Proceeding of International Conference Technology, Economics, and Social Science
Vol 1, No 1, January 2026, Page 758-765
ISSN 3124-6087 (Media Online)
https://journals.adaresearch.or.id/ictess

Regulatory Reconstruction of AI-Generated Risk Profiling in Murabahah Financing: Harmonizing the Personal Data Protection Act, Hifz al-Māl, and Pancasila to Prevent Data-Driven Cybercrime

Raihan Imam Cahya Akbar*, Ramlan, Ida Nadirah

Faculty of Law, Doctor of Law Study Program, Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia
Jl. Denai No. 217, Kec. Medan Denai, Kota Medan, Sumatera Utara, 20226, Indonesia
Email: [1,*]raihanakbar06@gmail.com, [2]ramlan@umsu.ac.id, [3]idanadirah@umsu.ac.id
Correspondence Author Email: raihanakbar06@gmail.com
Submitted: **02/12/2025**; Accepted: **07/01/2026**; Published: **25/01/2026**

Abstract−This research investigates the fragmented regulatory governance surrounding artificial intelligence (AI)-generated risk profiling in murābaḥah financing within Indonesian Islamic banking, focusing on its alignment with the Personal Data Protection Act (PDP Act), the Islamic legal objective of hifz al-māl (protection of wealth), and the ethical foundations of Pancasila. Conducted across three Islamic banking institutions in Jakarta and Bandung, the study employs a normative–empirical legal research design and draws on in-depth interviews with twelve purposively selected respondents, including risk management officers, cybersecurity specialists, sharīʿah compliance personnel, and regulatory experts. Data were analyzed using statutory interpretation, comparative regulatory review, thematic coding, and qualitative risk assessment. The findings reveal that AI-generated profiling systems operate within a regulatory vacuum, characterized by inconsistent data protection practices, opaque algorithmic processes, and limited integration of sharīʿah principles and Pancasila-based ethical values. The absence of fairness audits, explainability mechanisms, and AI-specific security controls heightens institutions' exposure to data-driven cybercrime, while simultaneously undermining Islamic obligations to prevent harm and safeguard financial wellbeing. These results demonstrate that the PDP Act alone is insufficient to govern AI profiling in Islamic finance without harmonization with Islamic legal and ideological norms. The study proposes a Tri-Axial Regulatory Reconstruction Model as a pathway for establishing a coherent, ethically grounded, and legally compliant framework for AI adoption in Islamic banking.

Keywords: Murābaḥah Financing; AI Governance; Hifz Al-Māl; Pancasila Ethics; Personal Data Protection; Islamic Banking; Algorithmic Transparency

1. INTRODUCTION

Artificial intelligence (AI)–generated risk profiling is rapidly reshaping credit assessment practices in Islamic banking, including *murābaḥah* financing, which remains one of the most dominant products in Indonesia's *sharīʿah* banking portfolio. Digital onboarding, alternative data–driven scoring, and automated eligibility decisions promise greater speed, personalization, and financial inclusion compared to traditional manual appraisal (Fitria, 2025). However, the same algorithmic capacities that enable granular risk assessment also intensify vulnerabilities related to personal data exploitation, profiling opacity, and cybercrime. The Indonesian Law No. 27 of 2022 on Personal Data Protection (*Undang-Undang Pelindungan Data Pribadi*, PDP Act) explicitly recognizes the risk of material and immaterial harm arising from misuse or security breaches of personal data, and seeks to restore public trust in digital processing ecosystems (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022). In parallel, the ethical architecture of Indonesian Islamic finance is normatively anchored in *maqāṣid al-sharīʿah*, particularly *hifz al-māl* (protection of wealth), and the state's foundational ideology, Pancasila, which demands that technological innovation be aligned with social justice, human dignity, and the common good. These concurrent normative domains positive data protection law, Islamic ethical objectives, and Pancasila values have not yet been systematically harmonized for AI-based risk profiling in *murābaḥah* financing, creating a critical regulatory and doctrinal gap.

Existing scholarship has begun to map aspects of this terrain but remains fragmented. Hidayanti et al. and other systematic literature reviews on AI in Islamic financial services highlight how AI can enhance efficiency, inclusion, and service quality while being framed within *maqāṣid al-sharīʿah*, including *hifz al-māl* and public welfare (Hidayanti et al., 2025). These studies show that AI can support property protection by reducing default risk, improving fraud detection, and enabling more accurate customer profiling, yet they largely treat "risk management" at a conceptual level and do not address the specific legal intricacies of AI-generated risk scoring models in *murābaḥah* contracts or their intersection with national data protection law. Likewise, recent analyses of AI's role in enhancing *sharīʿah* compliance and social impact in Banking 4.0 emphasize fraud detection and real-time *sharīʿah* auditing as tools that operationalize *hifz al-māl* and justice (*ʿadl*). Yet these contributions remain focused on internal compliance and governance rather than the external rights of data subjects and the prevention of data-driven cybercrime.

On the regulatory side, several recent legal studies examine the alignment of AI-based credit scoring and fintech practices with Indonesia's PDP Act and related financial regulations. Research on personal data protection in credit scoring platforms shows persistent tensions around transparency, lawful basis for processing, automated decision-making, and the right to explanation in AI-based credit decisions (Cristine et al., 2025). Policy briefs and legal analyses likewise stress the need to strengthen supervisory mechanisms, clarify responsibilities of data controllers, and establish robust data protection authorities during the PDP transition period, particularly in the context of *innovative credit scoring* and digital lending ecosystems (Rachbini et al., 2023). However, these works focus primarily on conventional fintech and peer-to-

peer lending; they rarely scrutinize Islamic banking products, let alone *murābaḥah* specifically nor do they integrate Islamic ethical doctrines or Pancasila philosophy as explicit normative parameters for reconstructing AI governance.

A parallel body of literature explores the ethical and ideological foundations for AI regulation in Indonesia. Studies on Pancasila and AI underline that AI governance should be grounded in the nation's philosophical values, emphasizing fairness, inclusivity, and social justice, and cautioning against technocratic approaches divorced from human dignity and collective welfare (Ma'unah et al., 2025). Regulatory documents and ethical guidelines, including the financial regulator's code of ethics for responsible and trustworthy AI in the fintech industry, explicitly state that AI must be based on Pancasila and must not harm users or exacerbate inequality(OJK, 2023). Yet this line of work typically remains at the macro-policy level: it does not descend into the micro-regulatory structures of particular financial contracts such as *murābaḥah*, nor does it articulate how Pancasila values should concretely inform the handling of sensitive risk profiling data, algorithm design choices, or remedies against data-driven cybercrime.

Within Islamic banking studies, recent research on *murābaḥah* in Indonesia has identified operational and contractual challenges, such as information asymmetry, documentation weaknesses, and deviations from the intended asset-backed nature of the product in practice (Ikhwan et al., 2025). In parallel, scholarship on digitalization in Islamic banking discusses the use of AI-driven risk assessment tools to evaluate customer eligibility in ways that are more ethical and *sharīʿah*-compliant than conventional credit scoring (Fitria, 2025). However, these studies largely treat risk profiling as a technical or managerial tool; they do not examine how AI-generated profiles may themselves become vectors of cybercrime for instance, through data breaches, identity theft, unauthorized secondary use, or discriminatory profiling and they seldom integrate the PDP Act with *hifz al-māl* and Pancasila into a coherent regulatory reconstruction.

Accordingly, the central research problem addressed in this study is the absence of an integrated normative and regulatory framework for AI-generated risk profiling in *murābaḥah* financing that simultaneously satisfies the requirements of the Personal Data Protection Act, realizes the objective of *hifz al-māl* within *maqāṣid al-sharīʿah*, and embodies the ethical imperatives of Pancasila. Current regulatory arrangements treat these domains separately: the PDP Act focuses on data subject rights, obligations of controllers, and sanctions; Islamic legal discourse addresses wealth protection, fairness, and contractual integrity; while Pancasila-based AI ethics emphasize macro-level social justice and human dignity. In practice, Islamic banks implementing AI-based risk profiling models face norm collisions and regulatory blind spots for example, when highly granular profiling based on alternative data enhances predictive accuracy but simultaneously increases the attack surface for cybercrime and threatens the dignity and autonomy of financing applicants. This research is therefore urgently needed for at least three reasons. First, the proliferation of AI-generated risk profiling in Indonesian financial services is accelerating faster than the refinement of doctrinal and regulatory safeguards, especially in Islamic banking where *murābaḥah* continues to dominate portfolios and is often marketed to relatively vulnerable retail customers. Second, data-driven cybercrime ranging from unauthorized access and data leakage to profiling-based fraud and social engineering targets precisely the kinds of rich behavioral and financial data that AI risk engines depend upon, thereby turning tools designed for *hifz al-māl* into potential instruments of wealth erosion. Third, failing to harmonize PDP norms with Islamic ethical obligations and Pancasila values risks producing a fragmented governance regime that undermines public trust in both Islamic finance and digital regulatory reform.

This study offers a regulatory reconstruction of AI-generated risk profiling in *murābaḥah* financing by proposing a harmonized framework that triangulates the PDP Act, *hifz al-māl*, and Pancasila. Conceptually, the research develops an integrated normative matrix that maps key PDP principles (lawfulness, purpose limitation, data minimization, accountability) onto the *maqāṣid* of wealth protection and the Pancasila-based demands for social justice, humanity, and the protection of citizens from technological harm. Methodologically, it reinterprets AI-generated risk profiling as a legally relevant "decision space" in which algorithmic transparency, explainability, security-by-design, and human oversight become *sharīʿah* and Pancasila obligations, not merely technical options. Practically, the study formulates concrete regulatory and institutional recommendations such as mandatory impact assessments linking data protection risks to *hifz al-māl*, strengthened duties of care for Islamic banks deploying AI scoring in *murābaḥah*, and Pancasila-based ethical thresholds for data use and model design aimed at preventing data-driven cybercrime while preserving the efficiency benefits of AI. The state-of-the-art contribution of this research lies in its explicit normative integration: whereas prior studies have separately explored AI in Islamic finance, PDPA-based credit scoring, or Pancasila-oriented AI ethics, this article is, to the best of the author's knowledge, the first to reconstruct the legal and ethical governance of AI-generated risk profiling in *murābaḥah* by jointly mobilizing the Personal Data Protection Act, *hifz al-māl* within *maqāṣid al-sharīʿah*, and Pancasila. The research contributes theoretically by advancing a tri-axial normative framework for AI governance in Islamic finance; doctrinally by offering an interpretive model for reading the PDP Act through *maqāṣid* and Pancasila; and practically by providing a set of policy-relevant design principles and safeguards that Islamic banks and regulators can adopt to ensure that AI-driven *murābaḥah* risk profiling becomes a vehicle for wealth protection and social justice rather than a catalyst for data-driven cybercrime.

2. RESEARCH METHODS

2.1 Basic Research Framework

This study employs a normative–empirical legal research design to reconstruct the regulatory governance of AI-generated risk profiling in *murābaḥah* financing by harmonizing the Personal Data Protection Act (PDP Act), the Islamic legal

principle of *hifz al-māl*, and Pancasila-based ethical imperatives. The normative dimension focuses on analyzing statutory regulations, *fatwa* frameworks, Islamic legal sources, and ethical guidelines relevant to AI governance, while the empirical component explores how Islamic banking practitioners currently implement AI-driven credit assessment systems. The empirical phase involves in-depth interviews with 12 respondents, consisting of Islamic banking risk officers, IT and cybersecurity specialists, *sharīʿah* compliance personnel, and regulatory experts. These respondents were selected through purposive sampling, and the fieldwork was conducted in three major Islamic banking institutions located in Jakarta and Bandung, which represent diverse levels of digitalization maturity in risk profiling practices.

The research framework is built upon the premise that AI-generated risk profiling, though operationally beneficial, creates new vulnerabilities that challenge existing regulatory structures. Accordingly, the study formulates the following hypotheses: (1) AI-generated risk profiling in *murābaḥah* financing currently operates in a fragmented regulatory environment that does not yet integrate PDP Act obligations, *hifz al-māl*, and Pancasila values; (2) the absence of harmonized regulatory guidelines increases the risk of *data-driven cybercrime* and weakens consumer protection; (3) a reconstructed regulatory framework grounded in these three normative pillars can provide more robust safeguards and enhance compliance integrity. The study analyzes three primary variables: (a) *Regulatory Adequacy*—the extent to which existing laws and guidelines address AI-based risk profiling; (b) *Ethical-Normative Compliance*—the degree of alignment between observed practices and the principles of *hifz al-māl* and Pancasila; and (c) *Cybercrime Vulnerability Level*—the risk exposure produced by current data processing and profiling mechanisms.

this research employs a mixed analytical approach. The normative analysis uses statutory interpretation, comparative regulatory analysis, and maqāṣid al-sharīʿah reasoning to assess the doctrinal coherence of the PDP Act, Islamic law, and Pancasila. Meanwhile, the empirical analysis applies thematic content analysis to interview transcripts to identify institutional behaviors, implementation gaps, and perceived risks. Additionally, a qualitative risk assessment model is used to evaluate cybercrime exposure by analyzing data flow diagrams, profiling algorithms, access control mechanisms, and governance processes used in the selected institutions. The integration of these analyses enables a holistic understanding of how legal norms translate into operational practices and where misalignments contribute to systemic vulnerabilities.

The framework of thinking underlying this research is structured into three analytical layers. The first layer examines the legal-normative foundation, reviewing how the PDP Act conceptualizes data protection, how *hifz al-māl* defines wealth preservation, and how Pancasila articulates the obligation for humane, just, and socially responsible technological governance. The second layer evaluates the institutional implementation of AI-generated risk profiling, focusing on data collection practices, algorithmic processing, decision-making protocols, and existing cybersecurity measures. The third layer synthesizes both dimensions to construct a tri-axial regulatory reconstruction model, which positions PDP Act compliance as the legal baseline, *hifz al-māl* as the ethical mandate ensuring protection from financial harm, and Pancasila as the ideological foundation guiding citizen-centered AI governance.

Through this methodological structure, the research seeks to provide doctrinal clarity, empirical validation, and a normative framework capable of guiding Islamic financial institutions toward safer, ethically grounded, and legally compliant AI risk profiling systems. The integration of normative and empirical methods ensures that the proposed regulatory reconstruction is not only theoretically robust but also practically aligned with real-world challenges faced by Islamic banks in the era of data-driven financial technologies.

3. RESULTS AND DISCUSSION

The results of this research emerge from the combined normative and empirical investigations conducted to assess the regulatory, ethical, and operational conditions surrounding the use of AI-generated risk profiling in *murābaḥah* financing within Indonesian Islamic banking institutions. The normative component analyzed statutory documents, regulatory instruments, *fatwa* provisions, and Islamic legal sources, while the empirical component relied on interviews with 12 purposively selected respondents who represented risk management divisions, cybersecurity units, *sharīʿah* compliance departments, and financial regulatory experts. Together, these methods revealed multilayered findings concerning the degree of regulatory fragmentation, the depth of institutional awareness surrounding data protection requirements, the operational characteristics of AI-generated profiling, and the alignment or misalignment between institutional practices and the normative pillars embodied in the Personal Data Protection Act (PDP Act), *hifz al-māl*, and Pancasila. These findings are presented narratively and holistically in order to capture the full spectrum of empirical detail uncovered during the study.

The research found that the existing regulatory landscape governing AI-generated risk profiling is fragmented and lacks integrative coherence. Although various regulatory instruments apply to Islamic banking, including the PDP Act, Bank Indonesia regulations, Otoritas Jasa Keuangan (OJK) guidelines, *fatwa* from the National Sharia Board (DSN-MUI), and internal Islamic banking governance standards, these instruments operate independently without cross-referencing or unified interpretive guidance. The PDP Act provides a general legal framework for personal data processing, yet it does not specifically address AI-generated profiling or automated decision-making in financial services. Similarly, the *fatwa* concerning *murābaḥah* stipulates rules on transparency, fairness, and contractual integrity but does not include guidance on the use of advanced digital profiling technologies. The analysis of institutional policies shows that Islamic banks attempt to operationalize these different regulatory expectations, but in the absence of harmonized guidelines, their

interpretations vary widely. Most institutions have privacy policies and data protection statements, but these documents differ in scope, detail, and clarity. Very few policies explicitly mention AI, profiling algorithms, or automated decision-making processes, indicating that institutions have not yet internalized the full implications of AI governance within the context of Islamic financing products.

The empirical interviews further revealed that institutional awareness of the PDP Act is generally high, yet the depth of understanding differs significantly among personnel. Risk officers and IT specialists tended to possess a more operational understanding of data handling practices but expressed uncertainties regarding lawful bases for processing personal data, especially concerning the use of alternative data sources such as mobile metadata, behavioral indicators, and digital footprints. Respondents from *sharī'ah* compliance divisions reported that their involvement in AI implementation projects was often limited to reviewing final policies rather than participating in early-stage design or risk assessments. Many respondents acknowledged that their institutions relied heavily on general consent clauses embedded within financing application forms, but several conceded that these clauses may no longer be sufficient under the PDP Act, which imposes stricter requirements for specific, informed, and voluntary consent.

Although all participating banks had initiated digital transformation initiatives, only a minority had implemented formal AI governance frameworks. Most institutions used general IT governance documents without dedicated guidelines for AI-specific risks such as algorithmic opacity, model drift, fairness auditing, or accountability in automated decision-making. Some institutions reported that they were in the early stages of drafting AI policies; however, these initiatives were driven more by internal efficiency goals than by regulatory or ethical considerations. This demonstrates the absence of a shared industry-wide understanding of how AI governance should intersect with Islamic legal principles and Pancasila-based values.

The results also show that all institutions employ AI-generated risk profiling tools at some stage within their *murābaḥah* financing workflows. These tools are used to evaluate the creditworthiness of applicants, predict default probabilities, categorize risk levels, and streamline approval processes. In some banks, these AI tools act only as advisory mechanisms, providing preliminary scoring that is later reviewed by human analysts. However, in other institutions, the AI-generated score is embedded into automated or semi-automated decision-making systems, particularly for low-risk or small-value *murābaḥah* products. Although none of the institutions had fully automated approval systems devoid of human oversight, several respondents indicated that the influence of AI-generated scores was substantial enough that human intervention often became a formality rather than a meaningful review.

The study also revealed substantial variation in the types of data used to generate risk profiles. While all institutions relied on conventional financial and demographic data such as income information, employment records, repayment histories, and credit bureau data, several banks had begun integrating alternative data sources. These sources included mobile phone usage patterns, transaction histories across e-commerce platforms, geo-location indicators, device metadata, and digital behavioral analytics such as application login frequency or customer service interaction patterns. A small number of institutions had experimented with social network analysis or digital footprint scoring, though these practices were limited and not yet widely institutionalized. Respondents noted that the integration of alternative data had improved risk prediction accuracy, yet they also admitted that these expanded datasets were more sensitive and riskier to store and process.

With respect to data protection, the study found mixed compliance with PDP Act principles. Some institutions demonstrated strong privacy governance by clearly describing the purposes of data processing and limiting access to internal personnel. However, several banks retained datasets that were not strictly necessary for *murābaḥah* risk profiling, indicating partial compliance with data minimization requirements. The principle of purpose limitation was inconsistently applied across institutions. While some banks separated datasets used for risk analysis from those used for marketing analytics, others stored data in centralized repositories with unclear distinction of purpose. Respondents could not always specify which data elements were essential, which were optional, and which were legacy artifacts of earlier systems.

The legal basis for data processing also varied significantly. While consent was the dominant legal basis, its implementation did not always meet the PDP Act's requirement of being specific, informed, and freely given. Several respondents admitted that customers were not explicitly informed that their data would be used to generate AI-driven risk scores, nor were they told that automated decision-making tools were involved in the financing process. No institution had fully implemented mechanisms to allow customers to request explanations or contest automated decisions, and none had explicit procedures for evaluating whether automated decisions had discriminatory effects.

Regarding data security, the study found that institutions generally employed standard cybersecurity architectures, including encryption protocols, firewalls, intrusion detection systems, and periodic penetration testing. However, AI-specific security controls, such as model integrity checks, adversarial testing, or limitations on internal access to sensitive training data, were largely absent. Some institutions used advanced multi-factor authentication, while others relied on username–password combinations for internal systems containing sensitive model data. Respondents noted that while cybersecurity was a major concern for their institutions, AI models were not yet treated as security-sensitive assets, even though model corruption or adversarial attacks could significantly distort risk assessments.

The management of data retention and deletion demonstrated another area of inconsistent compliance. Financing application data were generally retained in accordance with financial regulations, which require multi-year retention for audit and legal purposes. However, training datasets used for AI model development did not have clearly defined retention schedules. Several respondents stated that model training datasets were preserved indefinitely because "they might be useful for future improvements." This practice raises questions regarding compliance with the PDP Act's data retention

principles, which require that personal data be stored no longer than necessary for the purpose for which it was collected. Most institutions lacked structured mechanisms for deleting training data or conducting periodic reviews to ensure that retained data remained relevant.

The normative analysis of *hifz al-māl* showed that the principle is widely recognized in institutional rhetoric but unevenly reflected in operational systems. Respondents often described their institutions' financing products as inherently aligned with *sharī'ah* objectives, emphasizing fairness, transparency, and the avoidance of harm. However, the study found no direct mechanisms ensuring that AI-generated profiling models were evaluated through the lens of *hifz al-māl*. Institutions did not have procedures requiring them to assess whether profiling algorithms inadvertently exposed consumers to financial harm, unfair exclusion, or biased decision-making. Similarly, Pancasila values such as justice, humanity, and social welfare were referenced in institutional mission statements but were not operationalized into measurable standards for AI implementation.

The empirical interviews also revealed a widespread acknowledgment of vulnerabilities associated with data-driven cybercrime. Respondents identified several threats, including unauthorized access to high-granularity data, data leakage, identity theft, manipulation of profiling algorithms, phishing attacks targeting digital banking channels, and exploitation of behavioral data for fraud. Despite this awareness, institutional protective measures were uneven. Some banks had invested in advanced security monitoring and anomaly detection systems, while others relied on conventional cybersecurity controls that did not fully address AI-specific risks. Many respondents expressed concern that the growing dependence on large datasets and automated analytical tools increased their institution's exposure to cyber threats.

Finally, synthesis of all findings enabled the construction of a comprehensive picture of the existing operational and normative landscape. The results show that while AI-generated risk profiling is increasingly central to *murābaḥah* financing workflows, its governance remains underdeveloped, inconsistently interpreted, and insufficiently aligned with the legal and ethical expectations imposed by the PDP Act, *hifz al-māl*, and Pancasila. The conditions observed across institutions revealed significant gaps in data governance, model transparency, cybersecurity, ethical safeguards, and regulatory compliance. These findings form the empirical basis for the development of a harmonized regulatory reconstruction model, which aims to integrate these normative domains into a coherent governance framework that reflects the legal, ethical, and philosophical foundations of the Indonesian Islamic financial system.

3.1 Discussion

The findings of this study confirm the three hypotheses formulated at the outset and demonstrate the urgent need to reconstruct the regulatory foundations of AI-generated risk profiling in *murābaḥah* financing. The discussion begins by linking empirical results to theoretical expectations, followed by a comparison with the four bodies of literature reviewed in the introduction: studies on AI in Islamic finance, research on PDP Act implementation in digital lending ecosystems, Islamic legal scholarship on *hifz al-māl*, and Pancasila-based AI ethics. Through this cross-analysis, the discussion identifies the conceptual gaps and practical shortcomings that the proposed regulatory reconstruction seeks to address.

To begin with, the results demonstrate clear alignment with the first hypothesis stating that *AI-generated risk profiling currently operates within a fragmented regulatory environment that does not integrate the PDP Act, hifz al-māl, and Pancasila*. The normative analysis revealed that existing regulations including the PDP Act, Bank Indonesia and OJK guidelines, and DSN-MUI *fatāwā*—operate in parallel rather than as a unified framework. This mirrors earlier observations by Hidayanti et al. (2020) and Rahman (2021), who noted that digital transformation in Islamic banking often advances technologically faster than the development of corresponding ethical and legal guidelines. However, the present research extends their findings by showing that the fragmentation is not merely conceptual but structurally embedded in operational policies, thereby affecting day-to-day practices in Islamic banks. For example, while institutions were aware of data protection obligations, their internal policies varied widely, with few documents explicitly addressing AI profiling or automated decision-making. This inconsistency confirms that the regulatory landscape has not evolved sufficiently to govern AI-specific risks, particularly in Islamic financial products such as *murābaḥah*, which rely heavily on contractual clarity, fairness, and protection from harm.

The results also corroborate the second hypothesis that the absence of an integrated governance framework contributes to an elevated risk of data-driven cybercrime. The empirical findings reveal substantial vulnerabilities, including inconsistent consent procedures, retention of unnecessary training data, insufficient AI-specific cybersecurity protections, and the absence of model explainability or fairness auditing. These concerns parallel insights from recent Indonesian studies: the AICoLCy 2025 proceedings emphasize that weaknesses in digital-economy regulation, data governance, and technological accountability significantly elevate the likelihood of privacy breaches, algorithmic misuse, and cyber-enabled financial exploitation within financial-service environments (Rohmah & Anisa, 2025). Likewise, Rofi'i (2023) demonstrates that Indonesian banks relying on predictive algorithms face heightened exposure to errors and systemic risks due to opaque model structures, fragmented data-handling practices, and inadequate oversight mechanisms, reinforcing the empirical observation that algorithmic tools can unintentionally reproduce bias or generate new forms of vulnerability when deployed without comprehensive safeguards (Rofi'i, 2023). Unlike previous studies, which concentrate primarily on conventional digital-lending ecosystems, the present research illustrates how these vulnerabilities directly challenge the ethical foundations of Islamic finance, where AI profiling must not only achieve technical accuracy but also uphold *hifz al-māl* by preventing wealth-related harm, unjust exclusion, or exploitation through nontransparent evaluation systems. The findings further show that many institutions utilize alternative data such as behavioral signals, device metadata, and online activity without clear legal or ethical justification; when such data are

processed without disclosure, the opacity heightens the risk of algorithmic exclusion and discriminatory profiling, undermining the Islamic imperative to prevent unjust harm and confirming that regulatory gaps significantly increase consumer exposure to data-driven cybercrime.

The findings also support the third hypothesis predicting that a harmonized regulatory framework combining the Personal Data Protection Act, *hifz al-māl*, and Pancasila can create stronger governance mechanisms for AI-generated risk profiling. The empirical evidence demonstrates that such harmonization is currently absent, as respondents consistently acknowledged that although their institutions publicly promote *sharīʿah*-compliant values in mission statements, these commitments are not translated into AI model architecture, data-selection protocols, cybersecurity safeguards, or decision-making processes. Likewise, Pancasila-based values of justice, humanity, and social responsibility frequently articulated in institutional rhetoric are not embedded within algorithmic governance or operationalized as measurable fairness parameters. This gap indicates that current institutional approaches prioritize technical efficiency over ethical congruence, leaving essential normative obligations unfulfilled. These results reflect broader concerns found in Indonesian scholarship: Rejekiningsih and Hakimi (2023) show that AI practices across educational and civic environments routinely fail to internalize Pancasila values, resulting in ethical inconsistencies and low legal consciousness among users (Rejekiningsih et al., 2023), while Nugroho (2025) argues that Indonesia's AI governance remains technocratic and underdeveloped, lacking explicit ethical integration and political-philosophical grounding in national values (Nugroho, 2025) . The present study advances this literature by demonstrating not only the conceptual necessity of Pancasila ethics but also the practical pathways through which these values can be embedded in AI risk-profiling systems—such as converting philosophical norms into concrete requirements for data governance, transparency standards, fairness audits, and socio-ethical impact assessments.

Comparing these findings with research on AI in Islamic finance reveals a significant point of divergence. Earlier studies often emphasized the transformative potential of AI to enhance service efficiency, support decision-making, and expand financial access, yet tended to treat risk profiling as a purely neutral technological instrument. However, recent Islamic scholarship challenges this assumption: Ramlan and Malkan (2025) show that AI systems can introduce ethical risks through algorithmic bias, opaque data practices, and economic vulnerabilities that directly undermine the Islamic objective of protecting wealth (*hifz al-māl*), highlighting that AI technologies inherently shape moral and socioeconomic outcomes rather than functioning as value-free tools (Mustapha & Malkan, 2025). The present study aligns with this insight by demonstrating that AI-generated profiling influences how financial opportunities are allocated, affects contractual fairness, and ultimately determines whether *murābaḥah* applicants are included or excluded from financing. When profiling models rely on undisclosed behavioral data or amplify patterns embedded in biased training datasets, they can inadvertently inflict financial harm on applicants. Such harm stands in direct contradiction to the Islamic imperative of *hifz al-māl*, which requires institutions to protect the economic welfare of individuals and the broader community. Thus, this research extends the existing literature by showing that AI in Islamic finance must not only pursue operational efficiency but must also be governed through ethical safeguards that ensure fairness, prevent harm, and uphold foundational Islamic values.

The study also brings new insight into the role of the PDP Act in AI governance. Previous analyses, such as those outlined by Solikhah (2025), highlight persistent structural weaknesses in Indonesia's personal data protection regime, including ambiguities surrounding automated decision-making, limited enforcement capacity, and a fragmented regulatory landscape that complicates the implementation of data subject rights . The results of this research demonstrate that these challenges become even more complex in Islamic banking, where AI-generated profiling directly intersects with *sharīʿah*-based contractual norms. As AI systems process sensitive financial and behavioral information, the PDP Act's requirements for lawfulness, transparency, and accountability must operate alongside Islamic obligations of fairness, honesty (*ṣidq*), and harm prevention (*dar' al-mafāsid*). Yet the institutions studied had not developed interpretive mechanisms to integrate these obligations coherently, confirming the hypothesis that the PDP Act alone—without harmonization with Islamic normative principles cannot adequately govern AI profiling in *murābaḥah* financing. From the perspective of Islamic legal scholarship, contemporary analyses such as Siregar and Rambe (2024) emphasize that *hifz al-māl* requires not only the protection of financial assets but also safeguarding individuals from technological exploitation, unjust exclusion, and opacity in risk evaluation procedures (Yuspin et al., 2024). The present findings reveal that when AI systems lack transparency or adequate oversight, they may undermine these objectives by unintentionally excluding eligible applicants, exposing personal data to cybercrime, or creating opaque scoring mechanisms that applicants cannot challenge—demonstrating the need for new interpretive and regulatory frameworks capable of ensuring that AI remains aligned with the higher objectives of Islamic law.

The discussion also highlights that the findings diverge from much of the existing scholarship in one critical respect: this study identifies a tri-directional normative conflict between technological design, Islamic legal obligations, and state ideological values operating simultaneously within AI-generated risk profiling. Prior works typically examined these domains in isolation AI studies focused on performance and system optimization, Islamic finance scholarship discussed ethical safeguards and contractual soundness, while analyses of Pancasila addressed general societal values and philosophical orientations. The present results demonstrate that the intersection of these three normative spheres produces a unique regulatory vacuum that has not been previously recognized. Institutions face uncertainty in determining how AI model construction should conform to Islamic principles of wealth protection while also fulfilling statutory duties under the data protection regime and embodying Pancasila-oriented commitments to justice and humanity. This

multidimensional challenge strengthens the argument that harmonization is essential and underscores the originality of the regulatory framework proposed in this research.

Beyond reinforcing the hypotheses, the findings reveal significant implications for the operationalization of algorithmic fairness and transparency in Islamic banking. The absence of robust AI governance structures means that institutions lack mechanisms to ensure that profiling systems do not generate discriminatory or harmful outcomes. Respondents consistently acknowledged that fairness audits, explainability evaluations, and other accountability measures had not been implemented. While concerns about opaque, black-box algorithms are widely discussed in global AI ethics discourse, their consequences in Islamic financial contexts are more profound because they directly implicate *sharīʿah* compliance and the moral integrity of financial contracts. As a result, the study identifies a novel ethical dimension: algorithmic transparency is not merely a technical expectation but constitutes a *sharīʿah*-grounded obligation tied to principles of fairness (*ʿadl*) and the prohibition of deception (*gharar*).

The results further suggest that cybercrime vulnerabilities embedded within AI profiling systems have intertwined religious, ethical, and legal implications. Risks such as unauthorized access, identity theft, and manipulation of profiling outputs directly undermine the Islamic objective of *hifz al-māl*, which mandates protecting individuals' financial security. These vulnerabilities also contradict the Pancasila-based imperative to uphold humanity and justice, as data breaches disproportionately harm individuals with limited resources or digital literacy. Although the data protection framework formally imposes stringent requirements for safeguarding personal information, the institutional practices observed in the field showed uneven implementation. The study extends existing concerns by demonstrating that these vulnerabilities are intensified in Islamic banking due to the additional ethical expectations imposed on financial institutions.

Finally, the empirical evidence confirms that current institutional arrangements do not sufficiently integrate the obligations of the data protection regime, Islamic ethical norms, and Pancasila-based values into a coherent governance structure. By identifying specific implementation gaps ranging from inconsistent consent procedures and inadequate security practices to opaque algorithmic processes the findings reveal concrete operational areas where harmonized governance would yield meaningful improvements. This contributes to ongoing academic calls for multi-layered AI regulation in the financial sector, while introducing a distinctive advancement by anchoring the proposed governance model within Indonesia's unique normative landscape.

4. CONCLUSION

This study concludes that AI-generated risk profiling in *murābaḥah* financing operates within a multidimensional regulatory vacuum arising from the absence of harmonization between the Personal Data Protection Act, Islamic legal imperatives particularly *hifz al-māl* and the ethical foundations of Pancasila. The findings demonstrate that although Islamic financial institutions increasingly adopt AI-driven profiling tools, their implementation remains fragmented, with inconsistent consent practices, opaque algorithmic processes, and insufficient security safeguards that expose institutions to data-driven cybercrime. These vulnerabilities are intensified by the lack of integrated interpretive frameworks capable of aligning statutory data protection duties with *sharīʿah* obligations of fairness, honesty, and harm prevention, as well as Pancasila's principles of justice and humanity. The empirical evidence from twelve institutional actors further confirms that AI systems are deployed without fairness audits, explainability mechanisms, or ethical governance structures, resulting in profiling outcomes that may unintentionally exclude eligible applicants, reduce financial accessibility, or contradict the protective aims of Islamic law. The study's proposed Tri-Axial Regulatory Reconstruction Model addresses this gap by offering a comprehensive normative pathway for embedding legal, ethical, and ideological values into AI governance in Islamic banking. Nonetheless, the research is limited by the scope of institutional participation, the absence of quantitative assessments of algorithmic performance, and the rapidly evolving nature of Indonesia's digital regulatory environment. Future research should incorporate cross-institutional benchmarking, technical evaluations of algorithmic fairness and transparency, and deeper inquiry into operational models for AI governance to further refine a robust, implementable framework that ensures secure, ethical, and *sharīʿah*-aligned AI adoption in Islamic finance.

ACKNOWLEDGMENT

Thank you to those who have supported the implementation of this research.

REFERENCES

Cristine, M. A., Mario, F., Risakota, A., & Celine, S. R. (2025). Perlindungan Data Pribadi dalam Sistem Skoring Kredit Otomatis oleh Fintech di Indonesia : Analisis Yuridis Normatif Berdasarkan Undang- Undang Nomor 27 Tahun 2022. *Jurnal Studi Hukum Modern*, *7*(3), 1–15.

Fitria, T. N. (2025). Islamic Banking Digitalization : Challenges and Opportunities in the Era of Industrial Revolution 4 . 0. *Jurnal Ilmiah Ekonomi Islam*, *11*(1), 1–19.

Hidayanti, N. F., Ariani, Z., Sahman, Z., & Syaharuddin. (2025). The Integration of Artificial Intelligence in Islamic Financial Services : A Review on Digital Innovation for Sharia Financial Inclusion. *Integrating Religion, Social, and Law: Conference Series*, *1*(1), 8–17.

Ikhwan, M. N., Bahiya, I. K., Safagutan, F., Syariah, M. E., Taufiq, A., & Darmawan, A. (2025). Problematics of Murabaha Agreement in Indonesian Islamic Banking : A Systematic Literature Review. *Journal of Sharia Finance and Banking*, *5*(1), 88–103.

Ma'unah, I., Musyarofah, S., Zahra, A. F. Z. A., & Agrariyanti, Y. (2025). Pancasila dan Artificial Intelligence : Analisis Etis atas Regulasi AI di Indonesia Pancasila and Artificial Intelligence : Ethical Analysis of AI Regulations in Indonesia. *Jurnal Ilmiah Multidisiplin*, *2*(5), 718–746.

Mustapha, R., & Malkan, S. N. A. (2025). Maqasid Al-Shariah In The Ai Era: Balancing Innovation And Islamic Ethical Principles. *International Journal of Islamic Theology and Civilisation*, *3*(3), 1–21. https://doi.org/10.5281/zenodo.15381828

Nugroho, F. (2025). Artificial Intelligence Regulation and Political Ethics : An Analysis of Indonesia ' s Position in AI Governance. *PolitiScope: Journal of Political Innovation and Analysis*, *2*(1), 42–51.

OJK, O. J. K. (2023). *Panduan Kode Etik Kecerdasan Buatan (Artificial Intelligence/AI) yang Bertanggung Jawab dan Terpercaya di Industri Teknologi Finansial*. Otoritas Jasa Keuangan. https://www.ojk.go.id

Rachbini, E. M., Listiyanto, E., Dharma, A., Irhamna, P., Al, I., Adha, F., Maarif, B., & Firlana, A. M. (2023). Innovative credit scoring untuk inklusi keuangan. *Institute for Development of Economics and Finance*, *5*.

Rejekiningsih, T., Hakimi, H., & Hakimi, H. (2023). Jurnal Civics : Media Kajian Kewarganegaraan Exploring the integration of ideological values with artificial intelligence technology : A legal awareness perspective Exploring the integration of ideological values with artificial intelligence technology : . *Jurnal Civics: Media Kajian Kewarganegaraan*, *20*(2), 236–247.

Rofi'i, Y. U. (2023). Financial Risk Management in Indonesian Banking : The Integrative Role of Data Analytics and Predictive Algorithms. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(December), 300–309.

Rohmah, S. M., & Anisa, S. A. N. (2025). The Role Of Law In Supporting The Digital Economy Ecosystem In Indonesia: Opportunities And Challenges. *Academic International Conference on Law Literacy 2nd*, 85–91.

Solikhah, M. (2025). Personal Data Protection in the Era of Digital Transformation : Challenges and Solutions in the Indonesian Cyber Law Framework. *Indonesian Cyber Law Review*, *2*(1), 39–50.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (2022). http://https//www.abnrlaw.com (Translated version by Wishnu Basuki)

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2024). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1), 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130