

The Urgency of Regulation and Governance of Artificial Intelligence (AI) in Indonesian Finance: Comparison and Risk-Based Implementation

Afiq Ahmad Hanif^{1*}, Hasbir Paserangi², Arni Viratami Cahyani³

^{1,2}Civil Law Department, Faculty of Law, Universitas Hasanuddin, Indonesia

³Criminal Law Department, Faculty of Law, Universitas Hasanuddin, Indonesia

Email: ¹⁾ afiq.ahmadhanif@gmail.com

Received : 26 July - 2025

Accepted : 28 August - 2025

Published online : 01 September - 2025

Abstract

The rapid advancement of Artificial Intelligence (AI) presents significant opportunities and considerable challenges for the Indonesian financial sector. This paper examines the urgent need for a comprehensive regulatory framework and adaptive oversight mechanisms to govern AI applications in digital financial services in Indonesia. Currently, existing regulations are fragmented and insufficient to address the complexities of AI, including algorithmic accountability and potential biases that could lead to consumer detriment and systemic risks. This research employs a normative legal method, utilizing statutory, conceptual, and comparative approaches by benchmarking Indonesia's legal landscape against international best practices in the European Union, the United States, and Singapore. The study identifies a critical regulatory gap concerning legal liability for AI-induced losses, currently reliant on general civil code provisions (Article 1367 KUHPerdata) that may not adequately cover the autonomous nature of AI. It argues for the necessity of specific AI regulations focusing on risk-based approaches, transparency, accountability, and robust consumer protection, drawing insights from frameworks like the EU AI Act. The paper concludes by recommending institutional reforms and the strengthening of AI governance, grounded in Pancasila principles, to foster a secure, ethical, and inclusive digital financial ecosystem in Indonesia. This will ensure that AI innovation proceeds responsibly, safeguarding the public interest and national financial stability.

Keywords: AI Regulation, Digital Financial Services, Legal Liability.

1. Introduction

Technological developments in the current era of digitalisation have made human life easier. One form of technological development is the emergence of artificial intelligence (AI). AI is intelligence added to a system, or in other words, the ability of a system to interpret external data correctly, manage that data, and use the results for a specific purpose (Ririh et al., 2020). AI has been implemented in various fields, such as healthcare, education, law, and economics, with adaptive capabilities that continue to improve as data and algorithm sophistication increase.

In Indonesia, the growth of digital technology users shows great potential in supporting the transformation of the national financial system. At the beginning of 2023, the number of internet users in Indonesia reached 212.9 million people with an internet penetration rate of 77 per cent, while social media users in Indonesia were recorded at 167 million people, equivalent to 60.4 per cent of the total population. In addition, the number of active mobile



connections in Indonesia reached 353.8 million, equivalent to 128 per cent of the total population (Suryanegara, 2023).

The use of AI is estimated to contribute up to 12 per cent to the national Gross Domestic Product (GDP) by 2030, equivalent to USD 366 billion. Globally, AI adoption in the industrial sector has reached 56 per cent, with a potential contribution of up to USD 4.4 trillion through Generative AI technology. However, this development has not yet received a response from the Indonesian government.

Generative AI (GenAI) is a form of AI that is capable of recognising data patterns and producing adaptive outputs. In the financial sector, GenAI enables the automation of customer analysis processes, credit decision-making, violation services, transaction error mitigation, and fraud detection. According to a report by AC Ventures, BCG, and BCG X, 51 percent of financial institutions in Indonesia have adopted GenAI in their operations, while another 27 percent see great potential in developing innovative GenAI-based products and services. Furthermore, the report also shows that 61 percent of financial institutions in Indonesia feel they have strong technological readiness to adopt GenAI. However, the integration of this technology is not yet fully supported by adequate infrastructure and regulations. Based on data from the Global AI Index 2023, Indonesia still ranks 46th out of 62 countries, indicating the need for improvements in digital infrastructure to address challenges in AI development.

Challenges in the application of AI, particularly GenAI, include the risk of algorithmic bias, which can lead to inaccuracies in credit assessments, financial decision errors, and inaccurate investment predictions. On the other hand, there is still uncertainty regarding legal responsibility when AI systems cause losses to consumers. Regulatory fragmentation and weak oversight of adaptive digital systems also pose serious obstacles to creating a secure and inclusive digital financial ecosystem. Thus, current regulations still do not accommodate the complexity of AI.

As such, there is an urgent need to establish specific regulations and adaptive oversight mechanisms for the use of AI. Some studies focus on data protection, but there are not yet many that analyse the legal vacuum related to algorithm accountability and AI oversight models in the financial sector based on a risk-based approach.

The unlimited and further developable capabilities of AI make it the backbone of digital transformation in the financial sector. However, the absence of specific regulations has the potential to trigger a crisis of confidence and systemic losses. A comprehensive legal framework is needed to ensure clear legal accountability for the impact of AI use, as well as to create an effective and accountable governance and oversight system. Regulatory unpreparedness and weak oversight mechanisms open up the potential for errors in the use of AI that could harm various parties.

Based on this background, the research questions in this study are as follows:

1. What form of legal liability applies to losses arising from the use of AI in the financial sector?
2. To what extent is it urgent to establish appropriate oversight mechanisms to anticipate and manage the risks of AI implementation in digital financial services in Indonesia?

2. Methods

This study uses a normative research method analysed using a statute approach to examine legal provisions related to the use of AI in the financial sector in Indonesia, the European Union, the United States, and Singapore. Furthermore, a conceptual approach is used to understand the concepts of legal accountability, AI governance, and the principle of

prudence in the use of AI. Furthermore, this study also uses a comparative approach through benchmarking of the legal frameworks in various countries to identify best practices that can be adapted in Indonesia. Then, a case study approach is conducted by analysing the implementation of AI in the financial sector.

Data collection techniques were carried out through document studies of primary legal materials, namely laws and regulations, as well as secondary legal materials, such as scientific journals and official reports from international institutions. The data obtained was analysed qualitatively to identify forms of legal accountability, assess regulatory readiness in Indonesia, and formulate recommendations for the formation of regulations and adaptive oversight mechanisms for the use of AI in the financial sector. The selection of the European Union, the United States, and Singapore as objects of comparison was based on the consideration that these three countries have diverse and progressive approaches to AI regulation, thereby providing a comprehensive perspective for the development of a national legal framework that is adaptive and responsive to the challenges of the digital era.

3. Results and Discussion

3.1. Legal Framework for Regulating AI Usage in the Financial Sector

Data is an essential element that underpins the performance of AI. However, the availability of quality data in Indonesia still encounters various obstacles. The information available is often incomplete, unstructured, or inaccurate, thus creating doubts about its validity. On the other hand, the escalation of data breach incidents makes the protection of privacy and information security a legal urgency. The prevailing national regulatory framework has also not been fully adaptive to the needs of AI development. The existing provisions have not been entirely capable of accommodating the dynamics of advanced technology, while the absence of an integrated legal framework narrows the space for innovation (Ningsih et al., 2025).

The complexity of ethical and privacy issues inherent in the use of AI is further exacerbated by the low level of public awareness and the weakness of existing data protection regulations. Therefore, strategic steps are needed to enhance digital ethics literacy while at the same time establishing comprehensive regulations that are responsive to the advancement of AI across various sectors in Indonesia.

In Indonesian positive law, a number of relevant regulatory instruments can be identified, among others:

- a. Law No. 11 of 2008 on Electronic Information and Transactions (the ITE Law), which serves as the legal foundation for the use of electronic systems, including AI classified as an “Electronic Agent” by virtue of its automatic nature as stipulated in Article 1(8). Furthermore, Article 15 of the ITE Law obliges electronic system providers to ensure that the systems under their management operate reliably and securely. Financial institutions such as banks and fintech companies operating AI-based systems bear legal responsibility for the reliability and security of such systems.
- b. Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions (PSTE Regulation), which reinforces the principle of accountability for electronic systems, including the obligation of providers to guarantee the protection of personal data and system security. This is reflected in the provisions of Articles 3, 11, and 14, which regulate the operational obligations of system providers.
- c. Law No. 27 of 2022 on Personal Data Protection (PDP Law), which in Chapter IV explicitly sets out the rights of data subjects, including the right to obtain information

- and to correct their personal data. However, the PDP Law does not explicitly regulate mechanisms for objections to AI-based automated decisions. Moreover, delays in the issuance of implementing regulations following the expiry of the transitional period under this law further increase the urgency of formulating comprehensive technical rules on personal data protection, particularly in the context of data processing by autonomous systems.
- d. OJK Regulation No. 11/POJK.03/2022, which classifies AI as part of information technology and electronic banking services, as articulated in Article 1(2) and (3). This regulation obliges banks to establish standards, procedures, and auditing practices for the information systems they operate, including audits of the algorithms applied.
 - e. OJK Circular No. 29/SEOJK.03/2022, as the technical guideline for OJK Regulation No. 11/POJK.03/2022, which provides more detailed direction on cyber risk management and the safeguarding of information systems within technology-based financial services.
 - f. Law No. 10 of 1998 on Banking, which amends Law No. 7 of 1992, serves as the primary legal basis for the conduct of banking activities. Fundamental principles such as prudence, good governance, and the protection of customer data confidentiality set forth in this law constitute an essential foundation for the integration of AI into the banking and financial system. The implementation of AI must take these principles into account to ensure that its application does not conflict with the fundamental values of banking law in Indonesia.

The aforementioned basic provisions remain fragmented and have yet to form a comprehensive legal framework for regulating AI, particularly in relation to its scope, governance, and supervisory mechanisms. The absence of such comprehensive regulation carries the potential to create a legal vacuum, resulting in uncertainty in legal certainty. This condition may not only hinder the development of technological innovation but also increase the potential risk of losses, both for consumers and business actors in the financial sector, in both public and private domains.

In the study 'Generative AI: Shaping Indonesia's Business Ecosystem Tomorrow' conducted by KORIKA and Advisia Group in collaboration with IBM in 2024, the challenges and weaknesses faced by the financial services and manufacturing sectors are largely attributable to the limited availability of human resources with digital competencies, thereby affecting the efficiency of data management. Nevertheless, the potential utilisation of AI, particularly GenAI, is considered highly promising. This is reflected in findings showing that all respondents (100%) believe that the application of GenAI can enhance efficiency in delivering customer experience. To optimise the economic value of this technology, companies need to take into account their operational scale and internal capacity, as well as ensure that data governance practices and the application of digital ethics are aligned with prevailing legal provisions (Santana et al., 2017).

Circular Letter of the Ministry of Communication and Informatics No. 9 of 2023 on the Ethical Guidelines for Artificial Intelligence may serve as an initial reference in formulating more comprehensive regulation in this field. In the implementation of AI, which encompasses data processing and data management activities, ethics play a pivotal role and cannot be separated from the overall process. Given the complexity of data management by AI systems, the protection of personal data as well as the fulfilment of data subjects' rights must be carried out by prioritising ethical principles, as explicitly affirmed in the circular letter that ethics play a significant role.

In formulating such a regulatory framework, it is important to adopt best practice principles from various countries that have previously regulated the use of AI in the financial sector. Comparative studies of different international regulatory models may provide broad perspectives on effective legal approaches to managing AI-related risks while at the same time encouraging responsible technological innovation. Through a process of adopting and adapting relevant and ethical legal principles, Indonesia may develop a national policy that is not only contextual to domestic needs but also aligned with international standards, thereby filling the existing legal vacuum and enhancing the competitiveness of the national financial sector (Nasman et al., 2024).

As material for comparative analysis, the following presents a number of regulations from several countries that specifically govern the utilisation of AI in the financial sector, among others:

A. General Data Protection Regulation - European Union

One of the regulations that can serve as a reference in governing the use of AI is the General Data Protection Regulation (GDPR), which is the main legal instrument in the effort to harmonise personal data protection across all European Union member states. The GDPR has extraterritorial effect, thus binding not only entities operating within the European Union, but also any party outside the region that collects, processes, or utilises the personal data of data subjects residing in the European Union. The GDPR approach offers a regulatory model that is both strict and adaptive, emphasising fundamental principles such as transparency, accountability, and the strengthening of individual control over personal data (Ziqra et al., 2021).

The GDPR came into uniform effect on 25 May 2018 with the primary objective not only of addressing legal challenges arising from developments in information technology, but also of ensuring that such developments continue to respect human rights. One provision particularly relevant to the use of AI in the financial sector is Article 22(1), which grants individuals the right not to be subjected to decisions based solely on automated processing, including profiling, where such decisions produce legal effects or significantly affect the individual concerned (Lukács & Váradi, 2023). Profiling, as defined in Article 4(4) of the GDPR, encompasses the evaluation of personal aspects of individuals, such as financial circumstances or behaviour, thereby carrying significant implications for AI-based services, including credit assessment or risk analysis.

The GDPR explicitly emphasises the importance of transparency in automated decision-making processes (Bayamlioğlu, 2018). This transparency encompasses not only the disclosure of the existence of automated processes, but also the revelation of the underlying logic of the algorithms, the types of data being processed, and the potential consequences arising from such decisions. Transparency serves as a crucial instrument to enhance individual control over personal data, while also functioning as a means to mitigate potential algorithmic bias, systemic uncertainty, and information exclusivity.

In the specific context of the financial sector, the GDPR requires financial institutions to clearly disclose the operational principles of algorithmic systems, the characteristics of the data employed, and the impact of resulting decisions on data subjects. This obligation aims to ensure that financial institutions not only comply with principles of fairness, transparency, and accountability, but also provide mechanisms for individuals to challenge automated decisions or request human intervention. Moreover, financial institutions are required to establish internal audit mechanisms and conduct periodic evaluations of AI systems in use to guarantee the integrity and objectivity of the decisions produced (Pflücke, 2025).

Although the GDPR provides a robust framework for the protection of personal data, it does not specifically regulate technical methods for testing, evaluating, or mitigating bias in AI systems, particularly within the financial sector. Consequently, there remains scope for further development through additional regulations or technical soft law instruments in the context of algorithmic auditing and bias mitigation.

B. Artificial Intelligence Act - European Union

In April 2021, the European Commission proposed the Artificial Intelligence Act (AI Act) as the European Union's first regulation on artificial intelligence, aimed at establishing a legal framework based on a risk-based approach. This regulation classifies AI systems into three main categories: high-risk, low-risk, and minimal-risk, according to the potential impact on users' rights and safety. This classification determines the extent of compliance with legal requirements that must be met. For instance, in the financial sector, the use of AI for creditworthiness assessment or fraud detection falls into the high-risk category, which necessitates strict supervision, comprehensive impact evaluation, and adherence to standards of transparency and accountability.

The primary objective of this regulation is to promote sustainable AI innovation in Europe while ensuring maximal protection of individuals' fundamental rights. To this end, the AI Act requires national authorities to provide sandbox testing environments, enabling companies, particularly small and medium-sized enterprises, to develop and test AI systems in conditions resembling real-world scenarios before public deployment. This approach aims to create an AI ecosystem that is innovative and competitive, yet oriented towards legal compliance and consumer protection (Roy, 2024).

The predictive benefits offered by AI systems, particularly in the financial sector, are undeniable. However, their use also carries significant potential risks, including system opacity, errors in decision-making, unintentional discrimination, and limitations in explaining the outcomes generated. Consequently, the AI Act addresses these challenges by establishing the first regulatory framework that is both specific and comprehensive in governing the development and design of AI. The risk-based approach allows for differential regulatory application, whereby the higher the risk level of an AI system, the stricter the regulatory requirements imposed. In this way, the AI Act seeks to balance the promotion of innovation with the protection of individual rights (Mazzini & Bagni, 2023).

Although the AI Act aims to promote the development of trustworthy AI with a proportionate regulatory burden, its implementation presents specific challenges. Compliance with this regulation requires companies, including financial institutions, to conduct regular audits and evaluations, which results in increased operational burdens and significant costs, particularly for small and medium-sized enterprises. The provisions regarding risk acceptability in high-risk AI systems also require that residual risks be minimised or eliminated as far as possible, taking into account the state of the art in technology. However, a narrow interpretation of these criteria may hinder effective implementation and create an imbalance between proportionate regulation and the principle of system reliability (Fraser & y Villarino, 2024).

The AI Act also has the potential to slow down the innovation process, particularly for systems that offer substantial benefits but are categorised as low-risk. Therefore, although the AI Act is progressive, this regulation still requires careful adjustment to avoid creating disincentives for innovation.

In 2023, an agreement between the European Parliament and the Council of the European Union led to the adoption of this regulation in May 2024, with phased implementation scheduled across the European Union in 2025 and full enforcement in 2026

(Smuha, 2025). Although this regulation is not yet fully in force, one of the mandates set out in the AI Act is the obligation for each country to conduct sandbox testing.

Spain became the first country to follow up on this mandate by issuing Royal Decree 817/2023 in 2023, which implements a general rehearsal or trial application of the regulation without legal consequences in the event of non-compliance. This step is expected to serve as a precedent for other European Union member states to develop sandbox testing in preparation for the full implementation of the regulation (Ringe & Christopher, 2020). In addition, Spain established the Spanish Artificial Intelligence Supervisory Agency (Agencia Española de Supervisión de Inteligencia Artificial, AESIA) through Royal Decree 729/2023. AESIA aims to promote the development of practical testing environments for artificial intelligence systems, strengthen user protection, and reduce the potential for discriminatory bias (Pérez del Prado, 2025).

Starting in 2025, the Spanish government will implement the draft AI law, which is currently under legislative review. One provision of this regulation is administrative sanctions ranging from 7.5 to 35 million euros, with specific nominal adjustments for small and medium-sized enterprises. The implementation of this policy will be coordinated by a number of relevant institutions, including AESIA (Munusamy & Hashim, 2021). The draft has been prepared to align national policy with the EU AI Act, and to emphasise the development and use of AI technology that is ethical, inclusive, and beneficial to society. One of the main features of this draft is the introduction of a regulatory sandbox scheme, which is a controlled testing environment designed to promote AI innovation in compliance with legal requirements (Truby et al., 2022).

C. NIST Artificial Intelligence Risk Management Framework - US

Regulatory fragmentation also occurs in the United States, as each state has different rules regarding AI. The National Institute of Standards and Technology (NIST) has developed the NIST Artificial Intelligence Risk Management Framework (AI RMF) as a voluntary guideline for assessing and managing risks associated with artificial intelligence. Although the AI RMF is not legally binding, it forms part of soft law norms and best practices that encourage industry actors to implement its principles appropriately and responsibly. Therefore, the AI RMF plays a key role in shaping AI governance that is ethical, safe, and transparent without imposing rigid regulatory burdens (Barrett et al., 2022).

The AI RMF has evolved into a relatively more mature framework compared with other sources of AI risk management, encompassing comprehensive and detailed activities that enable stakeholders to identify high-priority areas and thoroughly evaluate their risk management programmes (Barrett et al., 2022). According to the National Institute of Standards and Technology, this framework is structured around four main functions, namely:

- 1) Govern, for establishing a risk management culture within the organisation;
- 2) Map, for recognising the operational context and identifying related risks;
- 3) Measure, for the assessment, analysis, and monitoring of identified risks; and
- 4) Manage, for prioritising and addressing risks based on their projected impact.

Within the AI RMF, governance, transparency, accountability, and trust are positioned as strategic components in building a fair, ethical, and responsible AI ecosystem. Governance plays a key role in ensuring clear policies and institutional structures at every stage of AI system development, implementation, and maintenance. Transparency, as a prerequisite for mitigating algorithmic bias, requires openness regarding decision-making logic and data sources. Accountability demands a clear division of roles and responsibilities, along with the conduct of audits to identify potential bias. Public trust is cultivated through responsive

practices and by ensuring that AI systems operate fairly and can be explained. Overall, the AI RMF provides a comprehensive framework to ensure that the use of AI technology is both technically efficient and aligned with principles of fairness, ethics, and social interest.

However, although this framework is highly comprehensive, its implementation is voluntary and not legally binding, meaning its adoption depends on the commitment of financial institutions to comply. While the framework identifies key issues, it sometimes provides insufficiently detailed guidance for practical implementation in the field.

Based on its historical development, the United States is a pioneer in the utilisation of AI technology, particularly in the financial sector, where AI applications have rapidly evolved alongside technological advancements since the term 'Artificial Intelligence' was first introduced by John McCarthy in 1956. In the early 1990s, AI began to be applied in the financial sector, initially for detecting and predicting money laundering cases through the FinCEN Artificial Intelligence System (FAIS) in 1993 (Kunwar, 2019).

Currently, major institutions in the financial sector such as JPMorgan Chase, Capital One, and Wells Fargo are pioneers in integrating AI into their operations. In their article, they also employ approximately 17.5 per cent of the total AI specialists working in the banking industry, demonstrating a progressive step in directing the use of AI towards efficiency and effectiveness in the financial sector. For example, JPMorgan Chase applies a risk-based approach in its governance to build a safe and ethical AI ecosystem, using the Model Risk Governance to evaluate potential risks that may arise from the implementation of machine learning and AI technologies. This is intended to ensure that the deployment of these technologies does not pose risks to either customer interests or the operational stability of the company.

Although it does not explicitly state a formal application of the NIST AI RMF, the approach implemented by JPMorgan Chase closely reflects alignment with the main functional structure of the AI RMF, namely Govern, Map, Measure, and Manage. This indicates that, although the AI RMF is a soft law guideline, the framework can function effectively in operational practice, particularly in the financial sector, where accountability and risk management are paramount.

D. AI Governance Frameworks - Singapore

Singapore is one of the countries with the most comprehensive and structured approach to AI governance in the world. The country has developed various regulations and normative instruments to ensure the ethical, safe, and accountable deployment of AI, including the AI Governance Framework Model, AI Verify, the Personal Data Protection Act (PDPA), and the principles of Fairness, Ethics, Accountability, and Transparency (FEAT). In addition, Singapore also has the Cybersecurity Act and the AI Model Risk Management Guidelines issued by the Monetary Authority of Singapore (MAS). By positioning AI as a strategic technology cluster in national economic development, Singapore acts not only as a user but also as a developer and global provider of AI solutions. Recognition of this preparedness is reflected in Singapore's top global ranking in AI Preparedness by the International Monetary Fund (IMF), as well as the launch of AI Verify as the world's first framework and testing tool for AI governance.

Singapore's approach to AI governance tends to be collaborative and principle-based on a voluntary basis. As of mid-2023, the government had not implemented binding regulations, instead focusing on learning from industry practices to formulate adaptive and contextual policies. This approach provides flexibility, allowing Singapore to avoid regulatory conflicts with global powers such as the United States, the European Union, and China, which adopt different AI regulatory strategies. However, reliance on soft law mechanisms raises questions

about long-term accountability, particularly concerning emerging technologies such as GenAI. Therefore, strengthening a more robust and accountable governance structure becomes crucial to ensure AI innovation continues while upholding ethical values and public trust.

As one of the largest banks in Singapore, DBS Bank has undergone a significant transformation in applying AI technology to optimise customer services and improve operational efficiency. By using AI in its risk management system, DBS Bank has achieved significant efficiencies, including an increase of up to 17 per cent in the value of funds saved from fraud attempts.

Based on the 2024 Sustainability Report published in March 2025, DBS Bank reported major updates in its risk management framework, including the implementation of AI-based risk assessments, strengthened governance and oversight of technology risks, and improvements to its defence systems against cyber threats. DBS Bank has also begun to integrate GenAI technology cautiously and gradually, with strict human oversight at every stage. The FEAT principles (Fairness, Ethics, Accountability, and Transparency) have been adopted as the foundation for the deployment of this technology, underscoring the bank’s commitment to transparency, customer data protection, and compliance with governance standards for handling data breaches.

Amid concerns about fraud and money mule activities, DBS Bank relies on AI, machine learning, and data analytics to detect and prevent such activities at an early stage. The fraud detection system is regularly updated, supported by the Anti-Scam Team working closely with the Singapore Police. In addition, the Anti-Mule Team uses AI models and advanced data analytics to identify suspicious transaction patterns and freeze funds obtained unlawfully.

The success of DBS Bank in integrating the FEAT principles into its AI-based operations demonstrates that, although the approach used is soft law and not legally binding, a comprehensively and appropriately designed framework can still provide effective protection. This approach offers institutions the flexibility to tailor the implementation of technology to their specific needs without deviating from the core values underlying these principles. It highlights the importance of adaptive and principle-based governance in the deployment of AI technology in the financial sector.

Based on the analysis of national regulatory frameworks and practices in various countries above, the author has prepared a comparative table to provide a more systematic overview of the approaches to regulating AI use in the financial sector. This table compares key aspects such as governance, legal accountability, personal data protection, and general approaches adopted by Indonesia, the European Union, the United States, and Singapore. The aim is to identify the strengths and weaknesses of each system and provide a basis for formulating a national regulation that is more adaptive and responsive to technological challenges.

Table 1. Comparison of AI Regulatory Frameworks in the Financial Sector

Regulatory Aspect	Governance	Legal Accountability	Data Protection	General Approach
Indonesia	No specific legal framework exists yet, still referring to the ITE Law, PDP Law, POJK No. 11/2022, and SEOJK No. 29/2022.	Principle of strict liability (Article 1367 of the Civil Code).	The PDP Law provides rights to personal data protection but does not yet regulate objections to	Fragmented and reactive. AI regulation in Indonesia requires harmonisation and regulatory updates to respond to rapid

Regulatory Aspect	Governance	Legal Accountability	Data Protection	General Approach
European Union	GDPR and AI Act: Classification of AI systems based on risk levels. Strict oversight of high-risk AI.	GDPR Article 22 prohibits fully automated decisions that have a significant impact without human intervention.	automated decisions. The GDPR emphasises individuals' rights over personal data, transparency, and control over automated data processing.	technological developments. Holistic, human rights-based approach. The AI Act supports sandboxes for risk-based innovation testing.
United States	NIST AI RMF: Voluntary approach consisting of four main functions, namely Govern, Map, Measure, and Manage.	No specific federal legal liability framework for AI exists yet. The NIST AI RMF is voluntary and does not directly create new legal obligations regarding accountability.	Sectoral and state-level approaches exist; there is no federal personal data protection law.	Industry-based soft law approach. The NIST AI RMF serves as a global guideline for AI risk management.
Singapore	The AI Governance Framework Model and AI Verify are used to assess ethics, transparency, and accountability in the development and deployment of AI.	There is still no binding regulation, but ethical guidelines (FEAT) from the Monetary Authority of Singapore (MAS) exist for accountability in AI use.	The PDPA supports explicit consent for the use of personal data. AI Verify is used to assess AI security and bias in data usage.	Collaborative and adaptive approach. Focus on regulatory flexibility and industry participation in AI policy development

3.2. Legal Liability for Losses Arising from the Use of AI in the Financial Sector

The development of AI technology in the financial sector has brought significant progress in terms of efficiency, speed, and service accuracy, particularly in payment systems, risk analysis, and fraud detection. However, alongside these benefits, there also arise risks of losses resulting from erroneous AI outputs, whether due to algorithmic flaws, data bias, or autonomous decisions that cannot be explained (the so-called black box problem) (Totschnig, 2020). These risks raise important questions about how the legal system can provide protection and enforce liability fairly and effectively for the affected parties.

From a technical perspective, AI in the financial sector operates through algorithmic approaches and large-scale data processing (big data), which enable the system to carry out assessments, detection, and predictions automatically (Dewi & Dewayanto, 2024). Examples include credit scoring systems that assess customer eligibility or fraud detection systems that

screen suspicious transactions in real time. Although designed to approximate human decision-making, AI still carries the potential to make errors with far-reaching financial consequences.

At present, Indonesia's legal framework does not yet have specific regulations that explicitly govern legal liability for the actions or errors of AI systems. In practice, legal liability for losses caused by AI is still based on Article 1367 of the Indonesian Civil Code (KUHPPerdata), which regulates liability for losses caused by persons or objects under someone's supervision. AI is positioned as an intangible property that may cause harm, and thus liability is imposed on the party that controls or supervises it (Simbolon, 2023).

Article 1367 paragraph (1) of the Indonesian Civil Code (KUHPPerdata) allows for the application of the principle of strict liability, meaning liability without the need to prove fault, as long as it can be established that there was control over the AI that caused the loss. This principle provides initial protection for the injured party, since it is sufficient to prove that a loss occurred and that there is a connection with the party exercising control over the AI, without having to trace elements of fault in detail.

However, in the context of AI that operates autonomously and in a complex manner, the principle of strict liability faces limitations. First, it is difficult to clearly identify who has dominant control over the AI, whether it is the system developer (software developer), the financial service provider, or the third party supplying data. Second, AI often engages in self-learning (machine learning) and makes decisions without direct human intervention, making it difficult to establish legal causation. Third, the "black box" nature of AI complicates the disclosure of decision-making processes, thereby weakening the transparency required in litigation.

In these circumstances, strict liability remains relevant but needs to be developed further. One approach is to strengthen the principle of risk-based liability, whereby the greater the complexity and risks of an AI system, the greater the obligations of supervision and accountability imposed on its operators. This principle encourages businesses not only to rely on the technical aspects of AI, but also to develop testing procedures, decision-making documentation, and system transparency as forms of risk mitigation that may serve as a basis for legal liability.

Another alternative is to promote a shared responsibility model, given that the AI ecosystem involves multiple actors. This model emphasises the importance of proportional allocation of responsibility between AI platform providers and users, particularly in the integration of AI into financial services. Therefore, contracts, technical standards, and service agreements should include clear liability clauses, as well as dispute resolution mechanisms. Such an approach helps prevent accountability gaps when losses occur beyond the control of a single party.

On the other hand, it is important to establish minimum accountability standards in the use of AI with wide-reaching impacts, such as credit and financial systems. These standards should include requirements for internal auditing, risk-based monitoring, and documentation of AI decision-making processes. Microsoft, through its Responsible AI Standard, stresses that the development and use of AI must be based on six core principles: fairness, reliability and safety, inclusiveness, transparency, and accountability. With such standards in place, AI operators can still be held accountable, even when AI acts autonomously.

Considering the potential risks of loss and the limitations of the existing legal framework, regulatory strengthening has become an unavoidable necessity to guarantee legal certainty and protection for affected parties. Legal reform should be directed towards creating a liability regime that is adaptive to technological dynamics, yet firmly grounded in the

principles of justice and legal protection. Strict liability can serve as the starting point, but it needs to be expanded through more detailed and contextual regulation, particularly concerning control over AI systems, evidentiary mechanisms, and the distribution of liability among the various stakeholders in the AI ecosystem.

3.3. The Urgency of Establishing Adaptive Regulations and Oversight Mechanisms

To date, Indonesia does not yet have specific and comprehensive regulations governing the use of AI in the financial sector. Several existing related laws, such as the Banking Law, the Law on Electronic Information and Transactions, the Personal Data Protection Law, as well as certain technical provisions under OJK and Bank Indonesia regulations, do not explicitly address the characteristics and complexities of AI systems, particularly those concerning autonomous systems, potential algorithmic bias, data security, and the challenges of liability in automated decision-making (Zaenudin & Riyan, 2024). This creates a gap that results in legal uncertainty, both for industry players and consumers.

The absence of specific regulations on AI poses a major challenge for regulators, given the rapid and large-scale development of technology. In practice, AI has already been widely applied in services such as chatbots, intelligent agents, and automated process methods, which have significantly improved operational efficiency and customer relations (Mikalef et al., 2023). However, because these systems operate autonomously on the basis of complex data, their decision-making processes cannot always be fully traced or controlled by humans. This indicates that the law should be able to adapt to technological dynamics, rather than forcing humans to adapt to the law. Therefore, if in the future we are faced with issues relating to AI, it is the law that must be adjusted and developed, not humans who must be compelled to conform to the existing legal framework. This line of thought aligns with Satjipto Rahardjo's theory of progressive law, which holds that progressive law enforcement is not merely about applying the black-and-white wording of regulations, but about realising the spirit and deeper meaning of statutes or law in its broader sense (Satjipto, 2009).

AI technology has unique characteristics that fundamentally distinguish it from conventional electronic systems. AI does not operate solely on standard programming logic; rather, it employs complex, machine-learning-based algorithms that enable the system to continuously learn, adapt, and make autonomous decisions based on ever-evolving and diverse data. The legal implications of such systems are profound, as AI can make decisions that are unpredictable and cannot be explained through human logic. The legal challenges that arise are not only related to proving fault or malicious intent, but also to establishing a causal link between the loss incurred and the decisions made by the system. Therefore, it is crucial to develop a new legal framework that governs principles of liability in the context of AI usage.

An ideal regulation would not only specify who is responsible, but also ensure the incorporation of principles such as accountability, algorithmic transparency, inclusiveness, credibility, and the obligation to disclose risks to consumers (Redita, 2024). These principles are essential to ensure that AI technology operates within clear legal boundaries, rather than in a legal vacuum. Without rigorous oversight, AI systems have the potential to generate discriminatory decisions that could harm consumers or even lead to serious violations of personal data protection.

In addition to substantive regulation, the establishment of effective and integrated oversight mechanisms is also an inseparable part of efforts to build a safe and equitable digital financial ecosystem. OJK and Bank Indonesia, as the main regulators of the financial sector, should be granted broader mandates to carry out supervisory functions over AI usage. This includes the authority to verify and certify AI systems employed by financial institutions,

mandate algorithm audits and periodic reporting on AI use, and establish consumer protection standards in line with principles of transparency and non-discrimination.

Supervision of AI usage should not be limited to responding after violations occur; it must be preventive from the outset, through oversight mechanisms implemented before AI systems are widely deployed in public services. This approach is crucial to prevent losses that may be difficult to remediate, given AI's highly adaptive nature and its operation at large scale and high speed. In this context, the application of preventive oversight aligns with perspectives emphasizing the importance of proactive and adaptive approaches to technological developments, including ensuring data quality, applying ethical practices, and maintaining consistent data security (Mahendra et al., 2024).

The urgency of regulating and supervising AI in the financial sector is further reinforced by global practices. The European Union, for example, has introduced the Artificial Intelligence Act, which adopts a risk-based approach whereby AI systems are classified according to their level of risk, from minimal risk to prohibited, imposing different legal obligations based on these categories. This approach represents a form of progressive regulation that balances public protection with technological innovation. Indonesia can draw lessons from this model to develop a national legal framework that is adaptive to global technological dynamics, while still respecting the characteristics and legal system of the nation based on Pancasila.

Therefore, the establishment of specific regulations and appropriate oversight mechanisms for AI use in the financial sector is an urgent need that cannot be postponed. The law must be able to address new realities in technological development and ensure that such advancements do not result in inequalities, losses, or violations of fundamental societal rights. Well-designed regulations will foster a digital financial system that is not only efficient, but also fair and transparent.

3.4. Recommendations for Institutional Reform and Strengthening Governance in AI Usage

In facing the digital era marked by the widespread use of AI, institutional reform and the strengthening of governance have become top priorities to achieve a responsive digital transformation. The use of AI in the financial sector presents regulatory and ethical challenges that existing institutional structures in Indonesia cannot yet fully address. Therefore, AI governance and policy must be grounded in the values of Pancasila, upholding principles of transparency and accountability.

First, institutional reform should be directed toward establishing a dedicated authority with the mandate, authority, and technical capacity to oversee AI. This body could either be independent or situated within an existing institution, such as OJK or Bank Indonesia, with its primary responsibilities including formulating AI supervisory policies, developing national standards for AI systems in finance, and establishing ethical guidelines and audit mechanisms for algorithm-based systems.

Second, AI governance in the financial sector must uphold the principles of transparency, accountability, and participation. Transparency is necessary to provide clarity and openness about how an AI system is developed, operated, produces outputs, and processes data. Accountability ensures that operators can be held responsible for AI systems that are developed and deployed in a manner that is reasonable, reliable, beneficial, fair, respectful of human rights, transparent, explainable, robust, and secure. Meanwhile, public participation is crucial to ensure that policies and regulations are not solely based on institutional perspectives, but also reflect public interests, particularly those of consumers who are most vulnerable to the impacts of AI use.

Third, institutional reform should also include strengthening internal oversight systems within financial service providers that use AI. Each institution needs a dedicated unit responsible for evaluating AI implementations in terms of legal compliance and adherence to ethical principles. Internal oversight should include regular algorithm audits, preparation of risk assessment and mitigation documents, and periodic reporting to supervisory authorities. This internal oversight should be linked to an incentive and sanction system that promotes compliance, including rewards for responsible innovation and penalties for violations of AI governance principles.

These governance and ethical principles have also been formulated in the OJK's AI Code of Ethics Guidelines, which establish five core principles: based on Pancasila, beneficial, fair and accountable, transparent and explicable, and robust and secure. These five principles form a crucial foundation for the responsible development of AI systems in the financial sector, aligning with Indonesia's need to ensure that AI applications adhere to ethical standards, accountability, and consumer protection.

Fourth, strong governance requires cross-stakeholder collaboration. According to the Agency for the Assessment and Application of Technology (BPPT), synergy is needed between the government, academia, industry players, and the public, orchestrated by ministries/agencies and an Ethics Commission (for oversight and policymaking), alongside non-governmental organizations that provide supportive functions and policy recommendations. The government can facilitate open and participatory policy dialogue forums and establish AI ethics research and development centers as a basis for policymaking. This collaboration is essential to develop ethical frameworks, balance oversight with support for AI development, strengthen consumer protection, and maintain national financial system stability.

Fifth, institutional reform and AI governance also require investment in human resource capacity building. Regulators and supervisors must possess digital competencies and a deep understanding of AI operations and their legal implications. Similarly, improving digital literacy among the public is essential so that consumers are aware of their rights and obligations when using AI-based financial services and can maintain control over personal data and system-generated decisions.

Strategically, all of the above recommendations align with the ethical and technology governance approach outlined in Indonesia's National Artificial Intelligence Strategy 2020–2045, which emphasizes participatory public policy, responsible oversight, and institutional strengthening to ensure inclusive benefits from AI use. Thus, institutional reform and strengthened governance are not restrictions on technological advancement, but rather state strategies to ensure that AI innovation develops within a sound legal framework, creating an inclusive, fair digital financial ecosystem that optimally protects consumers while safeguarding national financial system stability.

4. Conclusion

The rapid advancement of AI technology in Indonesia's financial sector has not been accompanied by adequate regulatory preparedness. This legal vacuum not only risks hindering the optimal use of technology, but also increases the likelihood of losses, data misuse, and automated decision-making that is detrimental to consumers. This study identifies three main issues that need to be addressed immediately: the absence of risk classification for AI use as stipulated in the Artificial Intelligence Act, the disparity between the increasingly widespread

use of AI and the weak oversight of algorithms, and the lack of comparative studies directly linking the national legal framework with global best practices in AI governance.

Additionally, regulatory fragmentation across sectors and the limited authority of supervisory bodies, such as the OJK and BI, further hinder the creation of a progressive and integrated legal system. Without expanded mandates and inter-agency coordination, oversight of advanced technologies like AI risks being ineffective. As a result, Indonesia risks becoming an open market for AI implementations that have not been tested ethically or legally, while other countries have established governance frameworks based on rights protection and the principle of caution.

Based on best practices applied in developed countries, a comparative study is needed to provide a constructive overview for Indonesia in adopting the principles contained in international regulatory models. These principles must then be aligned with national characteristics and needs, and harmoniously integrated with the values contained in Pancasila as the foundation of the state.

Therefore, the establishment of comprehensive and adaptive AI regulations is an urgent matter. These regulations must focus on the principles of responsibility, transparency, and accountability to ensure that financial institutions use technology ethically and do not jeopardise public interests. Technical standards such as algorithm audit requirements, human oversight, and regulatory sandbox mechanisms are also important to include in national policies. In this context, the AI Act provides a balanced framework between public protection and innovation, and can be adapted contextually to the values of Pancasila. Thus, Indonesia can build a more progressive legal system, in line with global dynamics, and capable of creating an inclusive, secure, and equitable digital financial ecosystem.

5. References

- Barrett, A. M., Hendrycks, D., Newman, J., & Nonnecke, B. (2022). Actionable guidance for high-consequence AI risk management: Towards standards addressing AI catastrophic risks. *ArXiv Preprint ArXiv:2206.08966*.
- Bayamloğlu, E. (2018). Transparency of automated decisions in the GDPR: an attempt for systemisation. *Available at SSRN 3097653*.
- Dewi, F. S., & Dewayanto, T. (2024). Peran Big Data Analytics, Machine Learning, Dan Artificial Intelligence Dalam Pendeteksian Financial Fraud: A Systematic Literature Review. *Diponegoro Journal of Accounting*, 13(3).
- Fraser, H., & Villarino, J.-M. B. (2024). Acceptable risks in Europe's proposed AI act: reasonableness and other principles for deciding how much risk management is enough. *European Journal of Risk Regulation*, 15(2), 431–446.
- Kunwar, M. (2019). *Artificial intelligence in finance: Understanding how automation and machine learning is transforming the financial industry*.
- Lukács, A., & Váradi, S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, 50, 105848.
- Mahendra, G. S., Ohyver, D. A., Umar, N., Judijanto, L., Abadi, A., Harto, B., Anggara, I. G. A. S., Ardiansyah, A., Saktisyahputra, S., & Setiawan, I. K. (2024). *Tren Teknologi AI: Pengantar, Teori, dan Contoh Penerapan Artificial Intelligence di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.
- Mazzini, G., & Bagni, F. (2023). Considerations on the regulation of AI systems in the financial sector by the AI Act. *Frontiers in Artificial Intelligence*, 6, 1277544.
- Mikalaf, P., Islam, N., Parida, V., Singh, H., & Altwaijry, N. (2023). Artificial intelligence (AI) competencies for organizational performance: A B2B marketing capabilities perspective. *Journal of Business Research*, 164, 113998.

- Munusamy, M. M., & Hashim, A. (2021). An analysis of the ASEM Education Process and its role in higher education. *European Journal of Education*, 56(3), 468–481.
- Nasman, N., Astuti, P., & Perwitasari, D. (2024). Etika Dan Pertanggungjawaban Penggunaan Artificial Intelengence Di Indonesia. *Jurnal Hukum Lex Generalis*, 5(10).
- Ningsih, N. H. I., SE, M. M., Misnawati, S. H., Muthia Sakti, S. H., Ordiyasa, I. W., Dadin Solihin, S. H., Batari, H. F., SH, M. H., Primasari, N. S., & Akhyar, C. F. (2025). *Hukum Ekonomi Digital: Regulasi Bisnis Di Era Teknologi*. PT. Nawala Gama Education.
- Pérez del Prado, D. (2025). *AI, right to information and new forms of participation: the Spanish experience*.
- Pflücke, F. (2025). Data Access and Automated Decision-Making in European Financial Law. *European Journal of Risk Regulation*, 16(1), 11–23.
- Redita, F. (2024). Menuju Era Digital: Tantangan Regulasi Bagi Penggunaan Artificial Intelligence Dalam Industri Perbankan. *Prosiding Seminar Nasional Bisnis, Teknologi Dan Kesehatan (SENABISTEKES)*, 1(1), 10–16.
- Ringe, W.-G., & Christopher, R. (2020). Regulating Fintech in the EU: the Case for a Guided Sandbox. *European Journal of Risk Regulation*, 11(3), 604–629.
- Ririh, K. R., Laili, N., Wicaksono, A., & Tsurayya, S. (2020). Studi komparasi dan analisis swot pada implementasi kecerdasan buatan (Artificial Intelligence) di Indonesia. *J@ Ti Undip: Jurnal Teknik Industri*, 15(2), 122–133.
- Roy, P. (2024). Enhancing Real-World Robustness in AI: Challenges and Solutions. *J. Recent Trends Comput. Sci. Eng*, 12(1), 34–49.
- Santana, A., Afonso, P., Zanin, A., & Wernke, R. (2017). Costing models for capacity optimization in Industry 4.0: Trade-off between used capacity and operational efficiency. *Procedia Manufacturing*, 13, 1183–1190.
- Satjipto, R. (2009). Penegakan Hukum suatu tinjauan sosiologis. *Yogyakarta: Genta Publishing*.
- Simbolon, Y. (2023). Pertanggungjawaban Perdata Terhadap Artificial Intelligence Yang Menimbulkan Kerugian Menurut Hukum Di Indonesia. *Veritas et Justitia*, 9(1), 246–273.
- Smuha, N. A. (2025). Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (EU Artificial Intelligence Act). *International Legal Materials*, 1–148.
- Suryanegara, M. (2023). Proposal of the Indonesian Framework for Telecommunications Infrastructure Based on Network and Socioeconomic Indicators. *Informatics*.
- Totschnig, W. (2020). Fully autonomous AI. *Science and Engineering Ethics*, 26(5), 2473–2485.
- Truby, J., Brown, R. D., Ibrahim, I. A., & Parellada, O. C. (2022). A sandbox approach to regulating high-risk artificial intelligence applications. *European Journal of Risk Regulation*, 13(2), 270–294.
- Zaenudin, I., & Riyan, A. B. (2024). Perkembangan Kecerdasan Buatan (AI) Dan Dampaknya Pada Dunia Teknologi. *Jurnal Informatika Utama*, 2(2), 128–153.
- Ziqra, Y., Sunarmi, S., Siregar, M., & Leviza, J. (2021). Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online. *Iuris Studia: Jurnal Kajian Hukum*, 2(2), 330–336.