780429055126-25>
- Barutu, S. (2025). Optimizing Big Data Analytics in the Era of Digital Transformation. In *Jurnal Komputer Indonesia (Ju-Komi)* (Vol. 3, Nomor 2, hal. 80–87). Science Analytical Institute. <https://doi.org/10.58471/ju-komi.v3i02.757>
- Bennett, C. J., & Bayley, R. M. (2025). Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments. In *Exploring the Boundaries of Big Data* (hal. 205–228). Routledge. <https://doi.org/10.4324/9781003695202-12>
- Bharati, R. (2024). Navigating the Legal Landscape of Artificial Intelligence: Emerging Challenges and Regulatory Framework in India. In *SSRN Electronic Journal*. Elsevier BV. <https://doi.org/10.2139/ssrn.4898536>

- Bholasing, J. (2022). How Technological Advances in the Big Data Era Make it Impossible to Define the 'Personal' in GDPR's 'Personal Data.' In *European Data Protection Law Review* (Vol. 8, Nomor 3, hal. 346–361). Lexxion Verlag. <https://doi.org/10.21552/edpl/2022/3/5>
- Biantoro, F. A. (2024). Personal Data Protection in Technological Developments Era. In *International Journal of Law Social Sciences and Management* (Vol. 1, Nomor 3). Yayasan Meira Visi Persada. <https://doi.org/10.69726/ijlssm.v1i3.29>
- Cheng, X., & Jia, Z. (2025). Challenges and Responses of China's Digital Copyright Protection Under the Framework of the CPTPP Agreement. In *Proceedings of the 1st International Conference on Politics, Law, and Social Science* (hal. 499–504). SCITEPRESS - Science and Technology Publications. <https://doi.org/10.5220/0014385300004859>
- Cupido, D. M. (2023). Contracts between Coastal States and Salvors as the Legal Regulatory Framework for Environmental Services in the Context of Salvage Operations. In *Maritime Salvage Operations and Environmental Protection* (hal. 93–101). Routledge. <https://doi.org/10.4324/9781003315506-7>
- Diksha, D., & Singh, D. N. (2025). Arrest Scams In The Digital Era: Legal Loopholes And Regulatory Challenges. In *International Journal of Research Publication and Reviews* (Vol. 6, Nomor 11, hal. 476–489). Genesis Global Publication. <https://doi.org/10.55248/gengpi.06.1125.3831>
- Fibrianti, N., & Holish, A. (2022). Consumer Personal Data Protection: Between Expectations and Reality. In *Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8-9 2021, Semarang, Indonesia*. EAI. <https://doi.org/10.4108/eai.8-6-2021.2314376>
- GARNO, Z. (2025). Insider Trading Challenges in the Digital Era: Legal and Ethical Considerations for U.S. Financial Market Regulation. In *Journal of Next-Generation Research 5.0*. Journal of Next-Generation Research 5.0. <https://doi.org/10.70792/jngr5.0.v1i3.75>
- Gou, X., & Wu, Z. (2024). *Challenges and Opportunities for Legal Education in the Digital Era: Perspectives from China*. Elsevier BV. <https://doi.org/10.2139/ssrn.4871981>
- Gulati, J. (2024). Analysing The Algorithm of Zoombombing as a Cybercrime in Digital Era: Legal Risks and Challenges. In *Journal of Electrical Systems* (Vol. 20, Nomor 4, hal. 2445–2452). Science Research Society. <https://doi.org/10.52783/jes.2751>
- Gurkov, A. (2020). Personal Data Protection in Russia. In *The Palgrave Handbook of Digital Russia Studies* (hal. 95–113). Springer International Publishing. https://doi.org/10.1007/978-3-030-42855-6_6
- Hafiz, M. (2024). *The Era of Artificial Intelligence: Examining Indonesia's Adaptability and Legal Challenges*. Center for Open Science. <https://doi.org/10.31219/osf.io/vk7jq>
- Hasan, L. K., & Putra, M. R. S. (2025). Electronic Contracts and E-Signatures in Indonesia: Legal Framework and Challenges in the Digital Revolution. In *Journal of Health Education Law Information and Humanities* (Vol. 2, Nomor 1, hal. 178–185). Rayyan Jurnal. <https://doi.org/10.57235/helium.v2i1.4769>
- Hendrawaty, E., & Bangsawan, S. (2020). Adoption of digital finance service in Indonesia: An empirical examination of an extended technological acceptance model. In *The Future Opportunities and Challenges of Business in Digital Era 4.0* (hal. 196–199). Routledge. <https://doi.org/10.1201/9780367853778-52>
- Herryani, M. R. T. R. (2023). Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia. In *Rechtsidee* (Vol. 11, Nomor 1). Universitas Muhammadiyah Sidoarjo. <https://doi.org/10.21070/jihr.v12i1.990>
- Hu, X., Wang, R., & Zhang, F. (2022). Research on legal issues of personal information security protection of college students in the era of big data—Taking the undergraduate students of

- China University of Geosciences (Beijing) as an example. In *Journal of Education, Humanities and Social Sciences* (Vol. 1, hal. 218–226). Darcy & Roy Press Co. Ltd. <https://doi.org/10.54097/ehss.v1i.664>
- Hutchinson, C. S., & Treščáková, D. (2021). The challenges of personalized pricing to competition and personal data protection law. In *European Competition Journal* (Vol. 18, Nomor 1, hal. 105–128). Informa UK Limited. <https://doi.org/10.1080/17441056.2021.1936400>
- Imasepti, K., & Mahmudah, S. (2024). Legal Protection in the Implementation of Personal Guarantees in Indonesia. In *International Journal of Multicultural and Multireligious Understanding* (Vol. 11, Nomor 5, hal. 425). Multidisciplinary Center. <https://doi.org/10.18415/ijmmu.v11i5.5787>
- Ivanova, S. V., & Rybak, S. V. (2025). Historical Stages in the Formation and Evolution of the Russian Regulatory Framework on the Use and Protection of Fauna. In *Legal Order and Legal Values* (Vol. 3, Nomor 3, hal. 29–39). FSFEI HE Don State Technical University. <https://doi.org/10.23947/2949-1843-2025-3-3-29-39>
- Jariyah, M., Setiyono, W. P., & Sriyono, S. (2023). *Personal Financial Management: Digital Age as Moderating variable Consumptive Behavior of Indonesian Sandwich Generation*. Universitas Muhammadiyah Sidoarjo. <https://doi.org/10.21070/ups.951>
- Kalina, J. (2025). Building trust in digital healthcare: Navigating disinformation, AI, ethics, and legal challenges. In *Digital Tools and Data for Innovative Healthcare* (hal. 3–25). Elsevier. <https://doi.org/10.1016/b978-0-443-27444-2.00003-4>
- Kapoor, P., & Sahoo, D. R. (2025). India-Africa Cooperation in the Digital Age: Navigating Privacy Protection and Emerging Challenges in the Global South. In *Advances in Social Science, Education and Humanities Research* (hal. 182–196). Atlantis Press SARL. https://doi.org/10.2991/978-2-38476-426-6_11
- Karisma, K. (2025). Legal and Regulatory Challenges in Implementing Blockchain-Enabled Renewable Energy Systems. In *NanoRevolution* (hal. 281–310). CRC Press. <https://doi.org/10.1201/9781003499732-15>
- Krasniqi, S. (2020). LEGAL PROTECTION OF PERSONAL DATA IN THE FUNCTION OF PROTECTION OF HUMAN RIGHTS AND FREEDOMS. In *International Journal of Research -GRANTHAALAYAH* (Vol. 8, Nomor 10, hal. 193–197). Granthaalayah Publications and Printers. <https://doi.org/10.29121/granthaalayah.v8.i10.2020.1785>
- Kumalaratri, G., & Yunanto, Y. (2021). URGENCY OF THE PERSONAL DATA PROTECTION BILL ON PRIVACY RIGHTS IN INDONESIA. In *Jurnal Hukum* (Vol. 37, Nomor 1, hal. 1). Program Doktor Ilmu Hukum Unissula. <https://doi.org/10.26532/jh.v37i1.13604>
- Laksmiana, I. N. H., & Permana, I. P. H. (2023). Legal Challenges for Digital Startup Development in Indonesia. In *Journal of Digital Law and Policy* (Vol. 2, Nomor 2, hal. 71–80). Yayasan Sinergi Widya Nusantara. <https://doi.org/10.58982/jdlp.v2i2.312>
- Lazuardy, M. S., Rachmawati, M., Marlina, T., & Umar, J. (2024). Legal framework for protecting bank customers against personal data leakage in the digital era: A study of Indonesian regulations. In *Indonesian Journal of Multidisciplinary Science* (Vol. 3, Nomor 10). International Journal Labs. <https://doi.org/10.55324/ijoms.v3i10.907>
- Makarim, E. (2020). Privacy and Personal Data Protection in Indonesia: The Hybrid Paradigm of the Subjective and Objective Approach. In *Information Technology and Law Series* (hal. 127–164). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-407-5_6
- Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. In *International Journal of Business, Economics, and Social Development* (Vol. 2, Nomor 4, hal. 143–152).

- Research Collaboration Community (RCC). <https://doi.org/10.46336/ijbesd.v2i4.170>
- Menon, P. (2025). The Legal Dynamics of Death. In *Law and the Digital Reanimation of the Dead* (hal. 15–46). Routledge. <https://doi.org/10.4324/9781003520559-2>
- Mohamed, E. (2022). Digital Technology in Architecture and Arts - Era Challenges. In *Proceedings of the Digital Technology in Architecture and Arts - Era Challenges*. DTAA21. <https://doi.org/10.21608/dtaa21.2022.1721>
- Mohamed, H., Darwish, D., & Shweekh, H. E. L. (2022). Digital Technology in Architecture and Arts - Era Challenges. In *Proceedings of the Digital Technology in Architecture and Arts - Era Challenges*. DTAA21. <https://doi.org/10.21608/dtaa21.2022.1725>
- Mohamed, R. (2022). Digital Technology in Architecture and Arts - Era Challenges. In *Proceedings of the Digital Technology in Architecture and Arts - Era Challenges*. DTAA21. <https://doi.org/10.21608/dtaa21.2022.1738>
- Musmualim, M., Fuad, F., & Suartini, S. (2024). Legal Protection for Consumers in Transactions E-Commerce by Era Digital. In *Eduvest - Journal of Universal Studies* (Vol. 4, Nomor 12, hal. 11935–11943). Green Publisher. <https://doi.org/10.59188/eduvest.v4i12.33413>
- Mustagfiroh, S., & Khoirina, N. N. (2025). Legal and Regulatory Challenges in the Implementation of Blockchain-Based Waqf in Indonesia. In *Walisongo Journal of Sharia Economic Law* (Vol. 1, Nomor 1). UIN Walisongo Semarang. <https://doi.org/10.21580/wishel.2025.1.1.29407>
- Napitupulu, B. (2022). SUPREME COURT DECISIONS ON PUBLIC INFORMATION AND PERSONAL DATA PROTECTION. In *Indonesia Private Law Review* (Vol. 3, Nomor 1, hal. 23–36). Fiat Justisia. <https://doi.org/10.25041/iplr.v3i1.2559>
- Nawawi, J. (2022). LEGAL PROTECTION OF PERSONAL DATA BASED ON REGULATION IN INDONESIA. In *Jurnal Al-Dustur* (Vol. 5, Nomor 1, hal. 96–106). IAIN BONE. <https://doi.org/10.30863/jad.v5i1.2581>
- Neves, A. (2020). Protection of Personal Data Regulation and Public Liberties. In *Advances in Information Security, Privacy, and Ethics* (hal. 1–18). IGI Global. <https://doi.org/10.4018/978-1-5225-9489-5.ch001>
- Nudan, P. W., Widodo, P., & Affifudin, M. (2024). Navigating the Starlink Era of Personal Data Protection in Indonesia. In *Formosa Journal of Science and Technology* (Vol. 3, Nomor 7, hal. 1447–1458). PT Formosa Cendekia Global. <https://doi.org/10.55927/fjst.v3i7.10139>
- Pengju, S. (2025). Legal Challenges to Personal Information Security in the Big Data Era and AI Regulatory Approaches. In *Journal of Commercial Law Review* (Vol. 9, Nomor 4, hal. 11–14). World Scientific Publishing House Ltd. <https://doi.org/10.47297/wspjclrwsp2516-249702.20250904>
- Pittiglio, R., Reganati, F., Ricci, F., & Tedeschi, C. (2020). Cybersecurity, Personal Data Protection and Crime Prevention from an Italian Perspective. In *The Palgrave Handbook of Corporate Sustainability in the Digital Era* (hal. 131–156). Springer International Publishing. https://doi.org/10.1007/978-3-030-42412-1_7
- Pour, H. N. (2025). DATA PROTECTION CHALLENGES IN SMART CITIES: AN EXAMINATION OF THE MALAYSIAN LEGAL FRAMEWORK. In *SSRN Electronic Journal*. Elsevier BV. <https://doi.org/10.2139/ssrn.5261163>
- Prodanov, G. (2021). CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA IN HIGHER EDUCATION. In *PROTECTION OF THE PERSONAL DATA AND THE DIGITALIZATION - CHALLENGES AND PERSPECTIVES 2021 CONFERENCE PROCEEDINGS* (hal. 172–179). University publishing house “Science and Economics”, University of Economics - Varna. <https://doi.org/10.36997/ppdd2021.172>

- Reljić, D., & Tul, D. (2025). Personal data and artificial intelligence: Legal and ethical aspects in the era of rapid IT development. In *XXII International Scientific Conference "Legal Days – Prof. Slavko Caric Law and justice"* - zbornik radova (hal. 593–604). The Faculty of Law for Commerce and Judiciary in Novi Sad. <https://doi.org/10.5937/pdsc25593r>
- Roşca, C. (2024). Chapter 4. Causes for regulatory concern and regulatory design challenges. In *Digital Arms for Digital Consumer Harms - Mapping Legal and Technical Solutions for Dark Patterns in EU Consumer Law*. Maastricht University Press. <https://doi.org/10.26481/mup.2403.04>
- Ruda, A. (2021). Legal and Ethical Implications of eHealth Big Data—A Comparative Perspective between Japan and Catalonia. In *Legal Challenges in the New Digital Age* (hal. 126–159). Brill | Nijhoff. https://doi.org/10.1163/9789004447417_009
- Sa'adah, B. L. N., Sukarmi, S., & Dewantara, R. (2024). Establishing A Personal Data Protection Agency for E-Commerce in Indonesia. In *Invest Journal of Sharia & Economic Law* (Vol. 4, Nomor 2, hal. 292–316). STAIN Ponorogo. <https://doi.org/10.21154/invest.v4i2.10031>
- Sanusi, S. (2024). LEGAL PROTECTION OF CONSUMERS IN E-COMMERCE TRANSACTIONS: A REVIEW OF CIVIL LAW IN THE DIGITAL ERA. In *POLICY LAW NOTARY AND REGULATORY ISSUES (POLRI)* (Vol. 3, Nomor 3, hal. 406–417). PT. Transpublika Jaya Abadi. <https://doi.org/10.55047/polri.v3i3.1348>
- Saware, D. S. M. (2024). *Personal Data Protection In Digital Age: Issues And Challenges*. San International Scientific Publications. <https://doi.org/10.59646/dataprotection/127>
- Sharma, A. D. V. L. (2025). Cyber Defamation in India: Legal Framework, Challenges and Jurisdiction in the Digital Age. In *SSRN Electronic Journal*. Elsevier BV. <https://doi.org/10.2139/ssrn.5752326>
- Sharma, V. (2025). Law and Emerging Technologies in Global Commerce: Regulatory Challenges in the Digital Transformation Era. In *Journal of International Commercial Law and Technology* (Vol. 6, Nomor 1, hal. 549–554). Vital Signs Press. <https://doi.org/10.61336/jiclt/25-01-51>
- Sinaga, S. (2025). DIGITAL ERA BUSINESS LAW TRANSFORMATION: LEGAL CERTAINTY ANALYSIS IN E-COMMERCE TRANSACTIONS IN INDONESIA. In *Jurnal Meta Hukum* (Vol. 4, Nomor 3, hal. 127–141). Yayasan Pendidikan Islam Tholabul Ilmi. <https://doi.org/10.47652/metahukum.v4i3.889>
- Sinulingga, D. A. (2022). Legal Certainty Of Aggregate Data Utilization In The Design Of Personal Data Protection Bill. In *Jambura Law Review* (Vol. 4, Nomor 1, hal. 18–37). Fakultas Hukum Universitas Negeri Gorontalo. <https://doi.org/10.33756/jlr.v4i1.11973>
- Soepeno, M. H., Korah, R., Prayogo, P., Rehulina, R., Tumewu, F., Tumiwa, J. R., Tuegeh, O. D. M., Troján, S., Kacz, K., & Tamas, M. (2025). *Developing a Sui Generis Legal Framework in the Digital Era for the Protection of Traditional Cultural Expressions: Implementation of Customary Land Acquisition in Emerging Economies Countries*. Elsevier BV. <https://doi.org/10.2139/ssrn.5367321>
- Stepenko, V., Dreval, L., Chernov, S., & Shestak, V. (2021). EU Personal Data Protection Standards and Regulatory Framework. In *Journal of Applied Security Research* (Vol. 17, Nomor 2, hal. 190–207). Informa UK Limited. <https://doi.org/10.1080/19361610.2020.1868928>
- Supriyanto, Rahardjo, T. M. S., Sumiyati, Noerdjaja, H., Pambudi, G. E., & Prabowo, M. S. (2025). Consumer Protection Legal Frameworks in Indonesia: The Challenges of E-Commerce and Data Privacy. In *Research Horizon* (Vol. 5, Nomor 2, hal. 119–128). PT Lifescifi Akademia Utama. <https://doi.org/10.54518/rh.5.2.2025.491>
- Taufan, R. A., & Sara, R. (2025). Evaluation of the Legal Framework for Digital Business in Indonesia in Addressing Technological Developments and Regulatory Challenges. In *International Journal*

- of Social Service and Research* (Vol. 5, Nomor 7, hal. 715–723). Ridwan Institute.
<https://doi.org/10.46799/ijssr.v5i7.1257>
- Uvarova, A. V. (2024). Organizational and legal framework for personal data protection in consumer p2p-lending. In *Vestnik of Saint Petersburg University. Law* (Vol. 15, Nomor 4, hal. 1061–1068). Saint Petersburg State University. <https://doi.org/10.21638/spbu14.2024.409>
- Varbanova, G. (2021). ELECTRONIC IDENTITY AND PERSONAL DATA PROTECTION. In *PROTECTION OF THE PERSONAL DATA AND THE DIGITALIZATION - CHALLENGES AND PERSPECTIVES 2021 CONFERENCE PROCEEDINGS* (hal. 156–162). University publishing house “Science and Economics”, University of Economics - Varna. <https://doi.org/10.36997/ppdd2021.156>
- Vashurina, S. (2025). Trust in Artificial Intelligence: Regulatory Challenges and Prospects. In *Legal Issues in the Digital Age* (Vol. 6, Nomor 2, hal. 69–86). National Research University, Higher School of Economics (HSE). <https://doi.org/10.17323/2713-2749.2025.2.69.86>
- Wibowo, B. S. (2025). Regulatory Challenges of AI-Driven Credit Scoring in Indonesian Banking: Between Algorithmic Bias and Consumer Protection. In *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS* (Nomor 11). Everant Journals. <https://doi.org/10.47191/ijmra/v8-i11-71>
-)2025. (شوشان ف). Digital Editing And Electronic Publishing:, A Legal Vision In Light Of The Ethical And Regulatory Challenges. In *مجلة جيل الدراسات المقارنة* (hal. 109). JiL Scientific Research Center. <https://doi.org/10.33685/1565-000-022-005>
- 文玉琴. (2023). An Empirical Legal Study of Personal Information Protection in the Era of Big Data. In *Dispute Settlement* (Nomor 5, hal. 2007–2017). Hans Publishers. <https://doi.org/10.12677/ds.2023.95272>