JOURNAL OF LEGAL AND SOCIAL CHANGES
Scientia Plus Corp
P-ISSN: 00000
E-ISSN: 00000

Evaluation Of Algorithmic Bias Potential In Ai Systems Within The Framework Of Personal Data Protection Laws

Tiara Saresty Dinda Pregiwati[1*] , Fachry Satrio Pringgowidigdo[2] , Khadijatun Nazmi[3] , Muhammad Naufal Nabil Aufa[4] , Yoga Galih Husodo[5] , Fara Via Alvida[6]

[1]Muhammadiyah University of Surakarta
[*]C100230468@student.ums.ac.id

Article

Keywords
Bias Algorithm; financial services sector; digital transformation; Artificial Intelligence; PDP

Article History:
Received: 17/12/2025
Reviewed: 20/12/2025
Accepted: 29/01/2026
Published: 31/01/2026

Abstract

Digital transformation has brought significant changes to the financial services sector, particularly through the application of Artificial Intelligence (AI) in customer risk analysis. AI improves efficiency and accuracy, but the extensive use of sensitive personal data raises risks of privacy violations, data misuse, and algorithmic bias, which can undermine fairness. Indonesia enacted Law Number 27 of 2022 on the Protection of Personal Data (PDP Law) as the legal foundation, yet this regulation has not fully anticipated the challenges and complexities of AI technology, such as algorithm transparency, independent audits, and accountability for automated decisions. This study employs normative legal research with statutory, conceptual, and case approaches to assess how well the UU PDP accommodates AI developments and the impact of algorithmic bias in customer risk analysis. The findings indicate that current regulation needs to be

strengthened with specific technical rules, the - establishment of independent supervisory bodies, and the implementation of AI governance in financial institutions. This research recommends adaptive regulations and inter-agency coordination to ensure effective and fair personal data protection in the digital era.

INTRODUCTION

The era of digital transformation has triggered a significant wave of innovation in the financial services sector. Amid increasingly intense competition, financial entities such as banks, finance companies, and financial technology companies are striving to improve operational efficiency, analytical accuracy, and competitive advantage. The key technology driving this change is *Artificial Intelligence* (AI), which, when applied specifically to customer risk analysis, has revolutionized conventional practices ranging from credit assessment processes and transaction monitoring for fraud detection to the personalization of financial products. However, behind the benefits of efficiency and optimization potential, there is a deep paradigmatic complexity in training and operating sophisticated AI systems. Financial entities require massive amounts of data as a key resource, most of which is sensitive customer personal data.

This data includes financial information, transaction history, digital footprints, and behavior patterns. Managing this type of data opens up risks related to privacy and security vulnerabilities. With the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia, this issue is no longer merely ethical, but has become an imperative legal obligation.

On the one hand, financial entities are encouraged to innovate; on the other hand, they are burdened with substantial responsibilities to protect customer data from potential misuse, algorithmic bias, and the threat of data leaks. Therefore, achieving the right balance between utilizing the potential of AI and ensuring personal data protection has become a critical focus and strategic challenge that will determine the future of a responsible and sustainable financial services sector.

In Indonesia, the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) is an important milestone in providing legal certainty regarding the privacy rights of citizens. However, with the rapid development of

technology , questions arise regarding the adequacy and accommodation of the technical and ethical aspects of AI use, particularly in the financial sector.

In addition, the use of AI also has the potential to cause algorithmic *bias*, which is the tendency for AI systems to produce subjective decisions due to unbalanced training data or discriminatory algorithm designs. This bias can have implications for unfairness in customer risk analysis, such as incorrect credit assessments or unfair treatment of certain groups.

Based on this, it is important to conduct this research to examine, legally and conceptually, the extent to which the Personal Data Protection Law has been able to adapt to the dynamics of AI technology, as well as how the risk of algorithmic bias can affect the accuracy and protection of customer personal data.

METHOD

This research is normative legal research, which focuses on reviewing the applicable positive legal norms and legal principles related to personal data protection in the use of *Artificial Intelligence* (AI) technology in the financial sector. This type of research is normative legal research, also known as *doctrinal legal research,* which examines law as a written norm or rule that regulates social relations.

This article uses *a statute approach* to examine regulations such as Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, as well as relevant Financial Services Authority regulations.

This article uses legal materials consisting of primary legal materials, namely laws and regulations related to personal data protection, information technology, and the financial sector. Legal materials were collected through a literature study by searching for laws and regulations, academic literature, official government documents, and scientific publications related to the research topic and analyzed qualitatively.

In addition, the novelty of this article lies in the formulation of an algorithmic bias evaluation framework based on the principles of the Personal Data Protection Law (Law No. 27 of 2022), which has so far been understood normatively and has not been operationalized in the context of artificial intelligence (AI) use. Unlike previous studies, which generally focused on the technical aspects of algorithmic bias or adopted foreign regulatory frameworks such as the GDPR and EU AI Act, this article offers a conceptual model for AI evaluation and governance rooted in Indonesia's national legal regime. Specifically, this article does not merely criticize the absence of AI regulations in the PDP Law, but also constructs a framework of AI accountability for data

controllers by using the principles of the PDP Law as *a legal-ethical benchmark* to assess, prevent, and mitigate algorithmic bias. Thus, the novelty of this research lies at the intersection of law, data protection, AI ethics, and algorithmic governance, which has not been widely developed in Indonesian legal literature to date.

RESULTS AND DISCUSSION

Definition and Typology of Algorithmic Bias

In an academic context, algorithmic bias is defined as the tendency of an AI system to produce *outputs* that systematically disadvantage or advantage certain groups due to data imbalance, model design, or the context of the system's application. Algorithmic bias itself is not singular but multidimensional, which can be classified as follows.

1) *Data Bias*, which arises at the stage of collecting and processing *training data,* includes:
   - *Sampling bias*, which is data that does not fairly represent the population.
   - *Label bias*, which is errors or prejudices in the labeling of historical data.
2) Model bias *(Model or Objective Function Bias)*, which originates from:
   - Algorithm design.
   - Objective functions that prioritize efficiency and profit.
3) *Deployment or Contextual Bias*, which arises due to:
   - How the AI system is implemented.
   - Use outside the original design context.
   - Lack *of human oversight.*
4) Sensitive Variable Bias and Proxy Bias, which arise when:
   - Sensitive variables (age, gender, region) are used directly.
   - Or are replaced by *proxy* variables that indirectly represent these sensitive characteristics.

The Personal Data Protection Law has sufficiently accommodated the development of AI technology in the context of customer risk analysis.

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is an important milestone in the Indonesian legal system that legitimizes individual privacy rights in the digital era. This regulation marks the presence of a comprehensive legal umbrella regarding the management of personal data, ranging from the definition of personal data, principles of lawful processing, obligations of data controllers and processors, to regulations regarding the rights of data subjects and sanctions for violations. These provisions provide a legal basis for financial institutions in managing customer data, including the use of Artificial Intelligence (AI) technology for risk analysis. Thus, normatively, the

PDP Law has provided a legal protection framework that Indonesia previously did not have comprehensively.

However, the rapid development of artificial intelligence technology has brought new challenges that are not yet fully accommodated in the substance of the PDP Law. In financial institution practices, the use of AI is commonly found in credit scoring, fraud detection, and risk analysis processes that rely on big data processing. AI systems are capable of automatically processing large amounts of data and generating instant decisions without human intervention. Although efficient, this automated nature raises legal issues, such as a lack of algorithm transparency, difficulty in determining accountability for the decisions produced, and the potential for discrimination due to data bias. This situation shows that the complexity of AI cannot be fully addressed by the general norms in the PDP Law, which is still oriented towards conventional data processing systems.

The results of normative analysis show that the PDP Law has regulated important principles relevant to the use of AI, such as lawfulness of processing, purpose limitation, data minimization, accuracy, and security. In addition, the PDP Law also guarantees the fundamental rights of data subjects, including the right to obtain information, correct erroneous data, withdraw consent, and delete personal data (right to be forgotten). In the context of financial institutions, these rights are the main instruments for protecting customers whose data is processed for risk analysis purposes. For example, in accordance with Article 15 of the PDP Law, financial institutions are required to obtain explicit consent from customers before using their personal data for AI model training. This provision shows that, normatively, legal protection mechanisms are in place to prevent customer data from being processed arbitrarily.

However, when these provisions are applied to the practical use of AI, it is apparent that the PDP Law is still too general. There are no explicit provisions on the obligation of algorithm transparency, independent audits of AI systems, or legal liability for errors or biases in automated decisions— . In practice, AI systems can automatically reject credit applications or assign high risk levels without explaining the reasons behind these decisions. This has the potential to violate the data subject's right to obtain an explanation and to reject automated decisions. Unfortunately, the PDP Law does not explicitly regulate the right to explanation as stipulated in data protection regulations in several international jurisdictions.

Another apparent weakness is the lack of detailed regulations on cross-border data transfers. Many financial institutions use cloud services or AI technology providers based overseas. This situation causes customers' personal data to be transferred to foreign jurisdictions that may not have protection

standards equivalent to those in Indonesia. Although Article 56 of the PDP Law regulates the transfer of data abroad, the provisions are still normative and require implementing regulations so that data transfer mechanisms can be properly monitored. Without strict supervision, customers' personal data could potentially be used outside the permitted context, especially in the AI model training process, which requires large volumes of data.

Apart from legal issues, the PDP Law has not yet substantially addressed the ethical and social dimensions of AI use, particularly in relation to algorithmic bias. AI systems in customer risk analysis are usually trained with historical data. If this data contains bias, the analysis results can be discriminatory against certain groups—for example, based on age, region, or employment status. Although the PDP Law regulates the principles of data fairness and accuracy, it does not provide technical guidance or algorithmic audit obligations for financial institutions. This contrasts with the provisions of the European Union's General Data Protection Regulation (GDPR) and EU AI Act, which explicitly require risk testing, algorithmic audits, and AI model transparency in the context of protecting individual rights.

Table 1.1 Comparison

Comparison Aspect	Indonesian PDP Law (Law No. 27 of 2022)	EU GDPR	EU AI Act
Regulatory Focus	Personal Data Protection	Data protection and subject rights	Risk-based AI regulation
AI Regulation	Implicit	Implicit *(profiling* and ADM)	Explicit and comprehensive
Algorithmic bias	Not specifically regulated	Prevented through the principle of non-discrimination	Strictly regulated and must be mitigated
Automated Decisions	Not specified	Restricted and can be rejected	Strictly monitored *(high-risk* AI)

Risk Assessment	None	Mandatory DPIA	Mandatory *risk assessment*
Algorithm Audit	General and normative	Right to explanation	Mandatory
AI transparency	Not specifically regulated	Credit *profiling is* restricted	Mandatory technical documentation
Financial Sector	Inadequate	Integrated with human rights	Credit assessment = High-risk AI
Ethical and Social Dimensions	Not yet adequate	Human rights integrated	Forming the basis of regulation

This table shows that Indonesia's PDP Law is still normative in nature, while the GDPR and EU AI Act have adopted a technical and ethical approach in anticipating the risk of discrimination due to the use of AI, particularly in the financial sector.

From an institutional perspective, the implementation of the PDP Law in the financial sector still faces practical obstacles. To date, a number of derivative regulations of the PDP Law are still being drafted, including the establishment of an independent personal data supervisory agency. Without a strong supervisory agency, the supervision of AI-based personal data processing cannot be carried out optimally. On the other hand, financial institutions under the supervision of the Financial Services Authority (OJK) tend to focus on compliance with financial regulations alone, without adequate internal mechanisms for auditing and supervising AI-based personal data processing. As a result, even though they are legally subject to the PDP Law, its implementation in the field still leaves significant gaps in supervision.

In the context of the legal relationship between data controllers and processors, the PDP Law has clarified the division of responsibilities between the two parties. However, in practice, these boundaries are often blurred when financial institutions collaborate with third-party AI service providers. These

providers not only carry out instructions but also play a role in algorithm development and automated decision-making. This situation raises the question of who should be held legally responsible in the event of data breaches or discrimination resulting from AI system decisions.

From the perspective of data subjects' rights, the use of AI for risk analysis raises concerns about the extent to which personal data is used and the extent to which customers have control over it. When transaction data, digital history, or even social media are used in risk assessment systems, customers often do not understand that their data has been processed to that extent. Although the PDP Law guarantees the right to obtain information and withdraw consent, exercising these rights is difficult in the context of AI systems that operate automatically and are complex. Furthermore, AI models are "black boxes," making it difficult to explain their decisions. This situation highlights the need for additional regulations that affirm customers' rights to obtain explanations and object to automated decisions.

When compared to developments in international law, Indonesia still lags behind in regulating the use of AI. The European Union, through the GDPR, has given individuals the right not to be subject to automated decisions that have significant legal implications, and has introduced the AI Act, which requires certification and auditing for high-risk AI systems. Singapore and Japan have even implemented AI governance frameworks that emphasize algorithm transparency and accountability. Meanwhile, Indonesia is still in the early stages, where the PDP Law serves as a general basis, but has not been supplemented with technical regulations that explicitly address ethical, accountability, and oversight aspects of AI in the financial sector.

Table 1.2 Comparison of Indonesian Law with International Law

Aspect	Indonesia	European Union	Singapore	Japan
Legal Instruments	Law No. 27 of 2022 on PDP	GDPR and EU AI Act	*AI Governance Framework* Model	*AI Governance Guidelines*
Right to Automated	Not explicitly regulated	Right to object to	Recognized in principle	Recognized normatively

Decision-Making		automated decisions with legal consequences		
High-Risk AI Regulation	No classification	Classified and strictly supervised	Context-based approach	Impact-based approach
AI Audit/Certification	Not regulated	Mandatory for high-risk AI	Recommended	Recommended
Algorithm Transparency	General principles	Right to explanation and technical documentation	Key principles	Key principles
Financial Sector	Not specifically regulated	*Credit scoring* = high-risk AI	Focus on *fairness and trust*	Focus on standard mitigation
Ethics and Accountability Dimensions	Not yet accommodated	Integrated *human* rights and *human- -based oversight*	Becoming the foundation of policy	Becoming a core principle

Through normative legal analysis, it can be concluded that the PDP Law has provided an important legal basis for personal data protection, but it is not yet fully adaptive to the dynamic and multidimensional characteristics of AI technology. The PDP Law is "technology-neutral," meaning that it does not directly mention or regulate terms such as artificial intelligence, machine learning, or automated decision-making. Consequently, the application of PDP Law principles to the context of AI requires broad interpretation, which has the

potential to create legal uncertainty. This normative vacuum not only affects financial institutions as data controllers, but also customers as data subjects who have the right to privacy.

Therefore, more specific implementing regulations are needed to regulate the use of AI in personal data processing. These regulations should include algorithm audit obligations, legal responsibility for automated decisions, transparency obligations for financial institutions, and objection mechanisms for customers. Regulations regarding cross-border data flows also need to be clarified so that protection standards are maintained, even if the data is processed by foreign service providers.

From an institutional perspective, the establishment of an independent and technologically competent personal data supervisory authority is urgent. This institution needs to coordinate with the OJK and Bank Indonesia in overseeing the implementation of AI systems in the financial sector. In addition, financial institutions must develop internal policies on AI governance, which include algorithm audits, risk assessments, and improving the ethical and legal literacy of employees. Public education on the rights of data subjects is also important to ensure that the public can exercise their rights effectively.

Thus, the results of this study show that although the Personal Data Protection Law has become an important foundation for the national legal system, this regulation has not been fully able to accommodate the development of AI technology in the context of customer risk analysis in financial institutions. There are still normative gaps and implementation weaknesses that need to be addressed immediately so that personal data protection can be effective and in line with the principles of fairness, transparency, and accountability. To that end, synergy between the government, regulators, financial institutions, and the public is needed to create a legal ecosystem that is adaptive to technological innovation but remains oriented towards the protection of human rights.

Potential Forms *of* Algorithmic Bias in AI Systems that Can Affect the Accuracy of Risk Analysis and Data Protection

Algorithmic bias is the tendency of artificial intelligence (AI) systems to produce biased decisions due to imbalances in training data, discriminatory algorithm design, or errors in the data interpretation process. In the context of financial institutions, algorithmic bias is a critical issue because AI plays a major role in determining risk analysis, credit granting, and fraud detection. When algorithms operate based on historical data that contains social preferences or discrimination, the results of the analysis can reinforce existing injustices.

According to Mehrabi et al. (2021) in the Journal of Artificial Intelligence Research, algorithmic bias can arise in three main stages, namely (1) data collection bias, when the data collected does not fairly represent the population; (2) algorithmic design bias, when the structure or parameters of the model reinforce discriminatory patterns; and (3) output bias, when the final results of the system have a negative impact on certain groups. In the practice of customer risk analysis, this can be seen when AI systems are more likely to assign high risk scores to groups of people with low economic profiles or from certain regions even though their actual financial data is acceptable.

Research by Kamiran & Calders (2022) confirms that bias in AI systems often stems from historical bias—that is, pre-existing social bias in the training data. For example, if a bank's historical data shows that most bad debts occur among low-income groups, the algorithm may consider all customers in that group to be high risk, without taking other individual factors into account. This condition clearly contradicts the principles of fairness and non-discrimination guaranteed in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

In addition, technical bias is also a challenge. Zliobaite's (2023) research in the AI & Ethics Journal explains that complex machine learning models (such as neural networks) are "black boxes," making it difficult to explain the reasons behind the decisions made by the system. The lack of transparency in these algorithms makes legal oversight difficult because there is no mechanism to ensure that automated decisions have been made fairly. In the context of customer data protection, this may violate the data subject's right to obtain an explanation of decisions that have legal implications, as stipulated in the principle of the right to explanation.

From a legal protection perspective, algorithmic bias poses a double risk. First, there is the risk of customer risk misclassification, which can lead to customers being unfairly denied financial services. Second, there is the risk of privacy violations, as biased AI systems can access and interpret personal data outside of its intended context. Chen et al. (2024) in Computers & Security found that AI-based financial systems that use digital behavior data (social media traces, location, and online activities) often result in over-profiling—the use of personal data beyond its original purpose, thereby potentially violating the principles of purpose limitation and data minimization in the PDP Law.

To address this, there needs to be an algorithmic accountability policy that requires financial institutions to conduct independent audits of the AI systems they use. These audits aim to identify and minimize bias and ensure that models do not produce discriminatory decisions. The European Commission (2023) in the

EU Artificial Intelligence Act emphasizes the importance of risk-based regulation, whereby high-risk AI systems (including financial risk analysis systems) must undergo risk assessment, certification, and transparency audits. Indonesia can adopt a similar approach through implementing regulations of the PDP Law so that the oversight mechanism is not only administrative but also substantive and technological.

In addition to audits, the implementation of an ethical AI framework in financial institutions is also an urgent need. This framework includes the principles of transparency, accountability, and fairness. According to Sukmana et al. (2022) in the Indonesian Journal of Law and Technology, the application of AI ethics in financial institutions is still limited to administrative compliance aspects and has not touched on technical mechanisms such as fairness testing or periodic algorithmic audits. Therefore, the Financial Services Authority (OJK) and the Ministry of Communication and Information Technology need to develop technical guidelines on AI governance that integrate legal, ethical, and technological aspects.

Conceptually, algorithmic bias also raises legal accountability issues. If discriminatory decisions originate from automated systems, who is responsible? In the context of the PDP Law, data controllers still have primary responsibility, but the division of responsibility with third-party AI technology providers is often unclear. Hoffmann et al. (2021) in the Harvard Journal of Law & Technology suggest that contracts between financial institutions and AI technology providers include clauses on shared accountability and the obligation of model transparency ( ) for external audits. This is in line with the principles of fairness and protection of data subjects' rights.

Thus, potential algorithmic bias in AI systems can affect the accuracy of customer risk analysis and weaken personal data protection. Without strong oversight and algorithmic transparency, financial institutions risk violating citizens' digital rights. Therefore, Indonesia needs to strengthen the regulations derived from the PDP Law with algorithmic audit mechanisms, automatic decision transparency obligations, and the establishment of an independent supervisory agency with the technical capacity to assess AI systems. Only through these steps can digital justice and customer rights protection be guaranteed in the era of artificial intelligence-based financial transformation.

On the other hand, the development of artificial intelligence (AI) technology has brought significant advances in the financial sector, particularly in credit risk analysis, fraud detection, and customer data security systems. However, behind the efficiency and automation offered, there is a phenomenon called algorithmic bias, which is the tendency for AI systems to produce unfair,

discriminatory, or inaccurate decisions due to imbalances in training data, model design, and algorithm parameters. Algorithmic bias can take various forms, including historical data bias, which occurs when past data reflects social or economic inequalities, causing AI models to learn from unfair data; representation bias, which occurs when data does not include balanced representation of all customer groups; measurement bias, which arises from errors in the collection or use of irrelevant indicators; pure algorithmic bias, which is caused by errors in model logic or algorithm parameters that favor certain groups; and interaction bias, which arises from user behavior that influences the model's learning data.

Algorithmic bias has a direct impact on the accuracy of risk analysis and customer data protection. If AI models are unfair or unbalanced, risk assessment results can be misleading, for example, rejecting customers who are actually creditworthy and instead accepting high-risk customers. In the context of data protection, bias can also cause problems because models often use sensitive personal data such as transaction history, location, and online behavior. If data processing is carried out without the principles of fairness and transparency, this has the potential to violate privacy rights protected by regulations such as the Personal Data Protection Law (PDP Law) No. 27 of 2022.

To mitigate these risks, various mitigation efforts are needed, such as independent data and model audits to identify potential discrimination , data diversification to ensure more balanced representation of various social, economic, and demographic groups, and the application of Explainable AI (XAI) to enable interpretation and transparency of algorithmic decisions. In addition, the establishment of ethical AI governance or an internal ethics council can help assess the ethical and legal risks of AI implementation, while regulation and compliance with international guidelines such as those of the OECD and the European Commission are important to ensure the responsible use of AI.

Thus, algorithmic bias poses a real threat to the objectivity and accuracy of AI systems, especially in the financial sector, which relies heavily on data for risk analysis. When AI models operate based on unbalanced data, the impact is not only technical errors but also violations of the principles of fairness and personal data protection. Therefore, financial institutions need to balance efficiency and algorithmic fairness through oversight, transparency, and policies oriented toward protecting customer rights.

CONCLUSION

This study reveals that the implementation of Artificial Intelligence (AI) in financial institutions yields substantial benefits, including increased efficiency, speed, and accuracy of analysis. However, these benefits come with significant vulnerabilities to personal data misuse and the risk of algorithmic bias that could

potentially harm customers. From a legal perspective, Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) has established a fundamental basis for protecting personal data, but it is not yet fully responsive to the complexity of ever-evolving AI technology.

The main findings of the study show that the PDP Law does not explicitly regulate crucial aspects, such as algorithm transparency, accountability mechanisms for automated decisions, independent audit obligations, and cross-border data utilization in AI models. This condition creates regulatory loopholes that can undermine the protection of customer privacy rights. Furthermore, the potential for algorithmic bias has been proven to affect the accuracy of risk assessments, particularly when models learn from historical data that is unbalanced or contains discrimination. Such bias has an impact on unfairness in credit scoring, risk assessment, and access to financial services. Similarly, the research results comprehensively indicate that Indonesia is still in the early stages of integrating data protection with AI governance. More robust harmonization between technology policies, data protection regulations, and the operational practices of financial institutions is needed to ensure that digital transformation takes place in a responsible and fair manner.

REFERENCES

Aritonang, Lenny Maria, Zyetwill Zyetwill, and Rara Handayani. 2025. "Legal Analysis of Personal Data Leaks and Identity Abuse in Banking Based on Law Number 27 of 2022 concerning Personal Data Protection." *Ranah Research: Journal of Multidisciplinary Research and Development* 7(5): 3146–58.

Fatmala Putri, Dewi, and Widya Ratna Sari. 2023. "Analysis of BSI Customer Protection Against Data Leaks in Using Digital Banking." *Scientific Journal of Economics and Management* 1(4): 173–81. https://doi.org/10.61722/jiem.v1i4.331.

Jamal Wiwoho. 2014. "Jamal Wiwoho." *The Role of Banks and Non-Bank Financial Institutions in Providing Fair Distribution for the Community*: 4. https://ejournal.undip.ac.id/index.php/mmh/article/view/9028.

Putri, ANTM, and L Nurhisam. 2025. "Implementation of Artificial Intelligence Technology in the Operations of Sharia Financial Institutions." *At-Tasharruf; Journal of Sharia Economics and* Business Studies 7(1):78–90. https://ejurnal.unmuhjember.ac.id/index.php/Tasharruf/article/view/3628%0Ahttps://ejurnal.unmuhjember.ac.id/index.php/Tasharruf/article/download/3628/1069.

Revalina, et al. 2025. "Revalina+Annisa+Antoine+3147." *Multidisciplinary Academic Journal* 2 (Misuse of Personal Data in Digital Transaction Technology in the Digital Banking Industry (Case Study of PT. Bank Syariah Indonesia)): 316–27.

Sulistyowati, Yayuk Sri Rahayu, and Chifni Darum Naja. 2023. "Application of Artificial Intelligence as Innovation in the Era of Disruption in Reducing the Risks of Sharia Microfinance Institutions." *Wadiah: Journal of Islamic Banking* 7(2): 117. https://jurnalfebi.iainkediri.ac.id/index.php/wadiah/article/view/329.

Wiriani, E, J Maknuni, E A Puspita, and ... 2025. "The Role of Artificial Intelligence in Mitigating Mobile Banking Transaction Risks: A Review of Governance and Data Ethics." JournalofTrends…6(1):103–11. https://www.journal.fkpt.org/index.php/jtear/article/view/2223.

Rais, N. A. R., & Nugroho, H. F. (2025). *Personal Data Protection in the Era of Artificial Intelligence: A Critical Review of Indonesia's Regulatory Readiness s Based on OECD Principles*. Global Journal of Law, AI & Ethics, 1(1), 14–19.

Junaidi, & Fadzil, R. M. (2024). Urgency of legal personal data protection in e-commerce transactions involving artificial intelligence. *Walisongo Law Review*, 6(2), 96–108. https://doi.org/10.21580/walrev.2024.6.2.25548

Barokah, K., Yuliati, & Madjid, A. (2024). Reconstructing legal liability models for AI misuse on personal data privacy in Indonesia: A constitutional law and regulatory perspective. *NEGREI: Academic Journal of Law and Governance*, 4(1), 203–210. https://doi.org/10.29240/negrei.v4i1.13199

Yuniari, I. D. A. W., & Mayasari, I. D. A. D. (2022). Legal protection of customer personal data when banks use artificial intelligence technology according to positive law in Indonesia. *Jurnal Kertha Negara*, 10(7), 665–675.

Yudha, M. W., Ramli, A. M., & Ramli, T. S. (2025). The use of personal data as a means of artificial intelligence training: A comparative study of privacy rights protection in Indonesia and the European Union. *CAUSA: Journal of Law and Citizenship*, 12(7). https://doi.org/10.3783/causa.v2i9.2461

Sianturi, O. J. M., Syahrasyid, M. Z., & Setiawan, K. A. (2025). Accountability crisis in the era of artificial intelligence: Legal analysis of algorithmic decision-making and its implications for the Indonesian legal system. Proceedings of the National Seminar on Information Technology & Computer Science (SEMASTER), 4(1), 98–102.

Saputra, R. F., Zamsuri, A., & Amri, A. D. (2025). Ethical challenges of technology in the use of artificial intelligence: Privacy, bias, and accountability in education in Indonesia. SEMASTER Proceedings, 4(1), 65–71.

Fitrianto, B. (2025). Legal Review of Bank Liability for Customer Losses Due to Artificial Intelligence (AI) in Credit Decision Making. *Milthree Law Journal, 1(1).*

Chairunnisa, S., & Amaniar, F. (2025). *AI and the Future: Ethical Challenges for Generation Z*. *4*(2023).

Informatika, J., & Vol, U. (2024). *No Title*. *2*(2), 128–153.

Kerta, W., Hukum, J., & Hindu, A. (2025). *No Title*. *8* (November), 98–109.

Kirana, K. B., & Silalahi, W. (2025). *Challenges of Artificial Intelligence (AI) Regulation from the Perspective of Personal Data Protection Law in Indonesia*. *5*(6), 1807–1817.

Mardohar, A., Togatorop, H., & Darmawan, D. W. (2024). *Digital Transformation in Achieving Sustainability in the Economic and Financial Sectors*. *7*, 16–31.

Samita, G. R., Wisesa, W., Setiawan, E. D., Hidayat, R., Rationality, B., Data, B., Cognitive, B., Algorithmic, B., Data, K., & Organization, E. (2025). *Integration of Artificial Intelligence and Bounded Rationality Theory in Addressing Business Decision-Making Uncertainty in the Big Data Era*. *2*(2), 1–12.

Sholihin, U. (2024). *Enhancing the Competitiveness of the MSME Market Through Digital Transformation*. *3*(2).