Research Article

The Potential Misuse of Artificial Intelligence Technology Systems in Banking Fraud

Hijriani[1*], Muhammad Nadzirin Anshari Nur[2], Sahyunu[3], Gulzhaina K. Kassymova[4]
[1]Master of Law, Postgraduate Universitas Sulawesi Tenggara, Indonesia
[2]Faculty of Technic, Universitas Halu Oleo, Indonesia
[3]Faculty of Economic and Management, Universitas Sulawesi Tenggara, Indonesia
[4]Abai Kazakh National Pedagogical University, Kazakhstan
***hijriani@gmail.com**

ABSTRACT

The use of Artificial Intelligence (AI) in the banking sector can enhance the effectiveness and efficiency of banking services. However, it also carries the risk of misuse by irresponsible parties, potentially leading to significant financial losses. This research aims to identify and analyze the potential misuse of AI in banking systems and provide recommendations for risk mitigation.This study employs a normative juridical research method, incorporating case studies and legislative analysis. The findings reveal vulnerabilities in AI algorithm security within the banking sector and demonstrate that AI implementation can be exploited for fraudulent activities. These findings underscore the need for updates to procedural laws, particularly concerning the evidence system, to establish clear criminal liability for legal entities or individuals.The study concludes that regulatory adjustments related to the evidence system and the implementation of banking principles are essential to minimizing the risks of AI-based fraud.

Keywords: Artificial Intelligence; Fraud; AI Security; Regulation; Risk Mitigation.

A. INTRODUCTION

Artificial Intelligence (AI) technology has transformed various aspects of life, including the banking sector (Hanila & Alghaffaru, 2023). In banking, AI is utilized to detect suspicious activities and prevent fraud (Hijriani et al., 2022). By analyzing transaction patterns and customer behavior with high speed and accuracy, AI proves to be more effective in identifying unusual transactions compared to conventional methods. However, despite its potential, AI also carries a significant risk of misuse by cybercriminals, who may manipulate the system to commit fraud (Yamin et al., 2024).

AI technology plays a crucial role in assisting banks in detecting suspicious activities and preventing fraud. Through machine learning, security systems can learn from past patterns and identify unusual transactions with greater accuracy (Hassan, Aziz, & Andriansyah, 2023). AI-powered security systems can process vast amounts of data rapidly (Christia et al., 2024) and efficiently compare it against datasets of normal customer activities, allowing for the swift detection of suspicious behavior (Kurniawan, Sastra, & Sudarma, 2020). By assessing abnormal transaction patterns and behaviors, AI enhances the identification of potential fraud cases (Lee,

2020). With more precise analysis, banks can mitigate financial risks and better protect their customers.

The use of AI in fraud detection offers several advantages over conventional methods. AI can analyze data rapidly and identify suspicious patterns more efficiently than manual methods (Shamaya et al., 2023). Implementing AI can significantly accelerate the fraud identification process. By utilizing AI systems, fraud committed by specific legal subjects can be detected with a high degree of certainty and accuracy (Kurniawan, Sastra, & Sudarma, 2024). AI also helps reduce false positives while increasing detection accuracy (Sinaga, Irmayani, & Hasibuan, 2024). Furthermore, AI can learn from new data and adapt to evolving fraud patterns, continuously updating its models to counter emerging fraudulent tactics (Mayana et al., 2024).

The implementation of AI technology in the banking industry holds substantial potential for detecting and preventing fraud. AI applications in banking include automating tasks for chatbots and voice assistants, document processing, transaction monitoring, fraud and money laundering detection, and decision-making in credit scoring processes. However, there have been instances where AI has been misused. Cybercriminals may exploit vulnerabilities in AI systems to steal customer data, including personal and bank account information.

One example of AI misuse in Indonesia is the case of a Bank Mandiri customer who lost IDR 128 million due to an account breach (Tempo, 2021). Fraudsters manipulate AI algorithms designed to detect fraud, making fraudulent transactions appear legitimate by altering transaction patterns to evade detection. Another case of AI misuse involves fictitious credit fraud or unauthorized changes to interest rates without the bank customer's knowledge. Perpetrators also employ algorithm engineering techniques to manipulate AI systems, gaining access to customer accounts by compromising security protocols (Mukhlis et al., 2024).

The modus operandi of such frauds often begins with phone calls or emails in which criminals impersonate bank representatives, requesting personal information from victims. These deceptive tactics highlight the need for stronger security measures and regulatory oversight to mitigate AI-related fraud risks in the banking sector.

The banking industry faces increasingly complex security risks, including threats from fraudulent activities (Lisaldy, Ismail, & Iryani, 2024). Various forms of fraud, such as identity theft, money laundering, and scams, pose significant risks to both banks and their customers (Jaeni & Astuti, 2024). While AI technology offers numerous advantages in fraud detection, certain vulnerabilities can be exploited by malicious actors. A critical concern that requires further analysis is how AI—originally designed to prevent fraud—can instead be manipulated by perpetrators to facilitate fraudulent activities. Key issues include adversarial attacks, overfitting and underfitting, data poisoning, and model inversion

attacks. This study aims to identify and analyze the potential misuse of AI in banking systems and provide recommendations for mitigating these risks.

Security vulnerabilities in AI technology can be exploited to commit fraud. These vulnerabilities often stem from weaknesses in algorithms, data integrity, and AI system implementation. Previous studies have highlighted adversarial attacks, in which manipulated inputs deceive AI models into making incorrect predictions. These altered inputs may appear normal to human observers but can cause AI models to fail in recognizing fraudulent patterns (Simanjuntak, Irmayani, & Nasution, 2024). In fraud detection, attackers may modify digital transaction data by adding noise or making subtle alterations to inputs (Suryawijaya, 2023), leading the AI model to misclassify fraudulent transactions as legitimate.

Criminal liability and fundamental banking principles—such as trust, transparency, and prudence—are essential for maintaining the integrity of the banking system and protecting customers from AI-related fraud. Additionally, discussions on information security, corporate crime prevention strategies, and legal ethics emphasize the importance of moral and ethical obligations in the use of AI within the banking sector.

Regulations governing AI and banking fraud are designed to ensure the safe, transparent, and responsible use of AI technology by financial institutions while preventing and addressing fraud-related risks. The Financial Services Authority (OJK) has issued POJK No. 11/2022 on the Implementation of Information Technology by Commercial Banks and POJK No. 21/2023 on Digital Services by Commercial Banks. These regulations mandate that banks must adopt information technology responsibly, ensuring fairness, transparency, and ethical compliance when implementing AI-driven digital services. For example, when AI replaces human-performed functions, banks must ensure responsible AI usage by adhering to ethical standards.

Moreover, banks must thoroughly understand AI's operational mechanisms to optimize its benefits while proactively mitigating potential risks. Law No. 10 of 1998, which amends Law No. 7 of 1992 on Banking, along with other Bank Indonesia regulations, requires banks to uphold customer trust by implementing robust internal control systems to detect and prevent fraud. The AI guidelines issued by OJK and Bank Indonesia promote the ethical and responsible use of AI, while the General Data Protection Regulation (GDPR) provides an international framework to protect personal data and prevent data breaches that could lead to fraud.

This research examines the misuse of AI in banking fraud and aims to provide a more comprehensive contribution to AI-based banking security. It focuses on criminal liability for AI-related crimes and strategies to mitigate the risk of technological misuse through a banking

principles approach. This study differs from previous research, such as the article by Lummatul Mahsya et al., which highlights that machine learning and deep learning are the most widely used fraud detection techniques among researchers, with credit card fraud being the most frequently studied subject (Mahsya et al., 2023).

Another relevant study on AI governance in Indonesia underscores the necessity of establishing a robust regulatory framework to manage the development, implementation, and ethical use of AI in the country (Lisaldy, Ismail, & Iryani, 2024). Similarly, research conducted by Rahmat Hidayat et al. explores the impact of AI on financial control, including its role in financial decision-making strategies, predictive analysis, and risk manipulation (Hidayat, Defitri, & Hilman, 2024). AI has been developed as a concept to mimic the human brain, enabling machines to perform tasks that typically require human intelligence (Soni, 2019).

Mardiana further examines cybersecurity measures, fraud detection systems, response strategies, and future research directions, with particular attention to the risks and negative implications associated with AI implementation (Hidayat, Defitri, & Hilman, 2024). Meanwhile, a study by Navleen Kaur identifies two fundamental aspects of AI: first, understanding human cognitive processes and second, replicating these processes through machine learning. AI in finance extends beyond chatbots and has significantly transformed various sectors, including banking (Kaur et al., 2020).

A comparative analysis of this study with previous research on AI applications reveals that no prior studies have specifically addressed the issue of AI misuse in Indonesia's banking sector. Therefore, this research differs from earlier studies, presents a novel contribution, and is essential for addressing emerging challenges in AI-driven banking security.

B. RESEARCH METHODS

The research method employed in this study follows a normative juridical approach, focusing on the analysis of legal documents and literature. This study utilizes a case approach, a statutory approach, and a descriptive-analytical approach (Suhaimi, 2023) to identify and analyze the potential misuse of AI in banking systems and provide risk mitigation recommendations. These recommendations are based on statutory regulations, the theory of criminal liability, and policy documents related to AI implementation in the banking sector. Data collection techniques involve a literature review to obtain primary legal materials, such as laws and regulations, as well as secondary legal materials, including legal journals, books, and scientific articles.

C. RESULTS AND DISCUSSION

Banking fraud refers to any form of deception conducted by exploiting the banking system for personal gain at the expense of others (Hijriani et al., 2022). This type of fraud includes activities such as embezzlement, identity theft, data manipulation, and unauthorized access to

customer accounts (Hijriani, Niasa, & Dewi, 2023). The advancement of information technology has influenced the evolution of criminal modus operandi, enabling crimes to be committed without direct interaction between the perpetrator and the victim (Tantimin, 2021).

This study focuses on the role of Artificial Intelligence (AI) in the development of information technology. While AI has the potential to enhance the efficiency of banking processes, it also poses significant risks, particularly regarding its potential misuse in banking fraud. With advanced data analysis capabilities and process automation, AI can optimize services and accelerate transaction processing. However, these same features can also be exploited by malicious actors to commit fraud, including identity manipulation, system hacking, and increasingly sophisticated phishing attacks that are more difficult to detect. Furthermore, the use of inadequately regulated AI algorithms may introduce vulnerabilities in banking security systems, allowing attackers to exploit weaknesses and carry out financial crimes with greater efficiency (Mayana et al., 2024).

1. The Potential Misuse of AI in Banking Fraud

In recent years, artificial intelligence (AI) has gained significant attention in the industrial sector due to its ability to provide efficient solutions. The financial industry has also adopted AI as a key component of future banking innovations.

The integration of AI technology in the banking sector represents an innovative approach to enhancing transaction efficiency and security. However, despite its numerous advantages, AI also presents risks of misuse that could result in substantial financial losses. According to a report by McKinsey & Company, approximately 25% of all online banking transactions are potentially vulnerable to fraud (Raharjo, 2021). While AI's ability to process vast amounts of data and identify patterns allows it to detect suspicious transactions, cybercriminals can also exploit this technology to develop more sophisticated and harder-to-detect fraudulent schemes.

Several types of AI present significant risks in their application, including:

a. Machine Learning

Machine learning (ML) is a technology that enables computers to learn from data and make predictions or decisions based on experience without requiring explicit programming (Erawati, Ardiani, & Santiago, 2024). By utilizing algorithms and statistical models, computers can recognize patterns and generate predictions based on previously analyzed data.

Facial recognition is one of the most widely used applications of machine learning. This technology can identify and verify human faces from images or videos. For instance, facial recognition is implemented in security systems to grant access to authorized individuals. Social media platforms, such as Facebook, also utilize facial recognition to automatically tag people in photos.

Machine learning in banking offers several

advantages, such as: 1) More effective fraud detection by analyzing large volumes of transactions in real-time (Anas & Zakir, 2024), as demonstrated by Bank of America, which uses machine learning algorithms to analyze millions of transactions daily (Gifari, 2020). The system can detect suspicious transaction patterns, such as numerous small transactions conducted in a short time across different locations. If anomalies are detected, the system immediately alerts the security team to take necessary actions; 2) Enhanced detection accuracy, as implemented by JP Morgan Chase using machine learning to improve credit card fraud detection (Ngamal & Perajaka, 2022). Their algorithm learns the normal purchasing patterns of each customer and can recognize unusual transactions, such as large purchases in a country rarely visited by the customer, reducing the number of undetected fraudulent transactions; 3) Automated transaction monitoring at HSBC through machine learning solutions (Setiyono, Sriyono, & Prapanca, 2021), reducing manual intervention and speeding up the response time to potential fraud, enabling quicker customer contact in case of suspicious activity on their accounts; 4) Behavioral data analysis by Behavioural Sciences (BBVA), using machine learning to analyze customer behavior, such as shopping habits and banking service usage patterns. With this information, BBVA can offer more tailored products, such as credit or investment offers customized to the customer's risk profile and preferences (Setiyono, Sriyono, & Prapanca, 2021); 5) Credit risk assessment at Wells Fargo, where machine learning is used to evaluate the credit risk of prospective customers (Alavi, 2016). Their algorithm analyzes transaction data, credit history, and various other factors to provide more accurate risk assessments, reducing default rates and increasing bank profitability.

However, the use of ML also poses threats, such as: First, Model manipulation by fraudsters. Fraudsters may try to "train" the machine learning model by making small, seemingly normal transactions to build a non-suspicious pattern (Bashayreh, Tabbara & Sibai, 2023). For example, a fraudster may make small purchases at different stores to avoid detection before conducting a larger fraudulent transaction. Second, Data quality and bias issues (Nouri, Salah, & AlOmran, 2024). If the data used to train a machine learning model in a bank is incomplete or biased (e.g., not covering all types of transactions or customer profiles), the model may not detect fraud effectively. This could lead to false positives (legitimate transactions flagged as fraudulent) or false negatives (fraudulent transactions not detected) (Syailendra, Lie, & Sudiro, 2024). Three, Dependence on technology vulnerable to cyber-attacks. Banks that rely too heavily on machine learning technology may be vulnerable if their systems are disrupted or hacked. For example, if a bank's fraud detection system is hacked and the algorithm is altered, fraudsters could conduct transactions undetected. Four, Access to personal customer data. Implementing machine learning requires access to customer personal

data, such as transaction history and identity information (Al Amaren, Md. Ismail, & Md. Nor, 2021). If this data is not well-protected, data breaches could occur, as happened to Capital One in 2019 (Kartini et al., 2023), where the personal information of over 100 million customers was leaked due to a cyber-attack. Five, Significant investment in infrastructure and human resources. Implementing machine learning in a large bank like Citibank requires substantial investment in infrastructure and human resources (Mulyani, Maryam & Le, 2023). Additionally, developing and maintaining an effective machine learning model requires experts and complex processes, which can be a challenge for smaller banks or those with limited resources.

b. Big Data Analysis

Big Data refers to vast volumes of data characterized by high update rates and diverse formats, including numerical data, text, images, and videos. With Big Data technology, data processing is no longer limited to samples, as the entire data population can be analyzed. This eliminates the need for an initial hypothesis, as observing all available data allows researchers to directly identify patterns and understand the phenomena under investigation (Muchlis, 2023).

Big Data analytics plays a crucial role in credit risk evaluation within the banking industry. This technology enables credit analysts to access and process large and complex datasets, allowing them to identify relevant patterns and trends for more accurate credit assessments (Makarim, 2013).

In-depth knowledge of Big Data and Artificial Intelligence (AI) is becoming increasingly essential for credit analysts (Muhammad, 2021). Analysts must understand how these technologies can enhance the accuracy of credit assessments while also identifying potential opportunities and risks associated with credit. The growing demand for more sophisticated credit risk analysis underscores the need for professionals who can integrate data-driven insights and advanced technology into decision-making processes (Khalil & Raj, 2023).

The use of Big Data analysis in banking offers several advantages, including (Radetzky, 2024):

a) Improved decision-making through predictive analysis.
b) Increased operational efficiency with process automation.
c) More accurate fraud detection and prevention.
d) Enhanced customer experience through more personalized services.
e) Better risk management.

However, there are also several threats, including: privacy and data security risks; vulnerability to cyber-attacks; complexity in implementation and maintenance; challenges in data analysis and interpretation, which, if not done correctly, may lead to incorrect conclusions that could affect business decisions; and dependence on data, which may overlook human factors and intuition in decision-making (Anugerah & Indriani, 2018).

c. Data Manipulation and Automated Attacks

The use of AI technology in banking can bring significant benefits, such as speeding up and increasing the efficiency of big data analysis, detecting anomalies that may indicate fraud, and better assessing risk. For example, banks can monitor transactions in real-time and identify suspicious activities that could lead to fraud. This is closely related to the fundamental principle in banking operations, which is the principle of prudence (Fitri, 2021). However, AI also has its weaknesses. If it falls into the wrong hands, it could be used to hack systems and steal sensitive information, leading to significant losses. One example is hackers using AI to carry out automated attacks on banking systems, identifying security gaps and stealing customer data. Additionally, the implementation of AI requires substantial investment in infrastructure, expertise, and ongoing maintenance (Dharmawan et al., 2023).

d. Phishing

Phishing is a form of cybercrime that uses social engineering techniques. The term for a phishing perpetrator is "phisher." Phishers aim to obtain sensitive information, such as usernames, passwords, and credit card details, with the goal of stealing this information for unauthorized use (Permana & Jamaludin, 2023).

Phishing involves requesting personal information from device users in order to misuse the victim's data, such as passwords, credit card numbers, and other sensitive details. Phishing takes various forms, including fake emails impersonating banks or email services, messages tailored specifically to individuals or organizations (spear phishing), fake phone calls (voice phishing), SMS messages with fraudulent links, redirection to fake websites through malware (pharming), and the use of social media to deceive victims. Fake applications can also be used in phishing schemes (Jaelani et al., 2024).

In phishing practices, perpetrators often impersonate reputable institutions, including banks (Erdiyanto, 2023). Online fraud that claims to be from a bank is often carried out by sending notification letters about transaction fee increases through personal mobile phone numbers to potential victims. The letter directs the victims to open a link leading to a website designed to resemble a legitimate bank's website. After accessing the link, victims are prompted to fill in personal data, such as ATM card numbers, card expiration dates, Card Verification Value (CVV), Personal Identification Numbers (PIN), access codes, or One-Time Passwords (OTP). If the victim enters the data completely, the fraudster can take over the victim's account and transfer funds.

Phishing becomes more sophisticated with the help of AI, enabling fraudsters to create highly personalized and convincing messages that are difficult to detect. Phishing attacks are a major risk in the banking sector, often resulting in significant financial losses. For example, in "Business Email Compromise" (BEC) attacks, fraudsters can use AI to create fake emails that closely resemble those of top bank officials,

tricking employees into transferring large sums of money to fraudulent accounts.

AI can also be used to create realistic and convincing fake identities, which can then be exploited to open bank accounts and commit large-scale financial fraud. Fraudsters may use these fake identities to conduct illegal fund transfers and money laundering activities. On the other hand, banks can leverage AI technology to better detect and verify identities, reducing the risk of fake accounts. However, traditional methods may not be sufficiently effective in detecting AI-generated fake identities, making it necessary to implement more advanced technology to counter this threat.

For instance, credit card fraud cases in Indonesia rank second-lowest compared to other countries in the Asia Pacific region. Meanwhile, according to data from Visa, Indonesia's fraud ranking is the third-lowest among Southeast Asian countries (Alhakim & Sofia, 2021). Kroll and ACFE Indonesia indicate that approximately 80% of organizations in Indonesia have fallen victim to fraud, with 39% reporting an increase in fraud incidents during the pandemic. Additionally, the survey found that the majority of fraud incidents were detected through whistleblower programs (62%) or internal audits (52%) (Tama, 2022). The most common credit card crimes are identity theft and Card Not Present (CNP) transactions. In identity theft cases, there were 402 incidents, each valued at approximately Rp 1.14 billion (Benuf, Mahmudah, & Priyono, 2019), while in CNP cases, there were 458 incidents valued at approximately Rp 545 million (Afqal, 2023).

e. The Use of Algorithms to Create Deepfakes

A concrete example of AI misuse in the context of banking fraud is the use of algorithms to create deepfakes. This technology enables perpetrators to produce highly realistic fake videos or audio that can be used to deceive customers or even bank officials. A study by Stanford University found that 99% of AI-generated deepfakes can evade human detection (Using AI to Detect Seemingly Perfect Deep-Fake Videos). This indicates that while banks may use AI technology to prevent fraud, perpetrators can also exploit the same technology to commit crimes.

Compared to conventional methods, where fraud detection relies on manual analysis and simpler alert systems, the use of AI offers greater speed and accuracy. However, this advancement also presents new challenges. For instance, the algorithms used to detect fraud can be biased, leading to false positives, where legitimate transactions are flagged as suspicious.

The comparison between the use of AI and conventional methods highlights that while AI provides a more efficient solution, the risk of misuse persists. Perpetrators can employ sophisticated techniques to exploit vulnerabilities in AI systems, while banks must continually update and enhance their algorithms to stay ahead of potential threats. Therefore, it is crucial for financial institutions to develop comprehensive security policies that combine AI technology with

human oversight in detecting and preventing fraud.

Collaboration between banking institutions and AI technology providers is essential. Banks need to invest in training and developing human resources to effectively understand and manage AI technology. Additionally, strict regulations are necessary to ensure that this technology is not misused. With the right approach, the potential for AI misuse in banking fraud can be minimized, allowing banks to fully leverage the benefits of this technology.

2. Criminal Liability for AI-related Crimes

In the current digital era, the use of Artificial Intelligence (AI) technology in the banking sector has expanded rapidly. However, with this development comes the potential for misuse, which can lead to criminal activities, including banking fraud. As a result, criminal liability for individuals who use AI to commit crimes has become a critical issue.

A concrete example of AI misuse in banking fraud involves the use of algorithms to create fake identities. Cybercriminals apply machine learning techniques to collect and analyze personal data, which can then be used to gain unauthorized access to bank accounts. Deloitte predicts that losses due to AI-driven fraud could reach $40 billion in the US by 2027 (Yamin et al., 2024). Additionally, Visa successfully prevented $40 billion in fraudulent transactions worldwide in 2023 with the help of AI technology (Permana & Jamaludin, 2023).

Given the significant impact of fraud, structured efforts are necessary to strengthen the enforcement of fraud prevention measures (Akbar, 2020). In today's digital era, criminal liability for those who exploit AI technology to commit fraud is becoming increasingly pertinent. When perpetrators use AI to carry out banking fraud, the question arises: who should be held accountable? Should it be the human perpetrator, the technology developer, or even the financial institution that may have failed to implement adequate security systems? According to a report by the World Economic Forum, 80% of executives believe current laws are inadequate to address crimes involving new technologies like AI (PwC, 2024).

From a legal perspective, criminal liability for perpetrators who exploit AI is complex due to the difficulty in identifying who is actually responsible. A study by Rina Shahriyani et al. indicates that the handling of cybercrimes in Indonesia faces many challenges compared to countries like the United States. Factors affecting the effectiveness of handling cybercrimes include insufficiently detailed legislation, with many existing regulations failing to specifically address the evolving forms of cybercrime. This makes law enforcement difficult due to a lack of clear legal grounds. Additionally, law enforcement agencies in Indonesia often lack the necessary resources, including digital forensic experts and technology needed to investigate and prove cybercrimes. The lack of coordination between agencies, such as the police, prosecutors, and other government

institutions, also hinders the law enforcement process. Moreover, low public awareness of the risks and impacts of cybercrimes often leads to underreporting of incidents or failure to take necessary preventive measures, posing a significant challenge in law enforcement against perpetrators using advanced technology. Other obstacles include the difficulty in tracking perpetrators, lack of strong digital evidence, and issues related to international jurisdiction (Shahrullah & Kiweikhang, 2014).

One of the main challenges in establishing criminal liability is the complexity of the technology itself. For instance, when AI algorithms are used to commit fraud, it is difficult to determine whether the fault lies with the user, the developer, or the system itself. The legal system in Indonesia currently lacks regulations that clearly address legal protection for victims who suffer losses due to erroneous output produced by AI. Liability for damages can only be imposed on legal subjects, such as individuals and legal entities, which are capable of having rights and obligations. This creates problems when autonomous, human-like technologies, such as AI, cause harm. AI is considered to have autonomous characteristics because it can operate independently without human intervention, especially since AI involves many parties such as programmers, data analysts, and users. Holding AI directly accountable is not feasible, as it would fundamentally alter the legal concept of liability (Simbolon, 2023).

Artificial Intelligence cannot be considered a legal subject. Although AI can solve various problems through knowledge input by humans, the human role remains crucial to the success of AI. AI systems require a complex knowledge base, which can be obtained from experts, literature, or databases, along with an inference engine capable of drawing conclusions based on that knowledge. However, AI cannot act beyond what has been programmed by humans, which makes AI's autonomous nature inherently biased, as it cannot operate beyond predefined instructions. This highlights the need for clear regulations to govern legal responsibility for all parties involved.

Furthermore, many countries still lack specific legal frameworks to address cybercrimes involving AI. In Indonesia, for instance, Law Number 1 of 2024, concerning the Second Amendment to Law Number 11 of 2008 on Information and Electronic Transactions (ITE Law), provides a legal basis for handling cybercrimes. However, it does not specifically regulate crimes involving AI in banking fraud, thus creating a legal loophole that criminals can exploit. Therefore, the government should update and strengthen existing regulations to keep pace with technological advancements.

Regulations related to AI can be found in various laws, including Law No. 19 of 2016 on Information and Electronic Transactions (ITE Law), Law No. 1 of 2023 on the National Criminal Code (KUHP Nasional), and Law No. 27 of 2023 on Personal Data Protection (PDP Law).

The Electronic Information and Transactions Law (UU ITE), first enacted in 2008 and amended most recently by Law No. 19 of 2016, regulates various aspects of electronic transactions and the use of information technology. Although it does not specifically regulate AI, several provisions in the Electronic Information and Transactions Law (UU ITE) can be applied in the context of AI use. Article 27 (which addresses the prohibition of negative content) regulates the dissemination of illegal electronic information, including content generated by AI systems, such as content containing defamation, pornography, or hate speech. Article 28 (regarding defamation) governs insults or defamation through electronic media, which can be carried out using AI, such as through chatbots or social media. Articles 32–34 (regarding the operation of electronic systems) require operators of electronic systems to be responsible for the services they provide, including when AI systems are used in those services.

The National Criminal Code (KUHP), although it does not directly regulate technology or AI, includes provisions that can be applied to unlawful uses of AI. For example, Article 27 of the ITE Law related to defamation can be combined with provisions in the National Criminal Code that regulate insults or defamation, such as Article 310 of the National Criminal Code. Article 378 of the National Criminal Code (Fraud) stipulates that if AI is used to commit fraud through electronic transactions or misleading communication, the person operating or utilizing AI for such purposes can be charged under this article. Additionally, Article 282 of the National Criminal Code (Pornography) states that if AI is used to create or disseminate pornographic content, the perpetrator can be subject to criminal penalties under this article.

The Personal Data Protection Law (Law No. 27 of 2023), which will come into effect in 2024, specifically regulates the collection, use, and processing of personal data in Indonesia. AI, which often involves the collection and analysis of large datasets, including personal data, is highly relevant in this context. Several key provisions in the PDP Law pertain to AI.

Article 15 (Collection of Personal Data) states that the collection of personal data must be done with the clear consent of the individual, and AI that processes personal data must adhere to this principle. Article 17 (Processing of Personal Data) mandates that any processing of personal data, including that conducted by AI-based systems, must have a legitimate purpose, be transparent, and be carried out with prudence. Article 25 (Security of Personal Data) emphasizes that the use of AI involving the processing of personal data must consider data security aspects to prevent data breaches or misuse of personal data. Articles 42–46 (Rights of Data Subjects) grant individuals the right to access, correct, and delete their personal data that may be processed by AI-based systems.

In general, AI is closely related to issues of personal data and privacy, so any use or

development of AI technology involving personal data must comply with the provisions in the Personal Data Protection Law (UU PDP). Legal challenges and the need for further regulation are essential to address the rapid advancements in AI technology. While several relevant legal provisions exist, regulations related to AI in Indonesia still need to be updated or expanded to address the fast-paced developments in this field. Some areas requiring further regulation include: legal responsibility for AI developers or operators who cause harm or violations; ethics and transparency in AI algorithms, such as the obligation to disclose algorithms used for automated decision-making; and regulation of AI for public interest purposes, such as in health, education, or government, which must adhere to strict standards regarding security and privacy.

Overall, while the ITE Law, the Criminal Code, and the PDP Law already cover several aspects relevant to AI, further development of more specific regulations is needed to address emerging issues with the adoption of AI technology in Indonesia.

One example of a fraud case involving AI at a major European bank is the Wirecard scandal in Germany. Wirecard employed a complex accounting fraud scheme to inflate its revenues and profits, resulting in billions of dollars in losses for investors (Shamaya et al., 2023). Although the perpetrators were eventually apprehended, the lengthy and complicated legal process revealed that the current legal system is ill-equipped to handle crimes involving advanced technology. This underscores the need for collaboration among law enforcement agencies, technology developers, and financial institutions to create a more effective legal framework.

With the increasing use of AI in various aspects of life, it is necessary to develop a holistic approach to addressing criminal liability. This includes training law enforcement to understand AI technology and its impact on crime, as well as developing regulations that are more adaptable to technological changes, thereby creating a better system for handling AI-related crimes and protecting society from the potential risks they pose.

3. Risk Mitigation of Technology Misuse

Implementing advanced AI technology for fraud detection and prevention is essential. In today's digital era, where financial transactions are becoming increasingly complex and rapid, banks must adapt to the latest technology to protect their assets and customers. AI-based systems can analyze transaction patterns in real time and detect suspicious anomalies more efficiently than traditional methods. A study by Deloitte showed that the use of AI in fraud detection could reduce the time needed to identify fraud by up to 80% (Gokhale et al., 2019). This highlights that investing in the right technology is crucial for risk mitigation, while also providing banks with a competitive edge in an increasingly competitive market.

Mitigating the risks of AI technology misuse in banking fraud requires a comprehensive and ongoing approach. One fundamental principle that

must be applied is transparency. Financial institutions must ensure that the algorithms used in their systems are understandable and auditable. This is essential to help customers feel secure and confident that decisions made by AI systems are not arbitrary. A study by Accenture showed that 70% of consumers trust banks more when they are transparent about their use of AI technology. By conducting regular internal and external audits, banks can ensure that AI usage in banking is not being misused. Additionally, implementing monitoring systems that can detect and prevent suspicious activities will further strengthen customer trust in financial institutions.

In addition to transparency, applying the principle of accountability in the development and implementation of AI technology is crucial. Every financial institution must have clear policies regarding who is responsible for decisions made by AI systems. For instance, if a credit decision is rejected by an AI algorithm, the bank must have a mechanism to explain the reasons for the rejection to the customer. This is important not only for customer satisfaction but also to ensure that AI systems do not operate in a discriminatory manner. Data protection laws in many countries can serve as an important reference to ensure that decisions made by AI do not infringe on individuals' rights.

A key banking principle, particularly the principle of prudence, involves the implementation of stricter regulations related to the use of AI technology. Financial regulatory authorities in various countries are developing regulatory frameworks governing the use of AI in the banking sector. For example, the European Banking Authority (EBA) has issued guidelines requiring banks to conduct comprehensive risk assessments before implementing AI technology (European Banking Authority, 2024). These regulations are designed to protect customers and ensure that the technology used does not result in harm or misuse. Moreover, strict regulations can encourage banks to be more responsible in their use of AI technology, creating a safer environment for all parties involved.

Education and training for employees are also critical aspects of risk mitigation. Banks need to educate both employees and customers about the risks associated with AI misuse and conduct regular cybersecurity training. Employees who understand how AI technology works and its potential risks will be better equipped to identify and address any issues that may arise. According to research by Deloitte, 65% of employees trained in AI technology feel more confident in identifying potential fraud (Permana & Jamaludin, 2023). Therefore, investing in human resource training should be a priority for financial institutions. This not only enhances employee capabilities but also helps foster a culture of security awareness within the organization.

Furthermore, collaboration between financial institutions, governments, and technology providers is essential. By sharing information and experiences, all parties can work together to develop better solutions for preventing the misuse of AI technology. For example, several

banks in Europe have formed alliances to share data and best practices in detecting and preventing AI-related fraud. This collaborative approach can help create a safer ecosystem for all parties involved and can also support the development of more effective policies and regulations on the use of AI technology in the banking sector.

Proper regulation is also necessary to govern the use of AI technology in the banking sector. Governments should work with financial institutions to develop regulatory frameworks that can address the challenges posed by new technologies. With clear regulations in place, a safer and more secure environment for customers can be created. Additionally, effective regulation can reduce the risk of AI technology misuse in banking fraud and ensure that financial institutions adhere to high ethical and professional standards. In this context, it is crucial for financial institutions to collaborate with authorities to ensure that AI-based banking systems are safe and beneficial for all parties involved.

The matrix below outlines several risk mitigation steps that banks can take:

Table 1. Risk Mitigation Matrix

No.	Mitigation Step	Description
1	Employee Training	Increasing awareness of AI fraud risks
2	Use of AI Technology	Implementing AI-based fraud detection systems
3	Regulatory Compliance	Adhering to applicable guidelines and regulations
4	Audit and Evaluation	Conducting regular audits of the AI systems in use
5	Collaboration with Third Parties	Collaborating with security technology providers

Source: (Vicente, 2024)

Thus, the implementation of AI technology in the detection and prevention of banking fraud involves not only the technology itself but also aspects such as transparency, accountability, education, collaboration, and regulation. Updating procedural law, particularly the burden of proof in determining which legal entity is responsible and subject to criminal sanctions, will be a challenge in addressing crimes involving AI in the banking sector. Modifying regulations related to the burden of proof and applying banking principles to minimize the risk of AI-based fraud are essential for combating such crimes in Indonesia.

All of these elements are interconnected and contribute to the creation of a safer and more reliable banking system. Therefore, it is important for financial institutions to continue investing in the right technology and developing policies that support the ethical and responsible use of AI. With a comprehensive and sustainable approach, it is expected that the risk of fraud will be reduced, and customer trust in financial institutions will be enhanced in the digital age.

D. CONCLUSION

The results of this study reveal security vulnerabilities in AI algorithms within the banking sector, highlighting that the implementation of AI in this sector can be exploited for fraudulent purposes. Therefore, there is a need to update procedural law, particularly the system of proof, to determine which legal entity is responsible for

criminal liability. The conclusion of this study emphasizes the importance of adjusting regulations related to the system of proof and applying banking principles to minimize the risk of AI-based fraud.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the Directorate of Research, Technology, and Community Service (DRTPM) of the Directorate General of Higher Education, Research, and Technology (Ditjen Diktiristek), Ministry of Education, Culture, Research, and Technology (Kemendikbudristek) for funding this research program under the Fundamental Research – Regular scheme. We also extend our appreciation to the Rector of Southeast Sulawesi University and his staff, as well as the research team, for their assistance and support in the completion of this research and the resulting article.

REFERENCES

JOURNALS

Afqal, Reva G. (2023). Analisis Deteksi dan Pencegahan Penipuan Kartu Kredit Menggunakan Teknik Data Mining dan Machine Learning. *Prosiding Seminar Kecerdasan Artifisial, Sains Data, Dan Pendidikan Masa Depan*, Vol.1, (No.1), pp.322–325. https://openjournal.unpam.ac.id/index.php/PROKASDADIK/article/view/40641

Akbar, Mohammad A. (2020). Mencegah Fraud di dalam Industri Perbankan. *Scientific Journal of Reflection: Economic, Accounting, Management and Business*, Vol.3,(No.1),pp.61–70. DOI: 10.37481/sjr.v3i1.126

Al Amaren, Emad Mohammad., Md. Ismail, Che Thalbi Bt., & Md. Nor, Mohd Zakhiri bin. (2021) The Fraud Rules In The Letter Of Credit Under Jordanian Legal System. *Sriwijaya Law Review,*Vol.5,(No.2),pp.218-235. http://dx.doi.org/10.28946/slrev.Vol5.Iss2.1058.pp218-235

Alavi, H. (2016). Comparative Study of Issuing Bank's Obligations towards Beneficiary of the Letter of Credit under UCP and English Law. *Hasanudin Law Review*, Vol.2, (No.3), pp.289-311. http://dx.doi.org/10.20956/halrev.v2i3.259

Alhakim, Abdurrakhman., & Sofia, Sofia. (2021). Kajian Normatif Penanganan Cyber Crime di Sektor Perbankan di Indonesia. *Jurnal Komunitas Yustisia*, Vol.4, (No.2), pp.377–385.https://doi.org/10.23887/jatayu.v4i2.38089.

Anas, Iqbal., & Zakir, Supratman. (2024). Artificial Intelligence: Solusi Pembelajaran Era Digital 5.0. *J-SAKTI; Jurnal Sains Komputer dan Informatika*, Vol.8, (No.1), pp.35-46. http://dx.doi.org/10.30645/j-sakti.v8i1. 764

Anugerah, Dian Purnama., & Indriani, Masitoh. (2018). Data Protection In Financial Technology Services (A Study In

Indonesian Legal Perspective). *Sriwijaya Law Review*, Vol.2, (No.1), pp.82-92. http://dx.doi.org/10.28946/slrev.Vol2.Iss1.112.pp82-92.

Bashayreh, Mohammad H., Tabbara, Amer., & Sibai, Fadi N. (2023). The Need For A Legal Standard Of Care In The Ai Environment. *Sriwijaya Law Review,* Vol.7*,* (No.1),pp.73-86. http://dx.doi.org/10.28946/slrev.Vol7.Iss1.1507.pp73-86.

Benuf, Kornelius., Mahmudah, Siti., & Priyono, Ery Agus. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology di Indonesia. *Refleksi Hukum,*Vol.3,(No.2),pp.145-160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Dharmawan, Ni Ketut Supasti., Kasih, Desak Putu Dewi., Samsithawrati, Putu Aras., Dwijayanthi, Putri Triari., Salain, Made Suksma Prijandhini Devi., Mahaswari, Mirah., Ustriyana, Made Grazia., & Moisa, Robert Vaisile. (2023). Quo Vadis Traditional Cultural Expressions Protection: Threats from Personal Intellectual Property and Artificial Intelligence. *Law Reform*, Vol.19,(No.2),pp.321-343. https://doi.org/10.14710/lr.v19i2.58639

Erawati, Kadek Nonik., Ardiani, Ni Nengah Dita., & Santiago, Gede Agus. (2024). E-Module Interaktif Berbasis Flipbook pada Mata kuliah Machine Learning Untuk Meningkatkan Kreativitas Mahasiswa. *Jurnal Penjaminan Mutu*, Vol.10, (No.1), pp.45-51. https://doi.org/10.25078/jpm.v10i01.3603

Erdiyanto, Rizqy P. (2023). Penipuan Mengatas namakan Bank Berbentuk Phising. *Jurnal Inovasi Global*, Vol.1, (No.2), pp.71–79. https://doi.org/10.58344/jig.v1i2.11

Fitri, W. (2021). Sharia Compliance in Micro Waqf Bank Business Activities: A Study of Protection of Consumer's Spiritual Rights. *Law Reform*, Vol.17, (No.1), pp. 107-120, https://doi.org/10.14710/lr.v17i1.37556.

Hanila, Siti., & Alghaffaru, Muhammad Afif. (2023). Pelatihan Penggunaan Artificial Intelligence (AI) Terhadap Perkembangan Teknologi Pada Pembelajaran Siswa Sma 10 Sukarami Kota Bengkulu. *Jurnal Dehasen Mengabdi,*Vol.2,(No.2),pp.221-226. https://doi.org/10.37676/jdm.v2i2.4890

Hassan, Moahammad., Aziz, Layla Abdel-Rahman., & Andriansyah, Yuli. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. *Reviews of Contemporary Business Analytics*, Vol.6, (No.1),pp.110-132. https://researchberg.com/index.php/rcba/article/view/153

Hidayat, Muhammad., Defitri, Siska Yulia., & Hilman, Haim. (2024). The Impact of Artificial Intelligence (AI) on Financial Management. *Management Studies and*

Business Journal, Vol.1, (No.1), pp.123-129. https://doi.org/10.62207/s298rx18

Hijriani, Hijriani., Borahima, Anwar., Irwansyah, Irwansyah., & Haeranah, Haeranah. (2022). Legal Certainty Against Banking Fraud Criminal Liability. *Baltic Journal of Law & Politics*,Vol.15,(No.7),pp.1361–1366. https://versita.com/menuscript/index.php/Versita/article/view/1265

Hijriani, Hijriani., Niasa, La., & Dewi, Ayu Lestari. (2023). Restorative Justice Approach to The Settlement of Banking Crime Cases. *Substantif Justice International Journal of Law*,Vol.12,(No.2),pp.1005-1010. https://doi.org/10.56087/substantivejustice.v6i1.206

Jaelani, Abdul Kadir,. Luthviati, Resti Dian, Siboy, Ahmad., Fatih, Sholahuddin Al., & Hayat, Muhammad Jihadul. (2024). Artificial Intelligence Policy in Promoting Indonesian Tourism. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, Vol.7, (No.1), pp.109–137. https://doi.org/10.24090/volksgeist.v7i1.10623

Jaeni, Ahmad., & Astuti, Tri Maryani Kusuma. (2024). Analisa Yuridis Fraud Sebagai Kejahatan dalam Asuransi Kesehatan Komersial Menurut Perspektif Perlindungan Para Pihak, Jurnal Syntax Imperatif: Jurnal Ilmu Pendidikan dan Sosial, Vol.5, (No.5), pp.1045-1056.https://doi.org/10.36418/syntaximperatif.v5i5.517

Kartini, Yati., Shodiqin, Muhammad., Veranita, Veranita., Susilawati, Susi., Sanusi, Muhammad., & Zahara, Anzu Elvia. (2023). Perbandingan Tingkat Literasi Perbankan Syariah dan Konvensional. *Innovative: Journal of Social Science Research*,Vol.3, (No.2),pp.14297–14312.https://j-innovative.org/index.php/ Innovative/article/view/2055

Kaur, Navleen., Sahdev, Supriya Lamba., Sharma, Monika., & Siddiqui, Laraibe. (2020). Banking 4.0: The Influence of Artificial Intelligence on the Banking Industry & How AI is Changing the Face of Modern Day Banks. *International Journal of Management*,Vol.11,(No.6),pp.577-585. DOI:10.34218/IJM.11.6.2020.049

Khalil, Ahmad., & Raj, S. Anandha Khisna. Assessing the Legality of Autonomous Weapon Systems: An In-depth Examination of International Humanitarian Law Principles. *Law Reform*, Vol.19, (No.2), pp.372-392, https://doi.org/10.14710/lr.v19i2.58497

Kurniawan, Ketut Adi., Sastra, N Putra., & Sudarma, M. (2020). Analisis Performansi dan Efisiensi Cloud Computing Pada Sistem Perbankan. *Majalah Ilmiah Teknologi Elektro*, Vol.19, (No.1), pp.11-18. https://ojs.unud.ac.id/index.php/mite/article/view/53917

Lee, J. (2020). Access to Finance for Artificial Intelligence Regulation in The Financial Services Industry. *European Business Organization Law Review,* Vol.21, (No.4), pp.731-757. https://doi.org/10.1007/s40804-020-00200-0

Lisaldy, Ferdinand., Ismail, Ismail., & Iryani, Dewi. (2024). Lex AI: Solution for Governance of Artificial Intelligence in Indonesia. *DIH: Jurnal Ilmu Hukum,* Vol.20,(No.1),pp.50-67. https://doi.org/10.30996/dih.v20i1.9632

Mahya, Lummatul., Tarjo, Tarjo., Sanusi, Zuraidah Mohd., & Kurniawan, Fitri Ahmad. (2023). Intelligent Automation of Fraud Detection and Investigation: a Bibliometric Analysis Approach. *Jurnal Reviu Akuntansi Dan Keuangan*, Vol.13, (No.3), pp.588-613. https://doi.org/10.22219/jrak.v13i3.28487

Makarim, E. (2013). Hybrid Paradigm From European And America Concerning Privacy And Personal Data Protection In Indonesia. *Indonesia Law Review,* Vol.3, (No.2),pp.101-114. DOI:10.15742/ilrev.v3n2.31

Mayana, Ranti Fauza., Santika, Tisni., Win, Yin Yin., Matalam, Jamil Andrian Khlil., & Ramli, Ahmad M. (2024). Legal Issues of Artificial Intelligence – Generated Works: Challenges on Indonesian Copyright Law. *Law Reform*, Vol.20, (No.1), pp.54-75. https://doi.org/10.14710/lr.v20i1.61262

Muchlis, M. (2023). Financial Performance: Big Data & Sustainabiity Competitive Advantage Studi Kasus Institusi Keuangan di Indonesia. *Sustainable Jurnal Akuntansi*, Vol.3,(No.2),pp.282–300. DOI:10.30651/stb.v3i2.20886

Muhammad, R. (2021). Analysis of Credit Risk, Intellectual Capital and Financial Performance of Listed Deposit Money Banks in Nigeria. *Account and Financial Management Journal*, Vol.6, (No.12), pp.2578-2591. https://doi.org/10.47191/afmj/v6i12.01

Mulyani, Sri., Mariyam, Siti & Le, Hieu Hong Trung. (2023). Legal Construction of Crypto Assets as Objects of Fiduciary Collateral. *Law Reform,* Vol.19, (No.1), pp.25-39. https://doi.org/10.14710/lr.v19i1.52697.

Ngamal, Yohanes., & Perajaka, Maximus Ali. (2022). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, Vol.2, (No.2), pp.59-74. https://doi.org/10.33541/mr.v2iIV.4099

Nouri, Zouhaier., Salah, Walid Ben., AlOmran, Nayel. (2024). Artificial Intelligence and Administrative Justice: An Analysis of Predictive Justice in France. *Hasanudin Law Review*, Vol.10, (No.2), pp.119-143. http://dx.doi.org/10.20956/halrev.v10i2.5541

Permana, Flea Akbar., & Jamaludin, Ahmad. (2023). Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phishing Crimes. *Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum Dan Filantropi,* Vol.5, (No.2), pp.201-216. https://doi.org/10.22515/jurnalalhakim.v5i2.7074.

Radetzky, Michael A. (2024). The Impact of Artificial Technology on Authors of a Cinematographic Creation. *Hasanuddin Law Review,* Vol.10, (No.1), pp.21-42. http://dx.doi.org/10.20956/halrev.v10i1.4780

Shahrullah, Rina Shahriyani., & Kiweikhang, Delfind. (2014). Tinjauan Yuridis Penanganan Kejahatan Siber (Cybercrime) di Sektor Perbankan Indonesia dan Amerika. *Journal of Judicial Review*, Vol.16, (No.2),pp.115–132. https://doi.org/10.37253/jjr.v16i2.155

Shamaya, Varen Putri., Ashara, Sabrina Nova., Sofyan, Achmad., Aprilia, Salsabila., Leonica, Arswarani., & Ratnawati, Tri. (2023). Studi Literatur: Artificial Intelligence Dalam Audit. *JRIME; Jurnal Riset Manajemen Dan Ekonomi*, Vol.1, (No.3), pp.255–267. https://doi.org/10.54066/jrime-itb.v1i3.461

Simanjuntak, Ebrika Nadia., Irmayani, Deci., & Nasution, Fitri Aini. (2024). Tinjauan Penerapan Kecerdasan Buatan dalam Keamanan Jaringan Tantangan dan Prospek Masa Depan. *Jurnal Ilmu Komputer Dan Sistem Informasi*, Vol.7, (No.2),pp.370-375. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/3578

Simbolon, Y. (2023). Pertanggungjawaban Perdata Terhadap Artificial Intelligence Yang Menimbulkan Kerugian Menurut Hukum Di Indonesia. *Veritas et Justitia*, Vol.9,(No.1),pp.246–273. https://doi.org/10.25123/vej.v9i1.6037

Sinaga, Novica Handayani., Irmayani, Deci., & Hasibuan, Mila Nirmala Sari. (2024). Mengoptimalkan Keamanan Jaringan Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman. *Jurnal Ilmu Komputer Dan Sistem Informasi*,Vol.7,(No.2),pp.364-369. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/3582

Soni, Vishal D. (2019). Role of Artificial Intelligence in Combating Cyber Threats in Banking. *International Engineering Journal For Research & Development,* Vol.4, (No.1), pp.1-7. https://doi.org/10.17605/OSF.IO/JYPGX

Suhaimi, S. (2023). Problem Hukum Dan Pendekatan Dalam Penelitian Hukum Normatif. *Jurnal Yustisia*, Vol.19, (No.2), pp.202-210. DOI:10.53712/yustitia.v19i2.477

Suryawijaya, Tito Wira E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, Vol.2,(No.1),pp.55-68. https://doi.org/10.21787/jskp.2.2023.55-68

Syailendra, Moody Rizqy., Lie, Gunardi., & Sudiro, Ahmad (2024). Personal Data Protection Law In Indonesia: Challenges And Opportunities. *Indonesia Law Review*,

Vol.14.(No.2),pp.56-72. https://scholarhub.ui.ac.id/ilrev/vol14/iss2/4

Tantimin, T. (2021). Legal Liability of Minors as Perpetrators of Online Buying and Selling Fraud in Indonesia. *Law Reform*, Vol.17, (No.2),pp.145-156. https://doi.org/10.14710/lr.v17i2.41738

Yamin, Ahmad Fachri., Rachmawati, Annisa., Pratama, Rio Aditya., & Wijaya, Jonathan Kevin. (2024). Perlindungan Data Pribadi dalam Era Digital: Tantangan dan Solusi. *Meraja Journal,* Vol.7, (No.2), pp.138-155. https://doi.org/10.33080/mrj.v7i2.352.

BOOKS

Christia, Abdi., Hadi, Achmad Setyo., Febriana, Aderina., Budihardjo, Andreas., Wiradarmo, Aulia Ardista., Elfriede, Dwining Putri., Ardianto, Eka., Silva, Elizabeth Novira Da., Sari, Faizah., Kusumadewi, Fitriana Nurindah., Widjojo, Handyanto., Prasetya, Prita., Hariyanto, Sandy., Trilaksono, Teddy., & Wijantini, Wijantini. (2024). *Kecerdasan Buatan: Arah dan Eksplorasinya (Cet.1).* Jakarta: Prasetiya Mulya Publishing.

Mukhlis, Iqbal Ramadhani., Putra, Randi Farmana., Datya, Aulia Iefan., Pipin, Sio Jurnalis., Reba, Felix., Al-Husaini, Muhammad., Mandowen, Samuel Aleksander., Zein, Neni Nur Laili Ersela., & Judijanto, Loso. (2024). *Algoritma Pembelajaran Mesin: Dasar, Teknik, dan Aplikasi.* Jambi: PT. Sonpedia Publishing Indonesia.

Raharjo, B. (2021). *Fintech Teknologi Finansial Perbankan Digital.* Semarang: Penerbit Yayasan Prima Agus Teknik.

Setiyono, Wisnu Panggah., Sriyono, Sriyono., & Prapanca, Detak. (2021). *Buku Ajar Financial Technology*. Sidoarjo: Umsida Press.

ONLINE SOURCES

Tempo. (2021). Daftar Kasus Raibnya Dana Nasabah: BCA, BNI, Sampai Bank Mandiri. Tempo.Co. Retrieved from https://bisnis.tempo.co/read/1464998/daftar-kasus-raibnya-dana-nasabah-bca-bni-sampai-bank-mandiri

Tama, Deni R. (2022). Kroll/ACFE Indonesia Fraud Risk Survey. Retrieved from. https://www.kroll.com/en/insights/publications/unreported-fraud-a-risky-blindspot-for-indonesia

European Banking Authority. (2024). Risk Assessment Report - July 2024. Retrieved from https://eba.europa.eu/publications-and-media/publications/risk-assessment-report-july-2024.

Gifari, J. (2020). 3 Jenis Algoritma Machine Learning yang Dapat Digunakan di Dunia Perbankan. Retrieved from https://dqlab.id/pahami-machine-learning-dalam-dunia-perbankan.

Gokhale, Nikhil,. Gajaria, Ankur., Kaye, Rob., & Kuder, Dave. (2019). AI leaders in financial

services; Common Traits of Frontrunner in the Artificial Race. Retrieved from https://www2.deloitte.com/us/en/insights/industry/financial-services/artificial-intelligence-ai-financial-services-frontrunners.html

PwC. (2024). 94% Investor Meyakini Pelaporan Perusahaan tentang Kinerja Keberlanjutan mengandung Klaim Tanpa Bukti: Survey Investro Global PwC 2023. Retrieved from https://www.pwc.com/id/en/media-centre/press-release/2024/indonesian/survei-investor--global-pwc-2023.html

Vicente, V. (2024). Risk Assessment Matrix: Overview and Guide. Retrieved from https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/#authors,