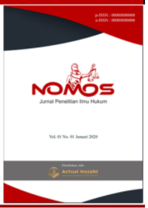
Nomos:
Jurnal Penelitian Ilmu Hukum
Vol. 5 No. 4 Tahun 2025 | Hal. 902 – 915



Legal Accountability in AI-Driven Banking Crimes: Regulatory Gaps and the Roles of Developers, Owners, and Users in Indonesia

Cynthia Putri Guswandi [a, 1*]
[a] Universitas Internasional Batam, Indonesia
[1] cynthia@uib.ac.id*
*korespondensi penulis

Informasi artikel :

Received:2 Juni 2025;
Revised: 23 July 2025;
Accepted: 6 August 2025.

Keywords:
Criminal Law;
Banking
AI Regulation;
Comparative Legal Study;
Security.

ABSTRACT

The development of Artificial Intelligence (AI) in the banking sector has triggered various potential criminal acts, presenting new challenges in the field of criminal law. Existing regulations reveal that the current legal framework has yet to adequately accommodate the complexity of cases involving AI systems, particularly with regard to assigning legal responsibility to developers, owners, and users. Most regulations remain focused on conventional criminal acts. This raises questions about the adequacy of Law No. 27 of 2022 on Personal Data Protection, various regulations issued by the Financial Services Authority (OJK), and the Indonesian Banking Artificial Intelligence Governance Guidelines in providing comprehensive legal protection. This study employs normative legal research with a comparative approach to regulatory systems in Singapore and China. It focuses on analyzing legal gaps and challenges in applying the principle of criminal liability to actors involved in AI-based banking systems. The findings highlight the necessity of strengthening regulations and updating legal doctrines to anticipate the complex risks posed by AI, while fostering accountability that adapts to technological advancements.

Kata-kata kunci:
Hukum Pidana;
Perbankan;
Regulasi AI;
Studi Hukum Perbandingan;
Keamanan.

ABSTRAK

Akuntabilitas Hukum dalam Kejahatan Perbankan Berbasis Kecerdasan Buatan: Kesenjangan Regulasi serta Peran Pengembang, Pemilik, dan Pengguna di Indonesia. *Perkembangan Artificial Intelligence (AI) dalam sektor perbankan telah memicu berbagai potensi tindak pidana yang menimbulkan tantangan baru dalam ranah hukum pidana. Berdasarkan peraturan yang ada, penggunaan AI di sektor ini menunjukkan bahwa kerangka hukum yang berlaku belum mampu mengakomodasi kompleksitas kasus kejahatan yang melibatkan sistem AI, khususnya dalam hal penetapan tanggung jawab hukum terhadap pengembang, pemilik, dan pengguna. Sebagian besar regulasi masih berfokus pada tindak pidana konvensional. Hal ini memunculkan pertanyaan mengenai kecukupan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, berbagai regulasi dari Otoritas Jasa Keuangan (OJK), serta panduan Tata Kelola Kecerdasan Artifisial Perbankan Indonesia dalam memberikan perlindungan hukum yang komprehensif. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perbandingan terhadap sistem regulasi di Singapura dan Tiongkok. Penelitian ini berfokus pada analisis kesenjangan hukum dan tantangan dalam penerapan prinsip pertanggungjawaban pidana terhadap pelaku yang terlibat dalam sistem AI perbankan. Hasil penelitian menunjukkan perlunya penguatan regulasi dan pembaruan doktrin hukum untuk mengantisipasi kompleksitas risiko kejahatan yang ditimbulkan AI serta mendorong akuntabilitas yang adaptif terhadap perkembangan teknologi.*

How to Cite : Guswandi, C. P. (2025). Legal Accountability in AI-Driven Banking Crimes: Regulatory Gaps and the Roles of Developers, Owners, and Users in Indonesia. *Nomos : Jurnal Penelitian Ilmu Hukum*, *5*(4), 902–915. https://doi.org/10.56393/nomos.v5i4.3224

Introduction

The development of artificial intelligence (AI) technology in Indonesia has demonstrated a remarkably rapid phenomenon, with the country recorded as one of the largest contributors of visits to global AI applications. In 2023, WriterBuddy reported that Indonesia ranked third worldwide, with a total of 1.4 billion visits, accounting for approximately 5.6% of all visits to AI applications globally (Nabilah Muhamad 2024). This phenomenon is increasingly relevant considering Indonesia's large population and widespread internet accessibility. The significant attention drawn by this trend is particularly evident through the widespread adoption of various AI applications by the Indonesian public, such as ChatGPT, which facilitates more efficient interaction between humans and technology (Putra, Taniady, and Halmadiningrat 2023; Mutmainnah and Pratama 2024; Ahzaza Fahrani and Gunawan Djajaputra 2024; Kurniawan, Hidayati, and Surdyanto 2023).

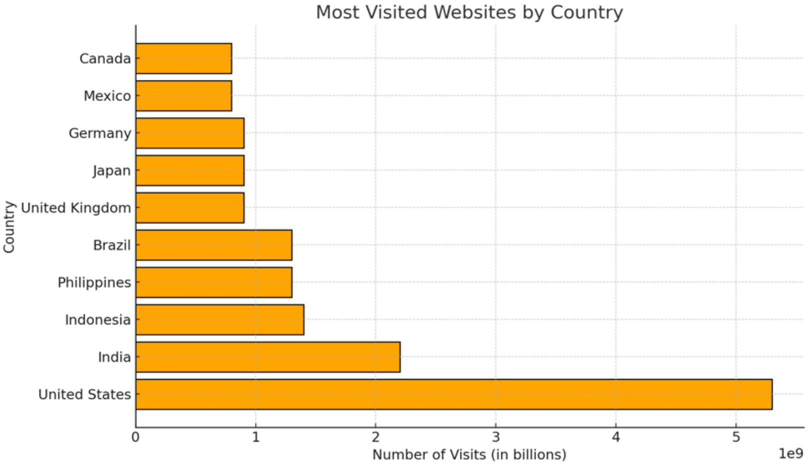


Figure 1. Highlights. the countries contributing the highest number of visits to AI applications worldwide.
Sourced: WriterBuddy's 2023 report on global AI application traffic (Nabilah Muhamad 2024).

In the banking industry, AI technology has brought substantial impacts across various operational aspects, including risk management (Permatasari, Salsabyla, and Nurfitri 2021), Banking services (Estefania and Widianto 2024), fraud detection (*fraud*) (Waromi, Rofingatun, and Siahay 2024), and other operational benefits have increasingly integrated AI technologies. McKinsey (2020) One industry report highlights that the implementation of AI in the banking sector offers four principal advantages: increasing profitability, enabling large-scale personalization, advancing omnichannel market development, and fostering corporate innovation ("Implementasi Artificial Intelligence (AI) Untuk Digital Banking," n.d.). The application of AI in banking operations is evident in various forms, including the use of virtual assistants or chatbots for customer service, fraud detection systems, and real-time risk monitoring. This is reflected in the fact that over 60% of major banks worldwide, including in Indonesia, have incorporated AI into their business systems ("Implementasi Artificial Intelligence (AI) Untuk Digital Banking," n.d.). Given the widespread use of AI in Indonesia's banking industry, this study addresses a central legal problem: the lack of clear legal accountability when AI systems autonomously commit harmful actions. The core issue lies in the absence of regulatory clarity on who bears criminal liability, developers, owners, or users when crimes are facilitated by AI. Unlike conventional offenses governed by clear human intent, AI challenges existing legal doctrine based on mens rea (criminal intent), creating a normative gap that demands doctrinal innovation.

However, despite the numerous benefits AI provides to the banking sector, its use also introduces significant legal risks and challenges, particularly concerning criminal offenses that may be facilitated through AI technologies. One of the AI-driven crimes that has emerged is the use of deepfake technology, which can be exploited to commit fraud or manipulate customer identities (Memei Apriana, Fransisco, and Any Nugroho 2025). This type of crime poses a serious threat that can harm both financial institutions and their customers. As the adoption of AI within the banking industry continues to grow, it becomes increasingly clear that effective oversight and appropriate regulatory frameworks are urgently needed to address these potential risks. Beyond AI-enabled crimes, issues such as consumer data manipulation and customer privacy violations also present pressing concerns. AI systems, which are designed to collect and analyze large volumes of data (big data), may be misused to access personal customer information without clear authorization or consent (Agustianto et al. 2025a). Data collected without proper oversight can result in harmful data breaches that significantly disadvantage customers (Isnugraheny, Megawati, and Susilawati 2024). Therefore, a comprehensive understanding of the responsibilities borne by AI developers, owners, and users within the banking sector is essential to ensure that the application of such technologies remains compliant with prevailing legal provisions, ethical standards, and consumer protection principles.

As the regulatory authority overseeing the financial services sector, the Financial Services Authority (Otoritas Jasa Keuangan/OJK) plays a pivotal role in educating and providing insights to stakeholders regarding both the potential and the challenges of AI implementation in the banking industry (Gandasari, Hidayat, and Siswajanthy 2025; Kartiko et al. 2024). In addressing these concerns, the OJK may organize webinars or training programs involving various parties, ranging from technology developers to banks that have adopted AI systems with the aim of enhancing their understanding of the risks involved and the responsibilities associated with the use of such technologies (Zakaria and Satyawan 2023). Nevertheless, within the scope of this study, a notable gap remains between das sein (the reality) and das sollen (what ought to be). On one hand, AI technology in the banking industry continues to advance rapidly; on the other hand, regulatory measures and supervisory mechanisms addressing AI-based crimes, data manipulation, and breaches of customer privacy have yet to reach a level of comprehensive and effective enforcement (WIllyams and Yusuf 2024).

This disparity raises important questions as to whether Law Number 27 of 2022 on Personal Data Protection, Law Number 11 of 2008 on Electronic Information and Transactions, various regulations issued by the OJK, and the Indonesian Banking Artificial Intelligence Governance Guidelines formulated by the OJK have provided sufficient legal protection and regulatory clarity concerning the application of AI within the banking sector. The absence of robust and adaptive legal frameworks has allowed opportunities for irresponsible parties to exploit AI technologies for criminal purposes within the financial services industry (Ihsan and Supriyadi 2024). Accordingly, this research seeks to identify and critically examine the legal issues associated with the use of AI in the banking sector, while also offering potential solutions to address the regulatory and supervisory gaps that currently persist. While prior studies have discussed AI's role in banking or emphasized user liability, they often overlook the shared legal responsibilities of developers and system owners. This research fills that gap by offering a broader normative framework that accounts for all actors involved in AI deployment and proposes legal reform grounded in risk-based accountability. This approach better aligns with the operational nature of AI, which can act beyond direct human intention.

This study focuses on the legal responsibilities of developers, owners, and users of Artificial Intelligence (AI) in the context of banking crimes. Each party plays a crucial role in preventing and addressing criminal activities involving AI, such as fraud, data misuse, and privacy violations. Developers are obligated to design secure systems that minimize the potential for misuse by irresponsible parties (Ghazmi 2021). Owners, in this case the banks, must ensure that the technologies they employ comply with prevailing regulations and established security standards (Frans et al. 2024). Meanwhile, AI users, including both customers and internal bank personnel, must be properly educated on the responsible and ethical use of AI systems (Chandra, Emirzon, and Yahanan 2019). Therefore, this study contributes to legal theory by arguing for a shift from traditional *mens rea*-based models of criminal responsibility to a risk-based liability framework. This proposed model emphasizes foreseeability, control, and systemic responsibility as key principles in regulating AI-driven financial technologies. This research is expected to make a significant contribution to the understanding of each party's responsibilities in the use of AI within the banking sector, while offering policy recommendations to support the creation of a secure and transparent banking environment. However, this study also acknowledges certain limitations, particularly in its coverage of specific AI-related criminal cases in Indonesia, given the limited availability of data and the relatively recent emergence of this phenomenon. Nevertheless, the findings of this research are intended to serve as a reference for developers, owners, and regulators in strengthening oversight and regulatory frameworks within the banking sector, as it navigates the challenges of an increasingly technology-driven era.

Research on artificial intelligence (AI) in relation to banking crimes is, in fact, not entirely new. Several scholars have conducted various studies aimed at understanding, developing, and optimizing AI technology within the field of criminal law in the banking sector. For instance, Mardian Putra Frans, Yudhistira Buana, Agustina Indah Intan Sari, Krismelia Panji, and Clivio Raharjo have analyzed the issue of corporate criminal liability of banks in cases where AI causes harm to customers, using the identification theory approach (Frans et al. 2024), Rahmi Ayunda and Rusdianto have focused on customer data protection in the context of AI use and emphasized the urgency for regulatory frameworks governing data protection in banking (Ayunda and Rusdianto 2021), Similarly, Abdul Hadi and Bima Guntara have discussed the absence of a specific legal framework addressing the use of AI in safeguarding personal data (Hadi and Guntara 2022). Based on these previous studies, it is evident that this research offers a distinctive contribution. Unlike earlier works, which primarily concentrated on the liability of banks as AI users, this study expands the scope by also examining the responsibilities of AI developers and owners, parties that are often overlooked in the discourse on criminal law in the banking industry. Furthermore, this research integrates a comparative analysis of international regulations and Indonesia's legal framework to propose more adaptive legal recommendations in response to the evolving use of AI in the banking sector.

Ultimately, this study also seeks to explore how existing regulations, both in Indonesia and other jurisdictions, might be adapted to address the emerging legal challenges arising from AI applications in banking services. Through this approach, the research aspires to offer new insights for strengthening legal systems governing AI use in the banking sector, while preventing criminal acts that could harm both customers and the financial services industry as a whole. Then This study formulates three main research problems as follows: What are the legal responsibilities of developers, owners, and users of Artificial Intelligence (AI) in the prevention of banking crimes?, How does the current regulatory system in Indonesia govern the responsibilities of AI developers, owners, and users in addressing AI-based crimes in the banking sector, and how does it compare to regulations in other countries? and What measures should be undertaken by banks (as AI owners) and other relevant stakeholders to ensure that the AI technologies in use comply with prevailing laws and regulations, and remain free from potential misuse that could result in harm?

Method

This study employs a normative legal research method, utilizing both statutory and comparative approaches. This methodology is chosen because the research focuses on legal responsibilities regulated by statutory provisions concerning the use of Artificial Intelligence (AI) in the banking sector, and how these laws are applied to prevent criminal acts (Priowirjanto, 2022). The normative approach is carried out by analyzing secondary legal materials, including national legislation such as Law No. 27 of 2022 on Personal Data Protection, regulations issued by the Financial Services Authority (OJK), academic legal literature, and official policy documents on AI governance (Disemadi, 2022). The selection of legal materials is based on their relevance to AI-related criminal liability in the financial sector and their authority in the Indonesian legal system. The study applies several interpretative techniques, such as systematic interpretation, to understand the coherence of AI regulations within the broader legal system, and teleological interpretation, to assess whether existing laws fulfill their intended objectives in regulating the use of AI to prevent banking crimes. In addition, the comparative approach is used to examine regulatory frameworks in Singapore and China, jurisdictions selected for their advanced and structured approaches to AI governance in financial services (Tan, 2021). These comparisons aim to identify potential gaps or lessons that can inform legal reforms in Indonesia. Methodologically, this research acknowledges certain limitations. First, it does not involve empirical validation through fieldwork or interviews, which may restrict insights into practical enforcement challenges. Second, the study recognizes a doctrinal limitation: the inapplicability of traditional *mens rea*-based liability in cases involving autonomous AI actions, which lack human intent. These challenges highlight the urgency of developing risk-based liability models that better reflect the operational nature of AI. Despite these limitations, the normative-comparative methodology enables a focused legal analysis and contributes to the formulation of more adaptive and forward-looking legal frameworks.

Result and Discussion

The responsibilities of AI stakeholders in the prevention of banking crimes. The development of Artificial Intelligence (AI) has brought about significant transformations across various industrial sectors, fundamentally altering operational systems in virtually every domain (Makridakis 2017). The banking sector has emerged as one of the fastest adopters of AI due to its dependence on data accuracy, transaction security, and real-time decision-making (Arifah, Wijaya, and Sholihah 2022; Indarto and Santoso 2024). AI has also become a defensive legal and technological tool, aimed not only at operational efficiency but at preventing increasingly complex financial crimes.

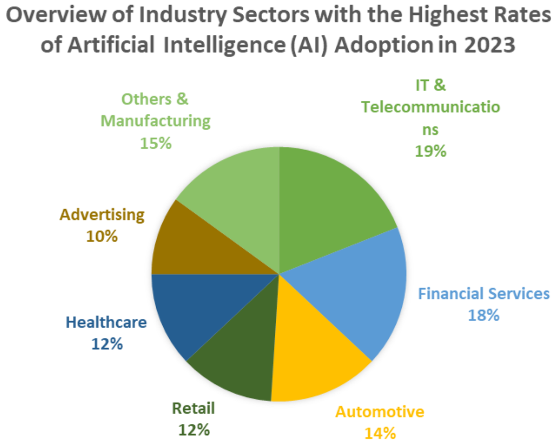


Figure 2. Industries with the Highest Rates of Artificial Intelligence Adoption
Source: Financial Services Authority (Otoritas Jasa Keuangan). (2025). *Governance of Artificial Intelligence in Indonesian Banking*. Retrieved from https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/

Based on the graph, it can be observed that the banking sector ranks second in terms of global adoption of artificial intelligence (AI). This reflects the urgency of embedding AI governance frameworks that are not only technical but also normative to address regulatory gaps in preventing misuse (Negarawati and Rohana 2024). However, behind these opportunities lie significant challenges, including the potential misuse of AI for banking-related crimes, the opacity of algorithmic processes, and ethical concerns surrounding personal data protection (Asriani et al. 2025). Consequently, it is imperative for the Indonesian banking sector to reinforce its AI governance frameworks in accordance with Financial Services Authority Regulation (POJK) No. 11 of 2022 on the Implementation of Information Technology by Commercial Banks and POJK No. 17 of 2023 on Commercial Bank Governance. Yet, both POJK No. 11 of 2022 and the Personal Data Protection Law (Law No. 27 of 2022) remain largely descriptive and lack explicit provisions on liability when AI operates autonomously. This exposes a doctrinal gap since Indonesian criminal law is still anchored on mens rea tied to human intent, leaving ambiguity when harm results from algorithmic actions without direct human control. This article adopts the theory of legal protection as the primary theoretical framework. As part of the government's efforts to safeguard the rights of its citizens, legal protection is implemented through regulations that are formulated and enforced upon every individual within the state's jurisdiction (Tampubolon 2016). According to Philipus M. Hadjon, legal protection is categorized into two forms: preventive protection and repressive protection. Preventive protection aims to avert violations by providing the public with an opportunity to express their views before a policy is enacted, whereas repressive protection serves as a remedial mechanism when legal rights have been violated, typically through legal processes such as complaints or lawsuits (Ranto 2019).

In the context of preventive legal protection, regulations and policies are essential to ensure that the development and use of AI in banking systems do not give rise to criminal risks, such as money laundering or digital fraud (Budiarto and Pujiyono, n.d.). However, without addressing doctrinal liability for AI autonomy, these preventive policies risk being purely procedural and failing to provide enforceable accountability. From a doctrinal perspective, applying traditional actus reus–mens rea principles to AI systems exposes major limitations. Because algorithms can act without human intent, this study highlights emerging debates on "algorithmic personhood" and proposes strict liability or reverse burden of proof for AI developers and owners. These approaches shift responsibility toward those with the greatest control over AI risk, closing gaps left by conventional fault-based liability. AI developers play a pivotal role in ensuring that the technologies they design are not only secure and efficient but also compliant with legal and ethical standards to prevent misuse in banking crimes. Rather than focusing solely on technical performance, developers carry a normative obligation to integrate accountability mechanisms within the architecture of AI systems. This includes designing algorithms capable of detecting transactional anomalies and potential fraud, while embedding strong cybersecurity protections to safeguard against malicious exploitation (Agustianto et al. 2025b). Beyond technical safeguards, developers must ensure auditability, transparency, and strict adherence to regulatory requirements such as Anti-Money Laundering (AML) and Know Your Customer (KYC), making these elements mandatory features rather than optional add-ons. AI owners, including banking institutions and fintech companies, hold the legal duty to ensure that AI deployment aligns with prevailing regulations and risk management frameworks (Frans et al. 2024). This responsibility extends beyond operational oversight into demonstrable due diligence: conducting systematic audits, ensuring traceability of AI decisions, and maintaining transparent systems to prevent regulatory loopholes. In addition, owners are required to provide comprehensive training for internal staff to understand both the technical operations and legal implications of AI use in detecting financial crimes. Effective collaboration with regulators and legal authorities becomes essential, positioning AI owners not merely as users of technology but as key actors in maintaining compliance and strengthening the overall banking security infrastructure.

Currently, the banking system has widely adopted AI-based technologies (Ramadhani and Trimuliani 2024; Amaliyah 2025; Dewi and Dewayanto 2024). Key implementations include *Fraud Detection Systems, Credit Scoring, Chatbot-Based Customer Services, Robo-Advisory Platforms, and Biometric Authentication Technologie*s. These applications illustrate the depth of AI integration into core banking operations, making them not only technological tools but also legal objects subject to regulatory oversight. While these systems enhance operational efficiency, they also generate legal questions concerning liability when AI errors occur, compliance with data protection laws, and the allocation of accountability among developers, owners, and users. Thus, their widespread adoption reinforces the urgency of clear regulatory frameworks to govern AI use in banking. One of the most crucial aspects in banking operations, particularly in the digital era and the increasing utilization of Artificial Intelligence (AI), is the obligation to safeguard the confidentiality and privacy of customer data (Prasetyo, Setyorini, and Michael 2025). This obligation is firmly regulated under Article 40 of Law Number 10 of 1998 concerning Banking, which stipulates that banks are required to maintain the confidentiality of information concerning depositors and their savings.

These provisions form the principal legal foundation for protecting personal customer data, including information processed by AI systems such as credit scoring, fraud detection, and chatbot services. However, current regulations were designed for human actors, not autonomous AI systems, creating uncertainty about liability when breaches result from algorithmic decisions rather than deliberate human intent. Sanctions for violations of these banking confidentiality provisions are set out in Article 47 of the Banking Law, which states that any person who intentionally breaches the obligation to maintain bank confidentiality, as regulated in Article 40, may be subject to criminal penalties. This reliance on “intentional” breach highlights a doctrinal gap: traditional fault-based liability assumes human intent (mens rea), whereas AI-driven processes can expose sensitive data without direct human action. Addressing this requires adapting banking confidentiality obligations to a risk-based framework that imposes strict liability on AI developers and owners, ensuring compliance regardless of algorithmic autonomy. Consequently, the implementation of AI within banking systems must remain within the boundaries of legal provisions, particularly with respect to the protection of customer personal data. Every AI data processing activity whether by developers, owners, or users should be governed not only by operational standards but also by explicit legal accountability mechanisms to close the regulatory gap between human and algorithmic actions. Additionally, this obligation is reinforced in Article 16 paragraph (1) letter b of Law Number 11 of 2008 on Electronic Information and Transactions.

Users of AI, including bank customers and employees, also bear significant responsibility in ensuring that this technology is used safely and appropriately. However, user responsibility must be situated within a structured accountability chain, where education and awareness complement but do not substitute, the primary legal duties of developers and owners (Ratuloli, Nubatonis, and Dinata 2025). Employees must be trained not only to operate AI but also to identify potential legal violations arising from algorithmic misuse, while customers should be informed of both the technological functions and their legal rights when engaging with AI systems. User education should go beyond technical literacy, incorporating awareness of compliance obligations and the mechanisms for legal recourse in cases of AI-driven harm (Junaedi et al. 2023). This aligns end-users with preventive legal protection models and ensures their role as active stakeholders in maintaining lawful AI use. Effective prevention of banking-related crimes necessitates close collaboration among AI developers, owners, and users. Collaboration must be institutionalized through clear regulatory frameworks that delineate each actor’s liability. Developers should carry strict design accountability, owners must demonstrate due diligence in operational oversight, and users are responsible for lawful interaction with AI systems. This tripartite model ensures that preventive and repressive legal protections function cohesively. With explicit accountability standards, secure technology, and comprehensive user education, AI can evolve into an effective legal and technological instrument for combating financial crime while reinforcing banking system integrity (Sari, Abigael, and Putri 2024).

AI-based banking crimes regulations: Indonesia and others countries. The advancement of Artificial Intelligence (AI) technology in the banking sector has prompted the government and relevant authorities in Indonesia to develop regulations aimed at mitigating the potential for AI-based crimes. The Financial Services Authority (Otoritas Jasa Keuangan, OJK) has taken proactive measures by issuing the Guidelines for Responsible and Trustworthy AI Ethics Code in the Financial Technology Industry (Arini 2025). This guideline, formulated with fintech associations such as AFTECH and AFSI, seeks to ensure ethical, transparent, and reliable AI deployment while mitigating future risks (Antara 2023). In addition to these guidelines, the OJK has issued several regulations, including POJK No.11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks. This regulation underscores the critical importance of risk management in technology usage by mandating policies and oversight mechanisms to prevent misuse of AI that could harm consumers and destabilize the financial system. Moreover, Law No. 27 of 2022 on Personal Data Protection (UU PDP) plays a pivotal role in regulating the use of personal data in the development and deployment Moreover, Law No. 27 of 2022 on Personal Data Protection (UU PDP) plays a pivotal role in regulating the use of personal data in AI deployment. However, both POJK and UU PDP adopt a conventional, human-centered liability model, lacking explicit provisions for autonomous AI decision-making. This creates a regulatory vacuum when breaches or harms are generated by algorithmic actions without direct human intervention (Aziz and Zaidan 2025).

As a comparison, Singapore's Monetary Authority (MAS) introduced the FEAT principles (Fairness, Ethics, Accountability, and Transparency) to govern AI and data analytics in the financial sector (Sudirman and Disemadi 2022). Unlike Indonesia's largely procedural POJK, FEAT embeds substantive accountability standards, explicitly requiring algorithmic explainability and risk allocation to financial institutions regardless of human intent. In contrast, China adopts a more centralized and stringent approach. Through the Cyberspace Administration of China (CAC), the government enforces strict oversight, including mandatory pre-approval of AI systems to safeguard national financial stability (Gong and Dorwart 2024; Tyrrell et al. 2025). China's model reflects a risk-based, state-controlled framework, emphasizing ex-ante prevention rather than post-incident liability. The comparative analysis reveals Indonesia's regulatory gap: while POJK and UU PDP provide general data and risk management rules, they lack doctrinal clarity on AI autonomy, algorithmic accountability, and burden of proof allocation. This study argues that Indonesia must adopt either a strict liability or reverse burden of proof regime for AI developers and owners, similar to the approach reflected in Singapore's FEAT and China's CAC oversight, to ensure enforceable accountability. Given the rapid development of AI, Indonesia must continuously update its regulations to remain relevant amidst emerging challenges. Policy reform must move beyond reactive compliance and incorporate adaptive legal doctrines that anticipate AI autonomy. Collaboration between regulators, academia, and industry remains critical (Azis and Redi 2025), but must be coupled with doctrinal innovation to bridge the liability gap. Digital literacy and public education are also critical in mitigating AI-based crime risks. To maintain this balance, Indonesia's regulatory framework must explicitly integrate both preventive measures (risk assessments, ex-ante approval) and repressive measures (strict liability, sanctions for AI misuse), aligning with international best practices while ensuring local relevance (Kristiyenda, Faradila, and Basanova 2025).

Legal compliance and ai misuse prevention. In the rapidly advancing digital era, Artificial Intelligence (AI) has become an integral part of various aspects of life. However, alongside this progress lies a significant challenge: ensuring that AI is used in compliance with applicable laws and is not exploited for harmful purposes (Farida and Wulan 2024). Consequently, a range of measures must be undertaken to address these challenges effectively. A primary step involves establishing clear and stringent regulations governing the development and deployment of AI. Current Indonesian regulations, while emphasizing risk management and data protection, remain descriptive and lack normative mechanisms to allocate liability when AI systems act autonomously. This creates a doctrinal vacuum in criminal law, which traditionally relies on human intent (mens rea). Regulations should therefore be carefully designed to accommodate technological innovation while upholding legal and ethical standards. The government plays a crucial role in formulating policies that balance innovation with the imperative of legal protection. Beyond regulation, adherence to ethical principles in AI development is equally essential. AI systems must be created with due regard for transparency, accountability, and non-discrimination. Embedding ex-ante obligations such as auditability and algorithmic explainability is critical to prevent AI misuse and address accountability gaps. This approach aims to prevent algorithmic biases that could disadvantage certain groups and to ensure that decisions made by AI remain fair and just (Irawan 2024).

Regular oversight must also be implemented to guarantee that AI usage remains within safe and lawful boundaries. Routine audits serve as a critical mechanism to identify potential deviations or abuses at an early stage, enabling prompt corrective action. Furthermore, the enforcement of stringent sanctions against those who misuse AI is imperative. Without clearly defined penalties, the risk of abuse escalates. Sanctions may include fines, revocation of business licenses, or other legal measures commensurate with the severity of the violation (Salsabila and Wiraguna 2025). However, to address AI autonomy, Indonesia needs to consider shifting from fault-based to strict liability or adopting a reverse burden of proof for AI developers and owners. This aligns responsibility with those who design and control AI systems rather than requiring proof of intent, which algorithms lack. Collaboration among the government, technology industry stakeholders, and academic institutions constitutes a cornerstone in ensuring AI's compliance with the law. Through effective cooperation, regulations and policies can be implemented more efficiently and remain adaptive to the continually evolving technological landscape.

Enhancing digital literacy among the public is a crucial aspect that requires significant attention. Education about Artificial Intelligence (AI), including both its benefits and risks, must be widely disseminated to raise public awareness about the potential misuse of this technology (Sudaryanto and Hanny 2023). A well-informed society will be better equipped to monitor and oversee the application of AI across various sectors. Technology companies must ensure transparency in the algorithms and decision-making processes embedded within their AI systems. This transparency enables the public to better understand how AI functions and empowers them to identify any deviations or injustices in its implementation. Data security is another critical element that cannot be overlooked. Therefore, enhancing protections for personal data is imperative to prevent leakage or misuse of sensitive information. Developers should consistently apply the principle of fairness throughout all stages of AI development to ensure the technology genuinely benefits everyone. One practical measure to prevent AI misuse is the establishment of whistleblowing systems (Harmen et al. 2025). Such systems allow individuals to report violations or abuses of AI safely and anonymously, without fear of retaliation (Dela and Frinaldi 2023). Ongoing research focused on AI security must be intensified. Through comprehensive studies, potential risks can be identified early, allowing for preventive measures before widespread misuse occurs. Risk assessments should not only analyze operational risks but also evaluate the allocation of legal responsibility when AI decisions cause harm, ensuring that liability does not disappear in the gap between human and algorithmic actions. International cooperation is also essential in regulating AI use. Given that AI is a borderless technology, national regulations must align with global standards to avoid conflicts and ensure harmonious utilization worldwide (Pakina and Solekhan 2024). Law enforcement agencies should be empowered with adequate technological tools and training to effectively address AI misuse cases promptly and accurately (BR 2025). At the same time, harmonization should include doctrinal debates on algorithmic personhood and accountability models to ensure Indonesia's framework aligns with evolving international norms.

The primary responsibility for the consequences of AI extends beyond its users to include the developers themselves. Developers must be accountable for their products and ensure that their technologies are not deployed for unlawful purposes. Certification and standardization of AI systems are critical in guaranteeing the safety and reliability of widely used AI technologies. AI intended for large-scale deployment should undergo rigorous certification processes to verify its security. Moreover, the protection of human rights must remain a fundamental consideration in AI applications. AI should never be employed to threaten or violate fundamental rights, including privacy, freedom of expression, and the right to be free from discrimination (Syahril et al. 2024). Ultimately, building a comprehensive legal framework requires integrating technical safeguards, ethical standards, and adaptive liability rules to ensure AI benefits society while mitigating risks in a sustainable and enforceable manner. In the rapidly advancing digital era, Artificial Intelligence (AI) has become an integral part of various aspects of life. However, alongside this progress lies a significant challenge: ensuring that AI is used in compliance with applicable laws and is not exploited for harmful purposes (Farida and Wulan 2024). Consequently, a range of measures must be undertaken to address these challenges effectively. A primary step involves establishing clear and stringent regulations governing the development and deployment of AI. Such regulations should be carefully designed to accommodate technological innovation while upholding legal and ethical standards. The government plays a crucial role in formulating policies that balance innovation with the imperative of legal protection. Beyond regulation, adherence to ethical principles in AI development is equally essential. AI systems must be created with due regard for transparency, accountability, and non-discrimination. This approach aims to prevent algorithmic biases that could disadvantage certain groups and to ensure that decisions made by AI remain fair and just (Irawan 2024).

Regular oversight must also be implemented to guarantee that AI usage remains within safe and lawful boundaries. Routine audits serve as a critical mechanism to identify potential deviations or abuses at an early stage, enabling prompt corrective action. Furthermore, the enforcement of stringent sanctions against those who misuse AI is imperative. Without clearly defined penalties, the risk of abuse escalates. Sanctions may include fines, revocation of business licenses, or other legal measures commensurate with the severity of the violation (Salsabila and Wiraguna 2025). Collaboration among the government, technology industry stakeholders, and academic institutions constitutes a cornerstone in ensuring AI's compliance with the law. Through effective cooperation, regulations and policies can be implemented more efficiently and remain adaptive to the continually evolving technological landscape. Enhancing Digital Literacy and Strengthening Responsible AI Use Improving digital literacy among the public is a crucial aspect that requires significant attention. Education about Artificial Intelligence (AI), including both its benefits and risks, must be widely disseminated to raise public awareness about the potential misuse of this technology (Sudaryanto and Hanny 2023). A well-informed society will be better equipped to monitor and oversee the application of AI across various sectors. Technology companies must ensure transparency in the algorithms and decision-making processes embedded within their AI systems. This transparency enables the public to better understand how AI functions and empowers them to identify any deviations or injustices in its implementation. Data security is another critical element that cannot be overlooked. Therefore, enhancing protections for personal data is imperative to prevent leakage or misuse of sensitive information.

Developers should consistently apply the principle of fairness throughout all stages of AI development to ensure the technology genuinely benefits everyone. One practical measure to prevent AI misuse is the establishment of whistleblowing systems (Harmen et al. 2025). Such systems allow individuals to report violations or abuses of AI safely and anonymously, without fear of retaliation (Dela and Frinaldi 2023). Ongoing research focused on AI security must be intensified. Through comprehensive studies, potential risks can be identified early, allowing for preventive measures before widespread misuse occurs. Risk assessments should be conducted prior to the broad implementation of AI systems. These assessments must analyze possible negative impacts and develop mitigation strategies to address any potential abuses. International cooperation is also essential in regulating AI use. Given that AI is a borderless technology, national regulations must align with global standards to avoid conflicts and ensure harmonious utilization worldwide (Pakina and Solekhan 2024). Law enforcement agencies should be empowered with adequate technological tools and training to effectively address AI misuse cases promptly and accurately (BR 2025). The primary responsibility for the consequences of AI extends beyond its users to include the developers themselves. Developers must be accountable for their products and ensure that their technologies are not deployed for unlawful purposes. Certification and standardization of AI systems are critical in guaranteeing the safety and reliability of widely used AI technologies. AI intended for large-scale deployment should undergo rigorous certification processes to verify its security. Moreover, the protection of human rights must remain a fundamental consideration in AI applications. AI should never be employed to threaten or violate fundamental rights, including privacy, freedom of expression, and the right to be free from discrimination (Syahril et al. 2024). The development of technology must always adhere to principles of responsibility to ensure that its benefits are realized fairly and sustainably by all.

Conclusion

This study finds that the responsibilities of AI developers, owners, and users in the banking sector must be understood not only in operational terms but also within a clear framework of legal accountability. The complexity of AI systems challenges traditional criminal law principles, especially the doctrine of actus non facit reum nisi mens sit rea, as AI actions may cause harm without direct human intent. Building on this, the study proposes a shift toward a risk-based liability model, where accountability is allocated based on control, foreseeability, and negligence rather than intentionality alone. To address this gap, the study recommends the establishment of a dedicated Banking AI Liability Regulation that imposes explicit duties on developers to ensure algorithmic transparency, AML/KYC compliance, and auditability as enforceable standards. For AI owners, including banks and fintech companies, the study advocates extending corporate criminal liability doctrines to AI governance, ensuring institutional responsibility even in cases of autonomous system failures. Users, both employees and customers, must be integrated into a mandatory digital literacy and reporting mechanism to strengthen early detection and prevention of AI misuse.Indonesia's current regulatory framework, while progressing, remains fragmented and reactive compared to Singapore's FEAT principles and China's stringent CAC oversight. Therefore, normative legal reform is urgently required, with coordinated synergy among the Financial Services Authority (OJK), Bank Indonesia (BI), the Ministry of Communication and Information (KOMINFO), and law enforcement agencies to build a unified and adaptive regulatory architecture. By combining doctrinal innovation, inter-regulatory collaboration, and proactive legislative reform, this study contributes to the development of an accountability framework that can accommodate AI autonomy, ensuring that banking AI technologies function as both operational and legal tools to prevent financial crime in the digital era.

Referensi

Agustianto, Agustianto, Henry Soelistyo Budi, Lu Sudirman, Nurlaily Nurlaily, and Windi Afdal. 2025. "Analisis Risiko Finansial Perbankan Melalui Artificial Intelligence (AI): Politik Hukum Dan Potensi Pengembangan Hukum." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 14 (1): 17. https://doi.org/10.24843/JMHU.2025.v14.i01.p02.

Ahzaza Fahrani, and Gunawan Djajaputra. 2024. "Legal Validity with Artificial Intelligence Technology on Gpt Chat as Legal Aid." *Journal of Law, Politic and Humanities* 5 (1): 54–61. https://doi.org/10.38035/jlph.v5i1.891.

Amaliyah, Rizki. 2025. "Efektivitas Penggunaan Teknologi Artificial Intelligence Terhadap Proteksi Keamanan Sistem Tata Kelola Perusahaan (Sektor Perbankan)." *Info Kripto* 19 (1): 49–60. https://doi.org/10.56706/ik.v19i1.121.

Arifah, Ika Diyah Candra, Mahaning Indrawaty Wijaya, and Silviana Mar'atus Sholihah. 2022. "JOB Replacement Artifical Intelligence Di Industri Jasa: Tinjauan Pustaka Sistematis." *Jurnal Ilmu Manajemen*, September, 911–29. https://doi.org/10.26740/jim.v10n3.p911-929.

Asriani, Asriani, Misnah Irvita, Robi Rendra Tribuana, and Rahmiati Ranti Pawari. 2025. "Pembangunan Hukum Di Era Digital: Tantangan Dan Peluang Bagi Negara Dalam Menghadapi Transformasi Teknologi." *Jurnal Bisnis Mahasiswa* 5 (1): 164–74. https://doi.org/10.60036/jbm.v5i1.324.

Ayunda, Rahmi, and Rusdianto Rusdianto. 2021. "Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence Dalam Aktifitas Perbankan Di Indonesia." *Jurnal Komunikasi Hukum* 7 (2). https://doi.org/https://doi.org/10.23887/jkh.v7i2.37995.

Budiarto, Agung, and Pujiyono. n.d. "Perlindungan Hukum Nasabah Pengguna Mobile Banking." *Perlindungan Hukum Nasabah Pengguna Mobile Banking* 9 (2): 300–308. https://doi.org/10.20961/privat.v9i2.60038

Chandra, Surya, Joni Emirzon, and Annalisa Yahanan. 2019. "Perlindungan Hukum Bagi Nasabah Pt Bank Mandiri (Persero) Tbk Sebagai Pengguna Fasilitas Layanan Mandiri Online." *Lex LATA* 1 (2). https://doi.org/10.28946/lexl.v1i2.496.

Dewi, Finecia Shinta, and Totok Dewayanto. 2024. "Peran Big Data Analytics, Machine Learning, Dan Artificial Intelligencedalam Pendeteksian Financial Fraud: A Systematic Literature Review." *Diponegoro Journal Of Accounting* 13 (3): 1–15.

Disemadi, Hari Sutra. 2022. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24 (2): 289. https://doi.org/10.37253/jjr.v24i2.7280.

Estefania, Vincencia Evelyn, and Yonatan Widianto. 2024. "Revolusi Layanan Perbankan : Studi Implementasi Teknologi AI Pada Bank BCA." *Jurnal Sistem Cerdas Dan Rekayasa (JSCR)* 6 (2): J41-J4-5. https://doi.org/https://doi.org/10.61293/jscr.v6i2.732.

Frans, Mardian Putra, Agustina Indah Intan Sari, Krismelia Y Panji, and Yudhistira Buana Cipta Ismara. 2024. "Pertanggungjawaban Pidana Bank Sebagai Pengguna Artificial Intelligence." *JURNAL USM LAW REVIEW* 7 (2): 901–15. https://doi.org/10.26623/julr.v7i2.9026.

Gandasari, Nur Mutiara, Rendy Riansyah Hidayat, and Farahdinny Siswajanthy. 2025. "Peran Otoritas Jasa Keuangan (OJK) Dalam Mengawasi Fintech Lending Sebagai Instrumen Ekonomi Digital." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3 (1): 399–408. https://doi.org/https://doi.org/10.62976/ijijel.v3i1.941.

Ghazmi, Shabrina Fadiah. 2021. "Urgensi Pengaturan Artificial Intelligence Pada Sektor Bisnis Daring Di Indonesia." *Jurnal Hukum Lex Generalis* 2 (8): 782–803. https://doi.org/10.56370/jhlg.v2i8.104.

Hadi, Abdul, and Bima Guntara. 2022. "Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence)." *Jurnal Hukum Mimbar Justitia* 8 (1): 233. https://doi.org/10.35194/jhmj.v8i1.2426.

Ihsan, Robby Maulana, and Aditya Prastian Supriyadi. 2024. "Pertanggungjawaban Hukum Tindak Pidana Ekonomi Melalui Artificial Intelligence Perspektif Hukum Islam Dan Hukum Positif Indonesia." *Journal of Islamic Business Law* 8 (1): 115–29. https://doi.org/https://doi.org/10.18860/jibl.v8i1.7089.

Indarto, Muhammad, and Bambang Santoso. 2024. "Efektivitas Pemanfaatan BigData Dalam Pengambilan Keputusan Strategis Di Industri Perbankan." *Jurnal Bisnis Dan Manajemen (JURBISMAN)* 2 (4). https://doi.org/10.61930/jurbisman.v2i4.900.

Isnugraheny, Rizqika Farah, Zahra Ekasiwi Megawati, and Siti Susilawati. 2024. "Optimalisasi Prinsip Kerahasiaan Data Nasabah Dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi." *Media Hukum Indonesia (MHI)* 2 (4). https://doi.org/https://doi.org/10.5281/zenodo.14181761.

Junaedi, Achmad Tavip, Nicholas Renaldo, Indri Yovita, Kristy Veronica, and Sudarno Sudarno. 2023. "Peluang Dan Tantangan Bank Syariah Di Era Perbankan Digital Dalam Persepktif Generasi Z." *Kurs : Jurnal Akuntansi, Kewirausahaan Dan Bisnis* 8 (2). https://doi.org/10.35145/kurs.v8i2.3462.

Kartiko, Nafis Dwi, Samuel Putra Soegiono, Carissa Amanda Siswanto, and Astrid Athina Indradewi. 2024. "Perlindungan Konsumen Sektor Keuangan: Peran OJK Dalam Menghadapi Ancaman Phising Dan Skimming." *Jurnal Studia Jurnal Kajian Hukum* 5 (2): 347–63. https://doi.org/https://doi.org/10.55357/is.v5i2.616.

Kurniawan, Wiwit, Tri Hidayati, and Annas Surdyanto. 2023. "Pengenalan Sistem Chatbot Interaktif Berbasis Chatgpt Dan Wolfram Alpha Untuk Mendukung Pembelajaran Di Era Digital." *Praxis: Jurnal Pengabdian Kepada Masyarakat* 3 (4): 6–10. http://pijarpemikiran.com/index.php/praxis/article/view/617/577.

Makridakis, Spyros. 2017. "The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms." *Futures* 90 (June):46–60. https://doi.org/10.1016/j.futures.2017.03.006.

Marheni, Ni Putu Ria Dewi. 2014. "Perlindungan Hukum Bagi Konsumen Berkaitan Dengan Pencantuman Disclaimer Oleh Pelaku Usaha Dalam Situs Internet (Website)." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 3 (1). https://doi.org/10.24843/JMHU.2014.v03.i01.p11.

Memei Apriana, Fransisco, and Any Nugroho. 2025. "Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (Ai) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual." *Journal of Social and Economics Research* 7 (1): 57–75. https://doi.org/10.54783/jser.v7i1.796.

Mutmainnah, Ummu Kaidah, and Muhammad Farhan Pratama. 2024. "Fenomena Artificial Intelligence Hallucination: Tantangan Penggunaan Data Bohong Terhadap Jalannya Praktik Advokat Menurut Hukum Indonesia." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 13 (2): 241–54. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v13i2.1781.

Nabilah Muhamad. 2024. "10 Negara Penyumbang Kunjungan Ke Aplikasi Artificial Intelligence/AI Terbanyak Global (2023)." Katadata Media Network. January 30, 2024. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/a49ed3eb121983b/indonesia-penyumbang-kunjungan-aplikasi-ai-terbanyak-ke-3-di-dunia.

Negarawati, Esa, and Siti Rohana. 2024. "Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital." *Jurnal Ekonomi, Bisnis Dan Manajemen* 3 (4): 46–60. https://doi.org/10.58192/ebismen.v3i4.2712.

Permatasari, Mutiara Dewi, Nisa Aurelya Salsabyla, and Nurfitri Nurfitri. 2021. "Application of Artificial Intelligence-Based Risk Management in Banking." *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi* 12 (2): 01–09. https://doi.org/10.33558/jrak.v12i2.2886.

Prasetyo, Dani Satiaji, Erny Herlin Setyorini, and Tomy Michael. 2025. "Penadahan Digital: Analisis Sistematis Kebutuhan Pengaturan Dalam Uu Ite." *Journal of Innovation Research and Knowledge* 4 (12): 9103–14.

Priowirjanto, Enni Soerjati. 2022. "Urgensi Pengaturan Mengenai Artificial Intelligence Pada Sektor Bisnis Daring Dalam Masa Pandemi Covid-19 Di Indonesia." *Jurnal Bina Mulia Hukum* 6 (2): 254–72. https://doi.org/10.23920/jbmh.v6i2.355.

Putra, Gio Arjuna, Vicko Taniady, and I Made Halmadiningrat. 2023. "Tantangan Hukum: Keakuratan Informasi Layanan Ai Chatbot Dan Pelindungan Hukum Terhadap Penggunanya." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 12 (2): 281–99. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v12i2.1258.

Ramadhani, Fanny, and Diva Trimuliani. 2024. "Pemanfaatan Sistem Artificial Intelligence Pada Industri Perbankan: Systematic Literature Review." *Jurnal Mutiara Akuntansi* 9 (1): 37–49. https://doi.org/10.51544/jma.v9i1.5281.

Ranto, Roberto. 2019. "Tinjauan Yuridis Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Melalui Media Elektronik." *Jurnal Ilmu Hukum: Alethea* 2 (2): 145–64. https://doi.org/10.24246/alethea.vol2.no2.p145-164.

Ratuloli, Samson, Orpa J. Nubatonis, and Husni Kusuma Dinata. 2025. "Analisis Perlindungan Hukum Terhadap Nasabah Pengguna Internet Banking Pada Bank Bri." *Petitum Law Journal* 2 (2): 343–57. https://ejurnal.undana.ac.id/index.php/plj/article/view/18641.

Sari, Khansa Inggita, Maria Claudita Abigael, and Ambar Krisna Putri. 2024. "Perlindungan Hukum Nasabah Terhadap Bocornya Rahasia Data M-Bangking Di Era Digital." *Jurnal Multidisiplin Ilmu Akademik* 1 (6): 335–47. https://doi.org/https://doi.org/10.61722/jmia.v1i6.3039.

Tampubolon, Wahyu Simon. 2016. "Upaya Perlindungan Hukum Bagi Konsumen Ditinjau Dari Undang Perlindungan Konsumen." *Jurnal Ilmiah Advokasi* 4 (1): 53–61. https://doi.org/10.36987/jiad.v4i1.356.

Tan, David. 2021. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 8 (8): 2463–78. https://doi.org/http://dx.doi.org/10.31604/jips.v8i8.2021.2463-2478.

Waromi, Juliana, Siti Rofingatun, and Adolf Z.D. Siahay. 2024. "Penerapan Teknologi Artificial Intelligence (Ai) Dalam Proses Pengenalan Pola Penipuan Dan Kecurangan." *Jurnal Review Pendidikan Dan Pengajaran (JRPP)* 7 (2). https://doi.org/https://doi.org/10.31004/jrpp.v7i2.27266.

WIllyams, Flugencius Janssen, and Hadi Yusuf. 2024. "Peran Otoritas Jasa Keuangan Dalam Mencegah Tindak Pidana Perbankan Dan Pencucian Uang Di Indonesia." *Jurnal Intelek Insan Cendikia* 1 (9): 5292–5308.

Zakaria, Rian, and Made Satyawan. 2023. "Strategi Implementasi Fintech Reward Crowdfunding Di Indonesia Sektor Ekonomi Kreatif." *Jurnal Bisnis Dan Manajemen West Science* 2 (02): 145–67. https://doi.org/10.58812/jbmws.v2i02.328.