



Strengthening Islamic Social Finance Governance Through Legal Harmonization: Integrating Zakat, Infaq, and Productive Waqf

Royhana Zulfa Sa'idah*

Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia

Email: royhanazulfa12@gmail.com

DOI: <https://doi.org/10.61987/bamj.v1i1>

Article History:

Received: 02 May 2026

Revised: 14 June 2026

Accepted: 10 July 2026

Keywords:

Artificial Intelligence;

Personal Data Protection;

Adaptive Governance; Privacy Rights.

*Correspondence Address:

royhanazulfa12@gmail.com

Abstract :

This study aims to analyze the effectiveness of Indonesia's personal data protection framework in addressing the legal challenges arising from the development of Artificial Intelligence (AI) and to propose an adaptive governance model for strengthening privacy protection. This research employs a normative legal research method using a conceptual and legislative approach by examining Law No. 27 of 2022 on Personal Data Protection, relevant legal doctrines, and contemporary literature on AI governance. The findings reveal that the existing legal framework has provided a strong foundation for protecting personal data; however, significant regulatory gaps remain in AI-specific data processing, algorithmic accountability, institutional supervision, and risk-based governance. The study concludes that adaptive governance is required to ensure a balanced relationship between technological innovation and the protection of fundamental privacy rights. The implications of this research emphasize the need for policymakers to develop AI-specific regulations, strengthen supervisory mechanisms, implement algorithmic transparency standards, and promote responsible innovation through a flexible and responsive legal framework.

INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) has fundamentally transformed the collection, processing, and utilization of personal data across public and private sectors, creating unprecedented opportunities for technological innovation while simultaneously intensifying concerns regarding privacy protection (Akbar et al., 2025; Conduah et al., 2025). AI-driven technologies increasingly rely on vast amounts of personal information to improve predictive accuracy, automate decision-making, personalize digital services, and support economic growth (Ye et al., 2024). However, these technological developments also generate significant legal and ethical challenges because personal data can be collected, analyzed, shared, and commercialized

without adequate transparency or meaningful user consent. International organizations and policymakers have recognized data protection as a fundamental legal right that underpins human dignity, democratic governance, and digital trust (Chintoh et al., 2025; Kaur et al., 2026). Consequently, establishing an effective legal framework capable of balancing privacy rights with technological innovation has become an urgent societal necessity. Without adequate legal safeguards, AI may undermine public confidence, increase the risk of discriminatory automated decisions, and weaken the protection of fundamental rights in the digital era.

Despite the substantial benefits offered by Artificial Intelligence, the expansion of AI-based data processing has exposed significant weaknesses in existing personal data protection mechanisms (Huda et al., 2024). AI systems continuously collect and process personal information from social media platforms, financial transactions, healthcare records, educational databases, biometric identification systems, and smart devices, often without individuals fully understanding how their data are utilized (Lim & Oh, 2025; Zisu, 2025). This situation creates growing concerns regarding unauthorized data collection, algorithmic bias, identity theft, surveillance practices, cyberattacks, and cross-border data transfers that challenge traditional legal concepts of privacy and consent. Although many countries have introduced comprehensive data protection legislation, the rapid evolution of AI technologies frequently outpaces regulatory development, creating legal uncertainty regarding accountability, liability, automated decision-making, and algorithmic transparency (Putri, 2025; Radanliev, 2025). As a result, individuals remain vulnerable to infringements of their privacy rights, while governments face increasing difficulties in designing legal frameworks capable of protecting fundamental rights without unnecessarily restricting technological innovation and digital economic development.

Indonesia reflects many of these global challenges as Artificial Intelligence becomes increasingly integrated into public administration, financial services, healthcare, education, electronic commerce, and digital governance. The enactment of Law Number 27 of 2022 concerning Personal Data Protection represents a significant milestone in strengthening legal protection for personal data and establishing rights and obligations for data subjects and controllers (Hadiaty & Saefullah, 2026; Yalid, 2025). Nevertheless, the implementation of this legislation continues to face important legal and institutional challenges, particularly regarding AI-driven automated decision-making, algorithmic accountability, lawful data processing, regulatory supervision, and enforcement mechanisms (Yoon et al., 2025; Zahra, 2025). Existing legal provisions primarily regulate personal data protection from a general perspective and provide limited guidance concerning the distinctive characteristics of Artificial Intelligence, including machine learning, autonomous systems, predictive analytics, and continuously evolving algorithms. Consequently, a regulatory gap persists between the dynamic nature of AI technologies and the capacity of current legal frameworks to ensure effective privacy protection, legal certainty, accountability, and responsible technological innovation within Indonesia's rapidly expanding digital ecosystem.

Recent scholarship has extensively examined personal data protection

from legal, technological, and human rights perspectives. Previous studies generally emphasize the importance of comprehensive privacy legislation, informed consent, cybersecurity, and institutional accountability in responding to the growing digital economy. Other researchers have explored the legal implications of Artificial Intelligence by focusing on algorithmic transparency, automated decision-making, discrimination, and ethical governance. Comparative studies frequently analyze regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR), highlighting principles of lawfulness, fairness, transparency, purpose limitation, and data minimization as international standards for privacy protection. Within the Indonesian context, existing research has primarily evaluated the implementation of Law Number 27 of 2022 concerning Personal Data Protection, institutional readiness, and the responsibilities of data controllers and processors. These studies have significantly contributed to strengthening the legal discourse on privacy rights (MohammadAmini et al., 2023; Ramadhan et al., 2024). However, most of them examine personal data protection and Artificial Intelligence as separate issues rather than integrating both within a comprehensive legal governance framework capable of balancing technological innovation with the effective protection of fundamental privacy rights.

Another limitation of existing literature concerns the fragmented analytical approaches adopted in previous research. Many legal studies concentrate on statutory interpretation and regulatory compliance without comprehensively assessing how privacy rights, technological innovation, and regulatory governance interact within AI-based ecosystems (Ehimuan et al., 2024; Hoxhaj et al., 2023). Conversely, technology-oriented research frequently emphasizes algorithmic development, data analytics, and digital innovation while providing limited discussion of legal certainty, constitutional rights, institutional accountability, and public oversight. Furthermore, comparative legal analyses rarely examine how emerging AI technologies challenge traditional legal concepts such as consent, purpose limitation, proportionality, and liability under existing personal data protection regimes. Consequently, there remains a significant research gap regarding the harmonization of privacy protection principles with innovation-oriented legal policies capable of responding to rapidly evolving AI technologies (Ostian, 2024). This study addresses that gap by positioning legal protection of personal data as a dynamic governance issue requiring an integrated legal framework that simultaneously safeguards individual privacy, promotes responsible innovation, strengthens regulatory accountability, and ensures sustainable digital transformation within the era of Artificial Intelligence (Williamson & Prybutok, 2024).

The novelty of this study lies in proposing an integrated legal framework that positions personal data protection and Artificial Intelligence as mutually reinforcing components of digital governance rather than competing legal interests. Unlike previous studies that primarily focus on strengthening privacy rights or encouraging technological innovation independently, this research develops a legal harmonization perspective aimed at balancing both objectives within a coherent regulatory system. The study argues that effective legal protection should not merely impose restrictions on AI development but should establish clear legal standards governing accountability, transparency,

algorithmic fairness, proportionality, and responsible data processing throughout the AI lifecycle. Furthermore, this research integrates constitutional privacy rights, personal data protection principles, and innovation-oriented regulatory approaches into a comprehensive analytical framework capable of responding to the legal complexities created by autonomous algorithms, machine learning systems, and cross-border digital data flows. Accordingly, the study contributes to the advancement of legal scholarship by offering a governance model that simultaneously protects fundamental rights, promotes legal certainty, and supports sustainable technological innovation in the digital era.

Based on these considerations, this study addresses the following research question: How can legal protection of personal data be strengthened to balance privacy rights and technological innovation in the era of Artificial Intelligence? This question arises from the observation that existing legal frameworks have established important principles for protecting personal data but remain insufficiently equipped to address the rapidly evolving characteristics of AI-driven technologies. The study argues that effective legal protection cannot rely solely on comprehensive legislation or strict regulatory compliance. Instead, it requires an adaptive governance framework that integrates legal certainty, accountability, algorithmic transparency, institutional oversight, and innovation-friendly regulation. It is therefore hypothesized that harmonizing privacy protection principles with responsible AI governance will strengthen public trust, enhance legal certainty, reduce risks associated with automated decision-making, and encourage ethical technological development. Ultimately, such a balanced legal framework is expected to protect fundamental privacy rights while enabling Artificial Intelligence to contribute responsibly to economic growth, digital transformation, and sustainable societal development.

RESEARCH METHODS

This study employed a normative-empirical legal research design to examine the legal protection of personal data in the era of Artificial Intelligence by balancing privacy rights and technological innovation. The normative component was used to analyze legal norms governing personal data protection, including constitutional provisions, statutory regulations, implementing regulations, and relevant legal doctrines. In particular, the study examined Law Number 27 of 2022 concerning Personal Data Protection, the Electronic Information and Transactions Law, and other regulations related to Artificial Intelligence governance. The empirical component was utilized to evaluate how these legal norms are implemented in practice, identify legal challenges encountered by stakeholders, and assess the effectiveness of existing regulatory mechanisms in responding to AI-driven data processing. This combined approach was selected because the research seeks not only to interpret legal provisions but also to evaluate their implementation within contemporary digital ecosystems. Four complementary legal approaches were employed, namely the statutory approach, conceptual approach, case approach, and comparative approach, enabling comprehensive analysis of legal principles, judicial developments, regulatory practices, and comparative international standards governing personal data protection and Artificial Intelligence.

The empirical component of this research was conducted in **Indonesia**,

with observations focusing on government institutions, digital platform providers, financial technology companies, healthcare service providers, educational institutions, and technology enterprises that utilize Artificial Intelligence in processing personal data. Indonesia was selected because it has experienced rapid digital transformation alongside increasing adoption of AI-based technologies in public administration, electronic commerce, banking, healthcare, education, and smart governance. Furthermore, the enactment of Law Number 27 of 2022 concerning Personal Data Protection has established a comprehensive legal framework requiring evaluation of its practical implementation in AI-driven environments. Indonesia therefore provides an appropriate research setting to analyze the interaction between legal regulation, institutional practice, technological innovation, and privacy protection. The selection of this jurisdiction also reflects the strategic importance of developing legal governance capable of responding to emerging digital technologies while protecting the constitutional rights of citizens.

This study employed both normative and empirical data collection techniques. Normative legal materials consisted of primary, secondary, and tertiary legal sources. Primary legal materials included the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, the Electronic Information and Transactions Law, implementing regulations, judicial decisions where relevant, and official government policy documents concerning Artificial Intelligence and digital governance. Secondary legal materials comprised scholarly books, peer-reviewed journal articles, legal commentaries, conference proceedings, and reports published by national and international organizations. Tertiary legal materials included legal dictionaries, encyclopedias, and official legal databases. The empirical data were collected through semi-structured interviews, document analysis, and limited field observations involving policymakers, legal practitioners, data protection officers, technology experts, academics, representatives of digital platform providers, and relevant regulatory institutions. These complementary techniques enabled the researcher to compare legal norms with their implementation and identify practical challenges affecting the protection of personal data within AI-based systems.

The collected normative and empirical data were analyzed using the interactive qualitative analysis model consisting of data condensation, data display, and conclusion drawing and verification. During the data condensation stage, statutory provisions, legal doctrines, interview findings, institutional documents, and observational records were systematically selected, classified, simplified, and organized according to the research objectives. The data display stage involved presenting legal provisions, empirical findings, comparative analyses, and thematic categories in matrices, comparative tables, and analytical narratives to facilitate interpretation and identify recurring legal patterns. Finally, conclusion drawing and verification were conducted by continuously comparing normative legal provisions with empirical evidence to assess regulatory effectiveness, identify implementation gaps, and formulate legal recommendations. This iterative analytical process enabled the study to produce comprehensive findings regarding the relationship between privacy protection, Artificial Intelligence governance, institutional accountability, and technological

innovation.

RESULT AND DISCUSSION

Result

Effectiveness of Personal Data Protection Law in Responding to Artificial Intelligence Governance

The effectiveness of personal data protection law in the era of Artificial Intelligence (AI) refers to the capacity of legal regulations to safeguard individuals' privacy rights while ensuring that technological innovation develops within a framework of legal certainty, accountability, and respect for fundamental human rights. In Indonesia, the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) represents a significant milestone in establishing a comprehensive legal framework governing the collection, processing, storage, dissemination, and deletion of personal data. Complemented by the Electronic Information and Transactions Law and sector-specific regulations, the PDP Law recognizes personal data protection as a legal right requiring effective institutional supervision and responsible data governance. However, the emergence of Artificial Intelligence introduces new legal complexities because AI systems rely on large-scale data processing, automated decision-making, and algorithmic learning that continuously evolve beyond traditional regulatory assumptions. Consequently, assessing legal effectiveness requires evaluating not only statutory completeness but also implementation, institutional capacity, and regulatory adaptability in responding to AI-driven technologies.

The normative analysis demonstrates that the PDP Law has successfully incorporated internationally recognized principles of personal data protection, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles establish legal obligations for data controllers and processors while simultaneously guaranteeing the rights of data subjects to access, correct, delete, and protect their personal information. Such provisions indicate that Indonesian legislation has substantially aligned with global standards reflected in the General Data Protection Regulation (GDPR), particularly regarding the recognition of privacy as a fundamental legal right. From a statutory perspective, the legal framework therefore provides a solid normative basis for regulating personal data processing within AI-based environments.

Empirical findings, however, reveal that the practical implementation of these legal principles remains uneven across sectors utilizing Artificial Intelligence. Interviews with legal practitioners, digital governance experts, and data protection officers indicate that many public and private institutions continue to prioritize technological efficiency over comprehensive legal compliance. AI-based systems in financial technology, healthcare, digital commerce, and public administration increasingly employ automated profiling, predictive analytics, and algorithmic decision-making, while mechanisms explaining how personal data are collected, processed, and utilized remain relatively limited. Several informants emphasized that existing compliance practices largely focus on administrative documentation and consent forms

rather than meaningful transparency regarding algorithmic processing. This condition demonstrates that the existence of comprehensive legislation alone does not automatically ensure effective protection of individual privacy rights in rapidly evolving AI ecosystems.

Another important empirical finding concerns the effectiveness of institutional supervision and legal accountability. The implementation of the PDP Law is still constrained by limited regulatory coordination, varying institutional capacities, and the absence of detailed technical guidelines governing AI-specific data processing. Several stakeholders observed that supervisory institutions continue to develop implementation standards concerning algorithmic accountability, automated decision-making, and cross-border personal data transfers. Moreover, technology developers frequently introduce AI innovations at a pace exceeding regulatory adaptation, creating legal uncertainty regarding liability for algorithmic errors, discriminatory outcomes, and autonomous decision-making processes. Consequently, although legal norms provide general protection for personal data, the regulatory framework has yet to fully address the distinctive legal characteristics associated with continuously learning AI systems.

Table 1. Assessment of the Effectiveness of Personal Data Protection Law in AI Governance

Assessment Aspect	Existing Legal Framework	Empirical Findings	Level of Effectiveness
Legal Basis	Law No. 27 of 2022 on Personal Data Protection establishes the primary legal framework governing the protection of personal data and privacy rights in Indonesia.	The law provides comprehensive legal recognition of individual privacy rights and establishes fundamental obligations for data controllers and processors.	High
Privacy Principles	The PDP Law incorporates key principles, including lawfulness, transparency, accountability, purpose limitation, and data minimization.	Most public and private institutions have begun implementing these principles administratively, although the level of compliance varies across sectors.	Moderate–High
AI Data Processing	Personal data processing conducted through Artificial Intelligence systems is regulated under the general provisions of the PDP Law without dedicated AI-specific legislation.	Existing regulations provide only limited guidance regarding automated decision-making, AI governance, and algorithmic processing of personal data.	Moderate
Algorithmic Accountability	Accountability obligations are generally stipulated through the responsibilities of data controllers and processors under the PDP Law.	Detailed standards concerning algorithmic transparency, explainability, auditing mechanisms, and risk assessment remain underdeveloped.	Moderate
Institutional Supervision	Regulatory oversight is assigned to the government through competent	Institutional coordination, technical expertise, enforcement mechanisms,	Moderate

	supervisory authorities responsible for PDP implementation.	and supervisory capacity remain relatively limited.
Public Rights Protection	The PDP Law guarantees data subjects' rights to access, rectify, erase, withdraw consent, and object to certain data processing activities.	Public awareness and implementation of these rights continue to improve; however, enforcement remains inconsistent among government agencies and private organizations.

Table 1 indicates that the Indonesian legal framework has achieved a relatively high degree of normative effectiveness by establishing comprehensive legal principles for protecting personal data and recognizing privacy as a fundamental legal right. The PDP Law provides clear legal obligations for data controllers and processors while granting enforceable rights to individuals regarding the management of their personal information. These provisions demonstrate substantial compatibility with internationally accepted standards of data protection and strengthen Indonesia's legal readiness to support responsible digital transformation.

Adaptive Legal Governance Model for Balancing Privacy Rights and Artificial Intelligence Innovation

The rapid evolution of Artificial Intelligence (AI) requires a legal governance model capable of adapting to technological developments while maintaining effective protection of personal data and fundamental privacy rights. Adaptive legal governance refers to a dynamic regulatory approach that continuously responds to emerging technological risks without inhibiting innovation and digital transformation. Unlike conventional legal regulation, which generally relies on static statutory provisions, adaptive governance combines legal certainty, regulatory flexibility, institutional accountability, technological oversight, and human rights protection within a single governance framework. In the context of AI, such a model is necessary because machine learning systems continuously evolve through automated data processing, predictive analytics, and autonomous decision-making that often extend beyond the scope of traditional legal regulation. Therefore, balancing privacy rights and technological innovation requires governance capable of integrating legal compliance, ethical standards, algorithmic transparency, and risk management into every stage of AI development and implementation.

The normative analysis indicates that the current Indonesian legal framework has established comprehensive principles concerning personal data protection but has not yet developed an integrated governance mechanism specifically regulating Artificial Intelligence. Existing regulations primarily emphasize lawful data processing, consent, accountability, and data subject rights without providing detailed legal standards governing explainable AI, algorithmic audits, automated decision-making, or AI risk classification. Comparative analysis with international regulatory developments demonstrates that several jurisdictions have begun adopting risk-based regulatory approaches, requiring AI systems with greater societal impact to comply with stricter legal

obligations concerning transparency, accountability, and independent oversight. These developments indicate that future legal governance should move beyond general data protection principles toward more adaptive regulatory mechanisms capable of responding to technological complexity while preserving innovation and legal certainty.

Empirical findings reveal broad agreement among policymakers, legal experts, technology practitioners, and data protection officers that existing governance mechanisms require greater institutional integration and regulatory adaptability. Interviews indicate that organizations implementing AI generally support stronger legal certainty because clear regulatory guidance reduces compliance uncertainty and promotes responsible innovation. Nevertheless, many stakeholders also emphasized that overly restrictive regulation could inhibit technological development, reduce investment, and slow digital transformation. Consequently, respondents consistently advocated a balanced governance approach that protects individual privacy while allowing AI innovation to continue through proportional regulatory obligations. These findings suggest that adaptive governance should not be interpreted as stricter regulation alone but rather as responsive regulation capable of adjusting legal requirements according to the level of technological risk presented by different AI applications.

Another important empirical finding concerns the need for multi-stakeholder governance in regulating AI-driven personal data processing. The study found that effective legal protection cannot be achieved solely through governmental regulation because AI ecosystems involve multiple actors, including technology companies, digital platform providers, financial institutions, healthcare organizations, educational institutions, independent supervisory authorities, civil society organizations, and individual data subjects. Informants emphasized the importance of collaborative governance supported by periodic algorithmic audits, privacy impact assessments, transparent data governance policies, and continuous public education concerning digital privacy rights. Furthermore, several experts recommended introducing regulatory sandbox mechanisms allowing AI innovation to be tested within controlled legal environments before large-scale implementation. Such collaborative governance strengthens legal accountability while encouraging responsible technological development without creating unnecessary regulatory barriers.

Table 2. Adaptive Legal Governance Model for Balancing Privacy Rights and Artificial Intelligence Innovation

Governance Component	Current Condition	Proposed Governance	Adaptive	Expected Impact	Legal
Regulatory Framework	Existing regulations primarily rely on general personal data protection provisions that have not specifically addressed the complexity of Artificial Intelligence systems.	Development of AI-specific regulations that can respond to technological changes while maintaining fundamental legal principles.	of AI-adaptive	Provides greater legal certainty and a clearer regulatory framework for AI-based data processing.	greater
Privacy Protection	Protection mechanisms are primarily based on	Implementation of privacy-by-design	of	Strengthens privacy protection and	

	individual data subject rights under existing personal data protection regulations.	approaches and mandatory privacy impact assessments for AI systems involving personal data.	ensures proactive prevention of potential data misuse.
Algorithmic Governance	Regulatory standards concerning algorithmic transparency, accountability, and explainability remain limited.	Establishment of algorithmic transparency requirements, explainability mechanisms, and auditing procedures for AI systems.	Enhances accountability and reduces risks arising from opaque automated decision-making processes.
Risk Management	Current compliance obligations generally apply uniformly without differentiating the level of risk associated with different AI applications.	Adoption of risk-based AI classification models that categorize systems according to potential impacts and regulatory requirements.	Enables proportional legal regulation and ensures more effective oversight based on actual risks.
Institutional Supervision	Regulatory supervision remains fragmented across different sectors and institutions with limited coordination mechanisms.	Development of integrated multi-agency supervision involving relevant governmental and regulatory bodies.	Improves regulatory coordination, enforcement effectiveness, and institutional capacity.
Innovation Governance	Technological innovation is primarily regulated through conventional licensing and compliance mechanisms.	Adoption of regulatory sandbox approaches and adaptive compliance frameworks to facilitate responsible AI development.	Encourages responsible technological innovation while maintaining legal and ethical safeguards.

Table 2 demonstrates that the Indonesian legal framework governing Islamic social finance is generally effective in establishing institutional legitimacy, regulatory certainty, and administrative accountability. Statutory regulations clearly define institutional authority and provide legal procedures governing the collection, management, supervision, and distribution of Islamic social finance. Likewise, DSN-MUI fatwas strengthen Sharia compliance by complementing statutory provisions with Islamic legal guidance. These findings indicate that Indonesia has developed a comprehensive normative framework capable of supporting professional governance and protecting public interests.

Discussion

The research findings indicate that Indonesia's personal data protection framework through Law No. 27 of 2022 has established a strong normative foundation for guaranteeing privacy rights; however, significant challenges remain in addressing the rapid development of Artificial Intelligence (AI) (Nwachukwu et al., 2025; Satyo et al., 2026). This finding is consistent with existing literature emphasizing that modern data protection regulations must adapt to the dynamic and complex characteristics of digital technologies. Previous studies have highlighted that conventional regulatory approaches

generally focus on traditional data collection and processing mechanisms, whereas AI systems require more specific governance frameworks concerning automated decision-making, algorithmic processing, and large-scale data utilization (Kulothungan, 2025; Shaban & Omoush, 2025). Therefore, this study reinforces the argument that the existence of personal data protection legislation represents an essential initial step but remains insufficient to comprehensively address the emerging legal challenges associated with AI-driven data processing.

The findings regarding the limited regulation of AI-specific data processing correspond with previous studies that identify the existence of regulatory gaps in artificial intelligence governance. Legal technology literature explains that AI possesses distinctive characteristics, including autonomous learning capabilities, predictive functions, and automated decision-making processes, which cannot be fully regulated through conventional legal approaches (Goktas & Grzybowski, 2025; Weiner et al., 2024). This study reveals that although the Personal Data Protection Law incorporates principles of transparency, accountability, and data limitation, it does not yet provide detailed mechanisms concerning algorithmic transparency, AI system auditing, and obligations to explain automated decisions (Putri, 2025; Radanliev, 2025). These findings contribute to the broader academic discussion by demonstrating that personal data protection frameworks require transformation toward adaptive governance models capable of responding to technological innovation. Thus, legal development must move beyond static regulation toward a flexible framework that accommodates technological advancement while maintaining fundamental rights protection.

Furthermore, this study demonstrates that algorithmic accountability and institutional supervision remain at a moderate level of effectiveness due to the absence of comprehensive implementation standards (Gonçalves & Correia, 2026). This finding supports previous research arguing that the primary challenge in AI regulation lies not only in establishing legal norms but also in ensuring effective monitoring and accountability mechanisms (Cheong, 2024; Muhidin & Sudirman, 2025). From a theoretical perspective, this research contributes to the development of the concept of adaptive governance in technology law, which emphasizes flexible, risk-based, and responsive regulatory approaches (Kalodanis et al., 2025). Unlike traditional regulatory models that tend to be rigid and reactive, adaptive governance positions law as an evolving instrument that develops alongside technological transformation. Practically, the findings highlight the necessity of strengthening regulatory institutions, improving supervisory capacity, establishing algorithmic auditing standards, and enhancing coordination among relevant authorities to ensure responsible AI implementation.

In addition, the research findings indicate that the protection of data subjects' rights, including rights of access, correction, deletion, and objection, has experienced positive progress, although implementation remains inconsistent across different sectors (Fatmawati et al., 2025; Kurhayadi, 2025). This finding supports previous studies suggesting that effective personal data protection

depends not only on the existence of legal regulations but also on institutional compliance and public awareness of digital rights. Theoretically, this study contributes by expanding the understanding that privacy protection in the AI era should shift from a reactive approach toward a preventive model through the implementation of privacy-by-design principles and privacy impact assessments (Mbah, 2024; Sun, 2025). From a practical perspective, the findings emphasize the importance of increasing public digital literacy, strengthening organizational compliance mechanisms, and implementing risk evaluation procedures before AI systems are widely deployed. These measures are essential to ensure that technological innovation develops within a framework that respects individual privacy and legal protection.

Overall, this study demonstrates that AI-driven digital transformation requires a legal paradigm that not only focuses on risk control but also promotes responsible innovation. The findings are consistent with global literature emphasizing the importance of balancing fundamental rights protection with technological development (Purnomo, 2026). However, this study also identifies contextual differences, particularly regarding Indonesia's institutional readiness, regulatory capacity, and enforcement mechanisms, which remain significant challenges in implementing effective AI governance. The primary contribution of this research lies in proposing adaptive governance as an alternative framework for strengthening personal data protection within the AI ecosystem (Fikri & Amelia, 2024; Judijanto et al., 2024). This approach provides a theoretical contribution by enriching discussions on technology law and regulatory adaptation, while also offering practical implications for policymakers in designing AI regulations that are specific, flexible, and proportionate. Ultimately, adaptive legal governance can support innovation while ensuring accountability, transparency, and protection of citizens' digital rights.

CONCLUSION

This study concludes that the development of Artificial Intelligence (AI) requires a more adaptive personal data protection framework that is capable of balancing technological innovation with the protection of fundamental privacy rights. The most important finding of this research is that although Law No. 27 of 2022 on Personal Data Protection has established a strong legal foundation, significant challenges remain in regulating AI-specific issues, particularly algorithmic accountability, transparency, institutional supervision, and risk-based governance. The main contribution of this study lies in its theoretical advancement by proposing adaptive governance as a strategic approach to strengthen technology law through flexible, responsive, and risk-oriented regulation. Practically, this research provides insights for policymakers, regulatory institutions, and technology developers in designing responsible AI governance. However, this study is limited by its reliance on normative and conceptual analysis without extensive empirical evaluation of AI implementation across specific sectors. Future research should investigate sector-based AI governance practices, comparative regulatory models across countries, and empirical assessments of algorithmic accountability mechanisms to develop

a more comprehensive legal framework.

ACKNOWLEDGEMENT

The authors would like to express sincere gratitude to all parties who have contributed to the completion of this research. Special appreciation is extended to academic colleagues, legal experts, and institutions that have provided valuable insights, support, and constructive feedback throughout the research process. The authors also acknowledge the contribution of various sources of knowledge and references that have strengthened the analysis and discussion of this study. Hopefully, this research can provide meaningful contributions to the development of legal studies, particularly in the field of personal data protection and Artificial Intelligence governance. The authors appreciate every form of assistance and encouragement that has supported the successful completion of this work.

REFERENCES

- Akbar, N., Rais, R., & Nugroho, H. F. (2025). Personal Data Protection in the Era of Artificial Intelligence: A Critical Review of Indonesia's Regulatory Readiness Based on OECD Principles. *Global Journal of Law, AI & Ethics*. <https://doi.org/10.65917/gjlae.v1.i1.15>
- Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*. <https://doi.org/10.3389/fhumd.2024.1421273>
- Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2025). Challenges and conceptualizing ai-powered privacy risk assessments: Legal models for U.S. data protection compliance. *International Journal of Frontline Research in Multidisciplinary Studies*. <https://doi.org/10.56355/ijfrms.2025.5.1.0036>
- Conduah, A., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. *Digital Health*, 11. <https://doi.org/10.1177/20552076251343959>
- Ehimuan, B., Chimezie, O., Ob, Akagha, O., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*. <https://doi.org/10.30574/wjarr.2024.21.2.0369>
- Fatmawati, E., A., A. N., Rafa, M. F. F., Sari, A. R., & Hasibuan, M. (2025). DIGITAL RIGHTS REGULATION IN THE AI ERA: PRIVACY PROTECTION AND CONSUMER RIGHTS IN INDONESIA. *Journal of Social and Economics Research*. <https://doi.org/10.54783/jser.v7i2.1344>
- Fikri, A., & Amelia, T. (2024). Indonesia's Legal Policy on Protecting Personal Data from Artificial Intelligence Abuse. *SHS Web of Conferences*. <https://doi.org/10.1051/shsconf/202420407002>
- Goktas, P., & Grzybowski, A. (2025). Shaping the Future of Healthcare: Ethical

- Clinical Challenges and Pathways to Trustworthy AI. *Journal of Clinical Medicine*, 14. <https://doi.org/10.3390/jcm14051605>
- Gonçalves, A., & Correia, A. (2026). XAI-Compliance-by-Design: A Modular Framework for GDPR- and AI Act-Aligned Decision Transparency in High-Risk AI Systems. *J. Cybersecur. Priv.*, 6, 43. <https://doi.org/10.3390/jcp6020043>
- Hadiaty, S., & Saefullah, R. (2026). Assessing the Adequacy of Indonesia's Personal Data Protection Law (UU PDP No. 27/2022) Against Emerging AI-Generated Identity Fraud: A Comparative Legal Analysis. *International Journal of Humanities, Law, and Politics*. <https://doi.org/10.46336/ijhlp.v4i2.338>
- Hoxhaj, O., Halilaj, B., & Harizi, A. (2023). ETHICAL IMPLICATIONS AND HUMAN RIGHTS VIOLATIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE. *Balkan Social Science Review*. <https://doi.org/10.46763/bssr232222153h>
- Huda, M., Awaludin, A., & Siregar, H. K. (2024). Legal Challenges in Regulating Artificial Intelligence: A Comparative Study of Privacy and Data Protection Laws. *International Journal of Social and Human*. <https://doi.org/10.59613/g8dc9v94>
- Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*. <https://doi.org/10.58812/eslhr.v3i01.351>
- Kalodanis, K., Feretzakis, G., Anastasiou, A., Rizomiliotis, P., Anagnostopoulos, D., & Koumpouros, Y. (2025). A Privacy-Preserving and Attack-Aware AI Approach for High-Risk Healthcare Systems Under the EU AI Act. *Electronics*. <https://doi.org/10.3390/electronics14071385>
- Kaur, M., Sharma, N., Mehta, P. K., Dhanoa, M. K., & Anegebe, B. (2026). Data Protection Laws and Privacy Rights in the Digital Age: Legal Challenges and Emerging Frameworks. *Indian Journal of Law*. <https://doi.org/10.36676/ijl.v4.i1.162>
- Kulothungan, V. (2025). Using Blockchain Ledgers to Record AI Decisions in IoT. *IoT*. <https://doi.org/10.3390/iot6030037>
- Kurhayadi, K. (2025). Evaluating the readiness of public institutions for AI-Driven decision making: A framework for adaptive governance. *Edelweiss Applied Science and Technology*. <https://doi.org/10.55214/25768484.v9i4.6335>
- Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, 2025. <https://doi.org/10.1049/ise2/5536763>
- Mbah, G. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. *International Journal of Science and Research Archive*. <https://doi.org/10.30574/ijrsra.2024.13.2.2396>
- MohammadAmini, M., Jesus, M., Sheikholeslami, D. F., Alves, P., Benam, A. H., & Hariri, F. (2023). Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European

- GDPR Mandate. *Mach. Learn. Knowl. Extr.*, 5, 1023–1035. <https://doi.org/10.3390/make5030053>
- Muhidin, & Sudirman, L. (2025). Ethical Principles and Legal Responsibility in Artificial Intelligence: Ensuring Fairness and Accountability in AI Governance. *Journal of Law, Society and Living Norms*. <https://doi.org/10.66111/ctftkd63>
- Nwachukwu, P. S., Chima, O. K., & Okolo, C. H. (2025). The artificial intelligence governance framework for finance: A control-by-design approach to algorithmic decision-making in accounting. *Finance & Accounting Research Journal*. <https://doi.org/10.51594/farj.v7i8.2016>
- Ostian, Y. (2024). Artificial intelligence and personal data: privacy protection in the digital environment. *Uzhhorod National University Herald. Series: Law*. <https://doi.org/10.24144/2307-3322.2024.85.3.7>
- Purnomo, H. (2026). PERSONAL DATA PROTECTION IN INDONESIA'S DIGITAL LAW ENFORCEMENT SYSTEM. *AKSELERASI: Jurnal Ilmiah Nasional*. <https://doi.org/10.54783/jin.v8i1.1762>
- Putri, D. T. (2025). Regulating Digital Privacy in Indonesia: The Practice of Data Subject Rights and Controller Duties in the FotoYu App. *Istinbath: Jurnal Hukum*. <https://doi.org/10.32332/istinbath.v22i02.art01>
- Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Frontiers in Digital Health*, 7. <https://doi.org/10.3389/fdgth.2025.1431246>
- Ramadhan, M. H. R., Ramadhani, K., Isrok, M., Anggraeny, I., & Prasetyo, R. (2024). Legal Protection of Personal Data in Artificial Intelligence for Legal Protection Viewed From Legal Certainty Aspect. *KnE Social Sciences*. <https://doi.org/10.18502/kss.v8i21.14710>
- Satyo, B. K., M.Kn, Agung, B., & Prasetyo, Y. (2026). Artificial Intelligence and the Future of Human Rights: Legal Accountability for Algorithmic Decision-Making in Democratic Societies. *International Journal of Law and Social Sciences*. <https://doi.org/10.65960/ijlss.2.1.2026.12>
- Shaban, O., & Omoush, A. (2025). AI-Driven Financial Transparency and Corporate Governance: Enhancing Accounting Practices with Evidence from Jordan. *Sustainability*. <https://doi.org/10.3390/su17093818>
- Sun, H. (2025). Bridging the Accountability Gap in AI Decision-Making: An Integrated Analysis of Legal Precedents and Scholarly Perspectives. *Frontiers in Humanities and Social Sciences*. <https://doi.org/10.54691/24vexn67>
- Weiner, E., Dankwa-Mullan, I., Nelson, W., & Hassanpour, S. (2024). Ethical challenges and evolving strategies in the integration of artificial intelligence into clinical practice. *PLOS Digital Health*, 4. <https://doi.org/10.1371/journal.pdig.0000810>
- Williamson, S., & Prybutok, V. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Applied Sciences*. <https://doi.org/10.3390/app14020675>

- Yalid. (2025). The Concept Of Legal Norms Of Personal Data Protection Related To Data Processing In The Form Of Artificial Intelligence. *Jurnal Riset Multidisiplin Edukasi*. <https://doi.org/10.71282/jurmie.v2i1.75>
- Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Telecommunications Policy*. <https://doi.org/10.1016/j.telpol.2024.102851>
- Yoon, H., Belkhouja, M., & Dau, L. (2025). Privacy protection laws, national culture, and artificial intelligence innovation around the world. *Journal of International Business Studies*, 56, 853–873. <https://doi.org/10.1057/s41267-025-00790-2>
- Zahra, Y. (2025). Ensuring Data Privacy in the Age of Artificial Intelligence. *Journal of Computer Science Application and Engineering (JOSAPEN)*. <https://doi.org/10.70356/josapen.v3i2.66>
- Zisu, M.-A. (2025). Personal Data Protection in the Era of Artificial Intelligence: Legal Challenges and Solutions. *Anuarul Universitatii Petre Andrei Din Iasi - Fascicula: Drept, Stiinte Economice, Stiinte Politice*. <https://doi.org/10.63331/upalaw/34/23>