Journal of Central Banking Law and Institutions, Vol. 5 No. 2, 2026, pp. 315 - 334
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
https://doi.org/10.21098/jcli.v5i2.421

LEGAL CERTAINTY FOR AI-RELATED CRIMES IN INDONESIA'S BANKING SECTOR

Fitria Damayanti,[a] Ridwan Arifin[b]

[a] Faculty of Law, Universitas Negeri Semarang, Indonesia, [b] Faculty of Law, Universitat de Barcelona, Spain
e-mail: fdamayanti645@students.unnes.ac.id; rarifiar119@alumnes.ub.edu

Submitted: 4 March 2025 - Last revised: 7 January 2026 - Accepted: 16 March 2026

Abstract

As the integration of artificial intelligence (AI) into Indonesia's rapidly evolving financial sector accelerates, the country faces critical challenges in ensuring legal certainty and protecting personal security. The rise of AI technologies in banking, fintech, and investment platforms introduces new complexities in regulatory oversight, particularly in preventing crimes such as fraud, money laundering, and cybersecurity breaches. This study examines legal certainty in the regulation of AI-related crimes in Indonesia's banking sector and its implications for personal security. The increasing use of AI in financial services has created regulatory challenges, particularly regarding personal data protection, fraud, and accountability. This research employs a normative juridical method with a statutory approach, analysing relevant Indonesian laws, including the Personal Data Protection Law, the Banking Law, the Electronic Information and Transactions Law, and the Financial Services Authority regulations. The findings reveal a legal vacuum in addressing AI-facilitated crimes, particularly regarding the allocation of responsibility and preventive mechanisms. Although existing regulations provide partial protection, they do not yet accommodate the specific risks posed by AI technologies in banking. This regulatory lacuna threatens legal certainty and personal security, particularly the right to privacy. This study highlights the urgency of developing explicit AI-related criminal laws for the financial sector to balance innovation and protection. This research is limited to doctrinal legal analysis and does not include empirical data, which may be explored in future studies.

Keywords: *artificial intelligence, banking sector, legal certainty, personal data protection*

I. INTRODUCTION

Technological developments have become increasingly rapid and uncontrollable. Technological progress drives a country's development by creating incentives for innovation and by encouraging the growth of industry, trade, finance, investment, and even institutional capacity.[1] This pattern of

[1] Ridwan Arifin et al., "Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia," *Jambura Law Review* 3 (2021): 137.

technological development is a double-edged sword, which requires special attention to prevent significant negative consequences. While this technological development has touched all aspects of our lives, it has drastically changed the financial sector.

One of the technological developments that is affecting the financial sector is Artificial Intelligence (AI). AI refers to the use of computers to emulate intelligent behaviour with minimal human intervention.[2] The Organisation for Economic Co-operation and Development (OECD) Principles on Artificial Intelligence establish five ethical principles as guidelines for the responsible development and use of AI, namely inclusive and sustainable growth, respect for human rights and democratic values, transparency and explainability of AI systems, robustness and security of systems, and accountability of AI actors through traceability and risk management.

The emergence of AI has had a positive impact on the financial sector, changing the traditional banking paradigm by advancing automation, deep data analysis, and transparency through blockchain security, and integrating new technologies such as machine learning and big data analytics.[3] This positive impact enables financial institutions to improve risk analysis, personalise services, and make more appropriate decisions based on their needs.

However, alongside technological developments in Indonesia, which have become increasingly advanced in the 21st century, significant problems have also emerged. One issue, personal data protection, is the main focus of studies in Indonesia. Under Law Number 27 of 2022 concerning Personal Data Protection, personal data refers to information about an individual who can be recognised or identified, either independently or when associated with other data, through electronic or non-electronic mechanisms, either directly or indirectly. In 2022, Indonesia was ranked 6th on the cybersecurity index for Southeast Asian countries. Data leakage cases in Indonesia do not only occur on social media. Compared with other Southeast Asian countries, Indonesia's cybersecurity received a score of 38.96 points.[4]

---

[2] Ibrahim Kamel, "Artificial Intelligence in Medicine," *Journal of Medical Artificial Intelligence* 7, no. 4 (2024): 11.

[3] Muhammad Rizki Sofyan and Abdurrozzaq Hasibuan, "Transformasi Digital dalam Industri Layanan Keuangan Implikasi dan Tantangan bagi Sektor Manufaktur," *Kohesi: Jurnal Sains dan Teknologi* 2, no. 4 (2024): 84 ; Zayran Mahir Qayyan, Ramesh Kumar. "Financial Inclusion and Economic Justice: The Role of Digital Finance in Empowering Indonesia's Poor," *Indonesian Economic Justice Review* 2, no. 1 (2025): 4.

[4] Waspiah et al., "Model Pelindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi," *Syntax Literate; Jurnal Ilmiah Indonesia* 8, no. 9 (2023): 5170; Ranty Mahardika Jhon, "Existence of Criminal Law on Dealing Cyber Crime in Indonesia." *Indonesian Journal of Criminal Law Studies* 3, no. 1 (2018): 29.

Table 1.
Amount of Data and Sources

No	Source	Data
1	dashboard.prakerja.go.id	17,331 data
2	ssso.datadik.kemendikbud.go.id	15,729 data
3	info.gtk.kemdikbud.go.id	10,761 data
4	djponline.go.id site	10,049 data
5	myaspk.bkn.go.id	7,000 data
6	daftarsscasn.bkn.go.id	6,770 data
7	ereg.pajak.go.id	5,083 data

Table 1 shows its alarming condition, which requires serious attention. As a tool of social control, the law must continually adapt to various phenomena in human life. According to legal experts, there are several functions of law, namely as a tool for social control, a tool for changing society, a tool for order and regulation of society, a means to realise social justice, a means of driving development, a critical function in law, a protective function, and a political tool.[5] From a human rights perspective, crimes against personal data caused by technological developments infringes on the right to privacy as outlined in Article 12 of the Universal Declaration of Human Rights (UDHR), and guarantees of the right to privacy in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), as well as the regionally recognised right to privacy over personal data under Article 21 of the 2012 ASEAN Human Rights Declaration.

When the right to privacy is infringed, it gives rise to a feeling of insecurity. Therefore, studies on legal certainty in financial crimes are urgent. It is necessary to study this because there are still very few Indonesian laws explicitly regulating financial crimes. This article addresses the legal vacuum in Indonesia to ensure legal certainty in the era of society 5.0.

Previous studies have examined some issues related to this legal vacuum. Waspiah et al. found that Indonesia must immediately adopt a special strategy to address various data-breach problems, including adopting a personal data protection legal framework modelled after those in Malaysia and Singapore.[6] On the other hand, Muhammad Ghozali et al., found that the National Cyber and Crypto Agency (BSSN) is a special independent institution, which is responsible for implementing cyber security efforts effectively and efficiently

[5] M. Yusuf Yahya and Harwis Alimuddin, "Roscou Pound: Hukum sebagai Alat Rekayasa Sosial (Keterhubungannya dengan Kaidah La Yunkaru Tagayyur Al-Ahkam Bi Tagayyuri Azzaman)," *Indonesian Journal of Shariah and Justice* 2, no. 2 (2022): 145.

[6] Waspiah et al., "Model Pelindungan Hukum."

through the utilisation, development, and coordination of all aspects of national cyber security.[7]

This research uses the statutory approach, namely a method that recognises hierarchy and the principles of statutory construction.[8] Meanwhile, the type of research used is normative juridical, namely, research that focuses on the body of literature in this field. This research includes studies on legal principles, synchronisation of laws and regulations, legal systematics, an inventory of positive law, and efforts to discern *law in concreto*.[9]

Several studies have examined the relationship between AI and financial regulation, including issues of digital governance and technological innovation. However, specific analysis of AI-facilitated crimes and their implications for legal certainty and personal security in Indonesia remains limited, particularly within the banking sector. This study, therefore, aims to fill this gap by examining how existing legal frameworks address emerging AI-related criminal risks in banking activities. The main research question guiding this study is: How does the current Indonesian legal framework address AI-related crimes in the banking sector, and to what extent does it ensure legal certainty and personal security? To ensure analytical depth and coherence, this research deliberately narrows its scope to the banking sector, given its central role in managing personal financial data and its heightened vulnerability to AI-based crimes. Other financial subsectors are discussed only as contextual references to support the primary analysis. Through this focused approach, the study seeks to contribute to the development of a more precise and responsive legal framework that balances technological advancement with the protection of individual rights.

II. LEGAL VACUUM ON REGULATIONS FOR PROTECTION FROM AI-ENABLED CRIME IN THE FINANCIAL SECTOR

The confidentiality of customer personal data is one of the main pillars of maintaining public trust in banking institutions. Banks play a strategic role in maintaining economic stability, which largely depends on customers' trust in the integrity and professionalism of these financial institutions. Confidentiality is strictly protected under Law Number 10 of 1998 concerning Banking,

---

[7] Ghozali, Muhammad, Nora Liana, Cut Afra, Zulfadly Siregar, and Muhammad Hatta, "Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya : Studi Kasus Peretasan Bank Syariah Indonesia (BSI)," *Cendekia: Jurnal Hukum, Sosial dan Humaniora* 2, no. 4 (2024): 802.

[8] Mochamad Mansur, "Analisis tentang Dikabulkannya Permohonan Wali Adhal atas Penetapan Pengadilan Agama," *Justitiable-Jurnal Hukum* 4, no. 1 (2021): 249.

[9] M. Najibur Rohman, "Tinjauan Yuridis Normatif terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia," *Jurnal Supremasi* 11, no. 2 (2021): 7.

which safeguards any information that reveals identity, financial transactions, or other information obtained in the course of the customer's relationship with the bank. A bank's failure to maintain confidentiality not only damages the financial institution's reputation but also exposes customers to potential losses and weakens trust in the banking system as a whole.[10]

Regulations governing personal data protection are set out in Law Number 27 of 2022 on Personal Data Protection (the PDP law), which is based on two principles. First, the protection of personal data is a fundamental human right that falls under the category of individual protection. Therefore, a strong legal foundation is needed to ensure the security of personal data based on the 1945 Constitution of the Republic of Indonesia. Second, personal data protection aims to safeguard citizens' rights, raise public awareness, and ensure recognition and respect for the importance of protecting personal data. Before the enactment of the PDP law, the regulation of personal data was scattered across various laws and regulations. To enhance the effectiveness of personal data protection implementation, it was necessary to establish a more structured framework within a single law.

The PDP law includes provisions regarding fundamental principles; categories of personal data; rights of personal data subjects; the process of personal data processing; responsibilities of personal data controllers and processors in managing such data; transfer of personal data; administrative sanctions; institutional aspects; international cooperation; public participation; dispute resolution mechanisms and legal procedures; restrictions on the use of personal data; and criminal provisions related to personal data protection. The PDP Law is a comprehensive effort to safeguard the security and privacy of personal data during processing, ensuring the fulfilment of the constitutional rights of personal data subjects. Despite the various aspects of personal data protection in this law, there remains a legal vacuum regarding the protection of AI-related personal data in the financial sector.

This vacuum creates a weakness: regulations regarding AI have not yet been established, especially since AI is key to storing personal data. This legal vacuum has the potential to cause legal uncertainty *(rechtsonzekerheid)* and regulatory ambiguity in society, which may ultimately lead to legal chaos *(rechtsverwarring)*. In other words, if something is not yet regulated, it may be considered permissible as long as clear procedures are followed; and if it is regulated, that does not necessarily mean it is prohibited.[11] This is in line with

[10] Widiya Dwi Novarianti et al., "Kerahasiaan Bank vs Hak atas Informasi: Mengurai Konflik Kepentingan dalam Perlindungan Data Pribadi," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 112.

[11] Moh Yusuf, "Kekosongan Hukum pada Penyiaran di Media Sosial," *Tadulako Master Law Journal* 8, no. 3 (2024): 243.

the principles in criminal law, namely the principle of *nullum crimen sine lege,* which means "there is no crime and no punishment without prior penal law".

Therefore, applications and machines that utilise AI must have permission and legal status so that they can be held criminally responsible for all risks that occur; besides that, regulations are really needed in the future as clearer references and guidelines.[12] Key provisions of the PDP Law are as follows:

1. Article 15
   This article emphasises the rights of Personal Data Subjects in the financial sector, particularly in the supervision of banking, capital markets, and other financial institutions. These exceptions include the need to maintain financial system stability and carry out law enforcement processes, which are considered essential to the security and integrity of the financial services sector. Based on this, personal data may be processed without the consent of the Personal Data Subject if it is used for monitoring and risk analysis purposes to maintain the health of the financial system. However, this implementation must adhere to principles of transparency and accountability to ensure data protection and respect individual rights within the limits established by law. Therefore, although Article 15 provides for financial sector supervision, it is important to monitor its implementation to avoid compromising the privacy of Personal Data Subjects.
2. Article 50
   Article 50 sets out obligations for the control of Personal Data in the financial sector, particularly for monitoring interests related to financial system stability and law enforcement. These exceptions include the need for strict supervision of financial institutions to prevent illegal actions and maintain market integrity. Accordingly, personal data may be processed without obtaining consent from the Personal Data Subject, provided it is conducted within the framework of state administration and in accordance with applicable regulations. However, it is vital to ensure that these transfers are not used for criminal purposes and that individual rights are respected, thereby maintaining transparency and accountability. Therefore, although this provides some measure of oversight for the financial services sector, its implementation must be carried out with care to protect the privacy of Personal Data Subjects.

From these two articles, it can be seen that discussions of the financial sector in relation to personal data protection have not been a particular focus. Existing exceptions have not been reconciled with related financial-sector regulations, creating confusion and gaps in the protection of personal data. These gaps provide opportunities for individuals who intend to commit crimes.

[12] Waspiah et al., "Model Pelindungan Hukum."

The PDP Law does not cover the protection of personal data affected by AI-related crimes. Meanwhile, regulations concerning crimes in the financial sector are currently only governed by Financial Services Authority Regulation (POJK) Number 16/2023 on the Investigation of Criminal Acts in the Financial Services Sector, which, hierarchically, still lacks sufficient legal authority to ensure legal certainty. This regulation was formulated pursuant to Law Number 21 of 2011 concerning the Financial Services Authority, which grants the Financial Services Authority (OJK) the authority to investigate criminal acts in the financial services sector. With the enactment of Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector, OJK's authority to investigate and handle violations in the financial services sector has been further expanded. Therefore, Financial Services Authority Regulation Number 22/POJK.01/2015 on the Investigation of Criminal Acts in the Financial Services Sector needs to be updated to align with Law Number 4 of 2023.

Law number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and the Criminal Code (KUHP) currently regulate fraud and misuse of electronic information. However, these provisions were not designed to address autonomous or semi-autonomous AI systems. Consequently, criminal liability remains unclear when AI acts as an intermediary, creating enforcement challenges and weakening legal certainty. Comparatively, the European Union has introduced the Artificial Intelligence Act, which adopts a risk-based approach to regulating AI systems, particularly those used in high-risk sectors such as finance. Meanwhile, the United States has promulgated sectoral guidelines and enforcement through financial regulators. These approaches demonstrate that explicit AI governance frameworks can strengthen legal certainty while supporting innovation. Their adaptation of these approaches to Indonesia requires careful consideration of the differences in legal culture, regulatory capacity, and enforcement mechanisms.

A comprehensive legal framework for the prevention of AI-enabled crimes must cover the following areas of the financial sector:

1. Banking
   Banking is a collection of financial institutions engaged in a variety of financial services, both consumer and commercial. In the digital era, banking faces new challenges such as data security, electronic fraud, and consumer protection. Current regulations have an obligation to address these issues by establishing stricter safety standards, promoting transparency, and protecting consumer rights.
2. Capital Markets, Financial Derivatives, and Carbon Exchanges
   Capital markets provide companies with access to funding from the general public through the issuance of securities. Financial derivatives,

such as options and futures, are implemented to manage risk. Carbon exchange originated as a carbon emissions trading mechanism, supporting sustainable environmental management goals.

3. Insurance, Guarantee, and Pension Funds
   The insurance sector facilitates financial protection for individuals or legal entities against certain risks through insurance products. Guarantee functions to guarantee the financial obligations of third parties, while pension funds manage savings for retirement purposes.
4. Financing Institutions, Venture Capital Companies, Microfinance Institutions, and Other LJKs
   Financing institutions facilitate loans to individuals or legal entities. Venture capital firms invest in a business with high growth potential. Micro and small financial institutions provide financial services to lower-income populations.
5. Financial Sector Technology Innovation, as well as Digital Financial Assets and Crypto Assets
   Technological innovation includes fintech, which is changing how financial services are delivered, including digital payments and online loans. Digital financial assets and crypto provide another investment-related solution, but also bring challenges regarding regulation and security.
6. Behaviour of Financial Services Companies and Implementation of Consumer Education and Protection

The behaviour of businesses in the financial services sector must comply with ethical and transparency principles to build public trust. Consumer education regarding financial products is vital for them to make appropriate decisions.[13]

Therefore, regulatory reform is needed to address AI-driven crimes, in addition to policies governing AI use in the financial sector.

Based on the need for a regulatory framework to provide legal certainty regarding crimes in the financial sector caused by AI, further regulation is needed to address:

1. Responsibility Arrangements
   Regulations regarding legal responsibility for losses arising from the use of AI apply to developers, service providers, and users of the technology, so that no party escapes responsibility.
2. Data Security and Privacy
   Data-related security requires regulations regarding personal data protection to prevent AI from accessing or manipulating financial data.

[13] Angkasa Angkasa et al., "Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim," *Lex Scientia Law Review* 7, no. 1 (2023): 156.

3. Audit and Transparency
   Audits and transparency are necessary to ensure that AI systems comply with applicable regulations and can be held accountable by the authorities.
4. Mechanisms
   Preparation of proactive risk-mitigation mechanisms, such as testing technology resilience against potential irregularities or criminal activity. Therefore, mechanisms for crime prevention regulations in the financial sector are necessary.
5. Framework
   Establishment of a framework to facilitate the cross-border nature of AI-based crimes, thereby preventing perpetrators from exploiting these advances for criminal purposes.

Regulations that are designed or formulated must follow the process of lawmaking, which consists of five stages: planning, formulation, discussion, ratification, and promulgation.[14] Efforts to achieve this require community participation, in line with Lord Acton's observation that "power tends to corrupt, and absolute power corrupts absolutely". The power to enact inequitable laws and minimal checks and balances make legal products produced before the amendments to the 1945 Constitution more profitable and in favour of powerful interests, resulting in a loss for society as a result of the enactment of corrupt laws. Law no. 5 of 1974 concerning Regional Government is an example of a law enacted by the new Order regime that created space for corruption. Very centralised central power.[15] Regions are only spectators in economic development. Because centralised power is so vast and tends to be authoritarian, this gives rise to massive corruption that benefits both individuals and the ruling group.

The principles that must be applied are enacting sound legislation (*beginsel van behoorlijke regelgeving*) based on Article 5 of Law Number 12 of 2011 on the Formation of Laws and Regulations (the Legislation Law), which governs the formation of laws and regulations. Seven main principles must be fulfilled: (1) clarity of purpose, which states that every regulation must have a clear purpose to avoid confusion; (2) appropriate institutions or formulating officials, ensuring that regulations are made by authorised institutions to guarantee legal force; (3) correspondence between type, hierarchy, and material content, which requires that regulations do not conflict with superior regulations; (4) can be

[14] Abdurrakhman Alhakim and Egia Ginting, "Analisis Pembentukan Undang-Undang Cipta Kerja pada Tahapan Perencanaan dan Penyusunan Berdasarkan Undang-Undang Pembentukan Peraturan Perundang-Undangan," in *Conference on Management, Business, Innovation, Education and Social Sciences (CoMBInES)* (Universitas Internasional Batam, 2021), 288.

[15] Fahmi Ramadhan Firdaus, "Pencegahan Korupsi Legislasi melalui Penguatan Partisipasi Publik dalam Proses Pembentukan Undang-Undang," *Jurnal Legislasi Indonesia* 17, no. 3 (2020): 282.

implemented, emphasising that regulations must be realistic and implementable in practice; (5) usefulness, ensuring that regulations truly benefit society; (6) clarity of formulation, so that the legal language used is easy to understand and does not give rise to multiple interpretations; and (7) openness, which requires that the regulatory formation process be carried out transparently so that the public can provide input. [16]

The impact analysis of providing these principles is significant. With clarity of purpose, the public can understand the meaning of each regulation, thus ensuring the fulfilment of these provisions. Appropriate institutions avoid legal conflicts and increase regulatory legitimacy. Conformity between types and hierarchies ensures that regulations support one another and do not conflict, thereby creating a cohesive legal system. The implementation aspect that can be carried out shows that the regulation is relevant to real conditions, while the usability ensures that the regulation provides real benefits for society. The clarity of the formulation helps the public understand the contents of regulations, and openness in the formation process provides space for public participation, strengthening democracy and accountability. Thus, following these principles not only creates sound written laws and regulations but also supports a legal system that is fair and responsive to society's needs.

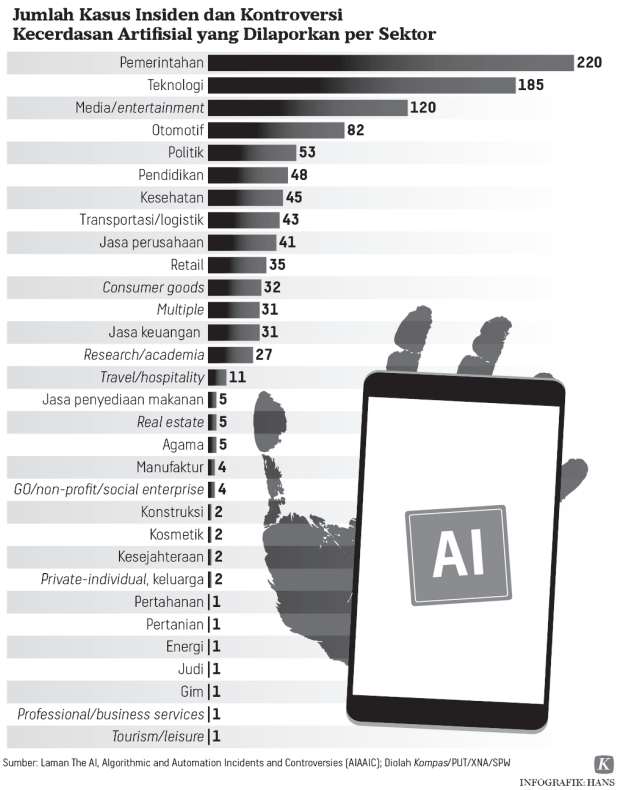
Providing legal certainty in the AI era arguably requires not only punitive mechanisms but also preventive governance, particularly in the banking sector, where personal data protection is central. Without these measures, AI implementation in banking may undermine both legal certainty and personal security.

III. IMPLICATIONS OF AI CRIME IN THE FINANCIAL SECTOR FOR PERSONAL SECURITY

The implications of AI-enabled crimes in the financial sector for personal security are significant, particularly regarding personal data protection. AI used to process massive amounts of customer data can become a tool for criminals to commit data theft.

[16] Angga Prastyo et al., "Pengaturan Asas Keterbukaan dalam Pembentukan Undang-Undang," *Jurnal Cakrawala Hukum* 11, no. 2 (2020): 129.

Figure 1. Number of AI Intelligence Incidents and Controversial Cases



Source: Kompas.com

The infographic in Figure 1 above shows the number of AI-related incidents and controversies reported across sectors, with the government sector leading with 220 cases. This was followed by the technology sector with 185 cases, reflecting the high use of AI in software and hardware development. Media and entertainment cases came in third with 120 cases, possibly related to issues such as deepfakes, algorithmic bias, or copyright infringement. The automotive (82 cases), politics (53 cases), and education (48 cases) sectors also recorded significant numbers, while the health sector (45 cases) showed the need to pay attention to the safety and accuracy of AI technology in medical services. Meanwhile, other sectors such as construction, energy, defence, and gaming recorded only around 1-2 cases, indicating that the application of AI remains limited in those sectors. Based on this data, it is clear that the use of AI needs to be evaluated to maintain transparency and ethical standards through strict, clear regulations.

This issue can be observed in several real-world cases in other countries and serves as a warning for the Indonesian market. The 2019 leak of personal data from more than 100 million Capital One customers is a clear example of the security risks faced by the financial sector due to gaps in AI-based technology. In this unfortunate incident, a former Amazon Web Services (AWS) employee exploited a weakness in Capital One's firewall configuration to access personal data, including names, addresses, credit scores, and other financial information. This crime exploited weaknesses in AI-based security systems, specifically in cloud computing management, which is integral to modern financial technology. Apart from causing major financial and reputational losses for Capital One, this case also raises concerns regarding the protection of personal data, especially for customers. Consumer protection is regulated by the General Data Protection Regulation (GDPR) in the European Union and the Consumer Financial Protection Bureau in the United States. In the authors' view, this case emphasises the need for regular audits of AI-based security systems, transparency in data management, and strict law enforcement to ensure technological protection in the financial sector, particularly regarding personal data.

Indonesia has recently been plagued by AI-driven fraud that fakes a person's voice or appearance. The scheme's target is people who are less technologically literate. Usually, this method involves false claims of having won a prize and ends with an attempt to transfer funds to the fraudster's account. A video circulated on the komdigi.go.id page on TikTok falsely claimed that the Minister of Finance, Sri Mulyani, would distribute IDR 50 million in business capital on the condition that the upload be shared with friends. Reporting from turnbackhoax.id, the video claiming that Sri Mulyani distributed IDR 50 million is a generative AI creation and was used to defraud.

Fraud utilising AI has become increasingly difficult to detect, as such practices often simulate legitimate activities. These scams often use deepfake technology, which makes them difficult to distinguish from reality. Deepfake is a technology that utilises generative AI to produce fake videos or audio that appear very realistic. University College London ranks deepfakes among the biggest threats facing society today.[17] Deepfakes' ability to imitate voices and alter digital content is often used to spread pornographic content, commit extortion, or disseminate misleading information to the public. This technology is frequently misused by certain individuals to take others' personal data without consent and secretly use it for criminal activities. Using this technology, images or videos can be manipulated to make it appear as if someone is doing something that never actually happened.

[17] Shannon Gandrova and Ricky Banke, "Penerapan Hukum Positif Indonesia terhadap Kasus Kejahatan Dunia Maya Deepfake," *Madani: Jurnal Ilmiah Multidisiplin* 1, no. 10 (2023): 652.

Scams using AI have become increasingly sophisticated, exploiting advanced technologies like deepfakes to deceive and manipulate individuals. One example of such fraud involves AI-generated voice imitation. The OJK has issued warnings about scammers using AI to replicate the voices of family members or close acquaintances. In this type of scam, a fraudster may call a victim using a voice that closely resembles someone they know, tricking them into following fraudulent instructions. AI's ability to produce highly accurate voice replicas makes this scam particularly convincing, often leading victims to unwittingly provide sensitive information or transfer funds.

Another troubling example is the use of AI-generated videos in scams. Recently, a scam involved a video call where the victim received a call from an unknown number featuring the face and voice of a well-known celebrity. The fraudster, using AI to create a digital clone of the celebrity, falsely claimed that the victim had won a large prize. This type of scam relies on AI's ability to analyse vast amounts of publicly available online content to create lifelike impersonations, making it increasingly difficult for individuals to distinguish between real and fraudulent interactions. Such scams demonstrate the alarming potential of AI technologies to manipulate not only voices but also images and videos, posing serious risks to personal security and financial safety.

Fraudsters typically use deepfake technology to impersonate trusted individuals, thereby manipulating victims' perception of authenticity. In another example, Bank Central Asia (BCA), a prominent player in Indonesia's financial sector, has taken proactive measures to address the growing concern of AI-based fraud. Through its website, BCA offers valuable educational resources to help individuals protect themselves from such threats. One of the most crucial tips is to avoid sharing personal information on social media, as this data can be exploited by malicious actors to create deepfakes and carry out fraudulent activities. Additionally, individuals are advised to exercise caution when receiving calls, messages, or emails from unknown numbers or accounts, as these could be attempts to deceive or defraud. Verifying the caller's identity through a trusted source is recommended to ensure credibility.

In cases where suspicious communication cannot be avoided, verification through official banking channels is strongly recommended to ensure legal and factual credibility. If the responses seem unclear or inconsistent, it is prudent to end the conversation immediately. Fraudsters often use high-pressure tactics, such as promising valuable items or creating a sense of urgency, to persuade victims to provide money or sensitive information. Individuals should never comply with such requests and should remain firm in rejecting demands for financial assistance or personal data.

Moreover, BCA emphasises the need to be vigilant for signs of AI-generated voice fraud. Deepfake technology can replicate a person's voice,

but it often includes unnatural pauses or distortions that can be detected with careful attention. Similarly, visual AI fraud can manifest as discrepancies in facial movements, mismatched features, or blurred backgrounds in videos. If something appears too perfect or overly polished, it is critical to approach the situation with scepticism and report any potential fraud. These steps are vital in safeguarding against the growing threat of AI-driven financial crimes.

From a legal perspective, the regulation of AI-related conduct remains fragmented, as existing laws were not formulated to address autonomous or semi-autonomous technological systems. This implementation is regulated by Article 26, paragraph (1), of the ITE Law, which states that the use of personal data must be approved by the data owner. Apart from that, the PDP Law provides a framework to ensure the security of personal information from unauthorised access. AI crimes in the financial sector not only threaten the privacy rights of every individual but also cause direct financial losses for victims, requiring strict supervision and law enforcement to protect personal security. Several aspects that must be regulated further in an effort to fill the legal vacuum are:

1. Threats to Data Security
   AI has the potential to process and manage massive volumes of financial data, which, in the absence of strict governance, may expose banking institutions to heightened risks of data misuse. If an AI system is implemented, sensitive data such as account numbers, transaction history, or personal information can be exploited by criminals for fraud and theft.
2. Increased Risk of Cybercrime
   AI also has the potential to aid in the commission of cybercrime, such as using deepfake technology to impersonate bank officials or clients, thereby defrauding many uninformed audiences or manipulating algorithms to steal funds or create fake transactions, resulting in misappropriation of funds.
3. Dependence on Technology
   Financial institutions that are highly dependent on AI systems may face significant legal and operational consequences in the event of system failures or malicious manipulation.
4. Algorithmic Discrimination
   Assessments carried out by AI can give rise to direct discrimination because it lacks empathy and therefore does not consider social aspects in its decisions. For example, poorly designed assessments can provide uncertain assessments based on location, occupation, or other demographic data, thereby hindering access to financial services for certain groups.

5. Unemployment Due to Automation
   AI replacing some human workers in the financial sector, such as bank tellers, credit analysts, or customer service staff, could lead to a decline in the use of human labour in the industry. This affects large communities, especially in countries with high levels of poverty, and is aligned with a decrease in the use of human labour.
6. Lack of Accountability
   The worrying condition in AI systems is that it is difficult to identify the responsible party, especially when multiple parties are involved, such as developers, service providers, and users. This can create increasingly difficult conditions that arise in the legal settlement process.

This shows the importance of strict supervision, clear regulations, and risk mitigation efforts in the use of AI in the financial sector so that this technology not only provides benefits but also minimises potential losses.

Looking at the personal security theory, there are things that need to be studied in more depth. The concept of personal security is rooted in human rights, introduced by American President Franklin D. Roosevelt in 1941. These rights encompass four fundamental freedoms inherent to every individual: the freedom of speech and expression, the freedom to worship according to one's beliefs, the freedom from want, and the freedom from fear. In this section, insecurity is defined as a pervasive and enduring state, which is consistent with the view that anxiety about loss is key to understanding the subjective experience of security. This provides valuable insight into how security and insecurity can influence an individual's self-confidence, as well as highlighting the ironic cognitive effects of worry about loss.

From a Human Rights perspective, personal security correlates with the right to privacy. If crimes against personal data caused by technological developments infringe the right to privacy under Article 12 of the UDHR. The right to privacy is increasingly relevant in today's digital era, where personal information can be easily accessed and misused. By affirming this right, Article 12 plays an important role in promoting individual autonomy and dignity. Article 12 of the UDHR serves as an important protection for personal privacy and reputation, reinforcing the principle that individuals must be free from unwanted interference and have access to legal remedies when their rights are violated.

The right to privacy is guaranteed in Article 17 of the ICCPR. The first statement asserts that every person has the right to be free from unlawful or arbitrary threats to their privacy, as well as from illegal actions that may harm their honour and reputation. This provides an understanding of the importance of protecting an individual's personal space, including personal

data, family relationships, residence, and communications. Protecting against threats of this kind requires clear legal guidelines and must not be carried out carelessly, thereby protecting individuals from arbitrary actions by authorities or third parties. The second statement clarifies everyone's right to seek legal protection against such threats or attacks. This means that individuals have the right to file lawsuits if their rights are violated, and that states have an obligation to provide a legal framework that protects privacy and reputation. Therefore, these two statements collectively form an important basis for protecting the right to privacy, requiring assurance that individuals are not only protected from violations but also have access to justice when their rights are threatened. In the context of a modern world increasingly influenced by technology, these principles become increasingly relevant for protecting individual dignity and autonomy.

Regionally, the right to privacy in relation to personal data is recognised in Article 21 of the 2012 ASEAN Human Rights Declaration. This article emphasises that every individual has a recognised right to privacy that protects them from arbitrary interference in their private lives. This right is enshrined in various international treaties and conventions, reflecting a global consensus on the importance of maintaining personal autonomy and dignity. Legal frameworks must continue to adapt to address emerging challenges in the digital landscape while ensuring that these fundamental rights are upheld without unfair infringement.

Among the various types of human rights, fundamental rights serve as the foundation of human rights themselves, namely the right to privacy.[18] If the right to privacy in this case is not protected, then Indonesia has also violated its international law obligations. When linked to constitutional rights, this right to privacy is affirmed in Article 28G of the 1945 Constitution, which states that every person has the right to protect themselves, their families, their rank, their dignity, and their property under their control. This includes protecting individual privacy from unauthorised interference.

IV. CONCLUDING REMARKS

In the ongoing development of technology, AI in particular has become a double-edged sword, requiring special attention to prevent significant negative consequences. This technological development has brought many changes

[18] Putra Wijaya and H. B. Gusliana, "Relevansi Hak Privasi dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," *Jurnal Ilmiah Wahana Pendidikan* 10, no. 22 (2024): 669.

across various sectors of life, including the financial sector. There are several aspects of AI that need further regulation to address the legal vacuum, namely security threats, increased risk of cybercrime, dependence on technology, algorithmic discrimination, unemployment due to automation, and lack of accountability. It is necessary to formulate regulations that still consider key principles, such as clarity of objectives, the appropriateness of the responsible institution or official, alignment of types, hierarchy, and regulated content, ease of implementation, the benefits produced, clarity in formulation, and aspects of transparency. Meanwhile, the implications of AI have negative effects on the financial sector, requiring early prevention to avoid compromising personal security and aligning with the right to privacy for every individual. The right to privacy is contained in various international human rights instruments. In the authors' opinion, there is a need for legal certainty, facilitated by a legislative body that explicitly regulates AI crimes in the financial sector, given the financial sector's vital role in a country's development. Therefore, this study recommends the formulation of explicit regulations governing AI-related crimes in the banking sector, including accountability mechanisms, mandatory risk assessments, and strengthened personal data protection standards.

REFERENCES

Alhakim, Abdurrakhman, and Egia Ginting. "Analisis Pembentukan Undang-Undang Cipta Kerja pada Tahapan Perencanaan dan Penyusunan Berdasarkan Undang-Undang Pembentukan Peraturan Perundang-Undangan." In *Conference on Management, Business, Innovation, Education and Social Sciences(CoMBInES)* (Universitas Internasional Batam, 2021), 284-96. https://garuda.kemdiktisaintek.go.id/documents/detail/3633999.

Angkasa, Angkasa, Filep Wamafma, Ogiandhafiz Juanda, and Bhanu Prakash Nunna. "Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim." *Lex Scientia Law Review* 7, no. 1 (2023): 119-178. DOI:10.15294/lesrev.v7i1.67558.

Arifin, Ridwan, Juan Anthonio Kambuno, Waspiah, and Dian Latifiani. "Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia." *Jambura Law Review* 3 (2021): 135–60. https://doi.org/10.33756/jlr.v3i0.9635.

Firdaus, Fahmi Ramadhan. "Pencegahan Korupsi Legislasi melalui Penguatan Partisipasi Publik dalam Proses Pembentukan Undang-Undang." *Jurnal Legislasi Indonesia* 17, no. 3 (2020): 282. https://doi.org/10.54629/jli.v17i3.679.

Jhon, Ranty Mahardika. "Existence of Criminal Law on Dealing Cyber Crime in Indonesia." *Indonesian Journal of Criminal Law Studies* 3, no. 1 (2018): 25-34. https://doi.org/10.15294/b69m5x33.

Gandrova, Shannon, and Ricky Banke. "Penerapan Hukum Positif Indonesia terhadap Kasus Kejahatan Dunia Maya Deepfake." *Madani: Jurnal Ilmiah Multidisiplin* 1, no. 10 (2023): 650–57. https://doi.org/10.5281/zenodo.10201140.

Ghozali, Muhammad, Nora Liana, Cut Afra, et al. "Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya : Studi Kasus Peretasan Bank Syariah Indonesia (BSI)." *Cendekia: Jurnal Hukum, Sosial dan Humaniora* 2, no. 4 (2024): 797–809. https://doi.org/10.70193/cendekia.v2i4.113.

Kamel, Ibrahim. "Artificial Intelligence in Medicine." *Journal of Medical Artificial Intelligence* 7, no. 4 (2024): 10–12. https://doi.org/10.21037/jmai-24-12.

Mansur, Mochamad. "Analisis tentang Dikabulkannya Permohonan Wali Adhal atas Penetapan Pengadilan Agama." *Justitiable-Jurnal Hukum* 4, no. 1 (2021): 248–53. https://doi.org/10.56071/justitiable.v4i1.339.

Novarianti, Widiya Dwi, Athalia Pranata Putri S. Meliala, Nova Arini Stevia Yusuf, and Bintang Naharika Citra Melati. "Kerahasiaan Bank vs Hak atas Informasi: Mengurai Konflik Kepentingan dalam Perlindungan Data Pribadi," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 103–14. https://ejurnal.kampusakademik.co.id/index.php/jmia/article/view/3180.

Prastyo, Angga, Samsul Wahidin, and Supriyadi Supriyadi. "Pengaturan Asas Keterbukaan dalam Pembentukan Undang-Undang." *Jurnal Cakrawala Hukum* 11, no. 2 (2020): 125–35. https://doi.org/10.26905/idjch.v11i2.4136.

Qayyan, Zayran Mahir, and Ramesh Kumar. "Financial Inclusion and Economic Justice: The Role of Digital Finance in Empowering Indonesia's Poor," *Indonesian Economic Justice Review* 2, no. 1 (2025): 2-5. https://doi.org/10.65815/jmdp2575.

Rohman, M. Najibur. "Tinjauan Yuridis Normatif terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia." *Jurnal Supremasi* 11, no. 2 (2021): 1–10. https://doi.org/10.35457/supremasi.v11i2.1284.

Sofyan, Muhammad Rizki, and Abdurrozzaq Hasibuan. "Transformasi Digital dalam Industri Layanan Keuangan Implikasi dan Tantangan bagi Sektor Manufaktur." *Kohesi: Jurnal Sains dan Teknologi* 2, no. 4 (2024): 80–89. https://garuda.kemdiktisaintek.go.id/documents/detail/4327694.

Waspiah, Novera Sekar, Ammirah Lies, Tegar Islami, Setyaning Wida, and Salisa Widayaning. "Model Pelindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi." *Syntax Literate; Jurnal Ilmiah Indonesia* 8, no. 9 (2023): 5165–79. https://doi.org/10.36418/syntax-literate.v8i9.13662.

Wijaya, Putra, and H. B. Gusliana. "Relevansi Hak Privasi dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945." *Jurnal Ilmiah Wahana Pendidikan* 10, no. 22 (2024): 662-672, https://doi.org/10.5281/zenodo.14574771.

Yahya, M. Yusuf, and Harwis Alimuddin. "Roscou Pound: Hukum sebagai Alat Rekayasa Sosial (Keterhubungannya dengan Kaidah La Yunkaru Tagayyur Al-Ahkam Bi Tagayyuri Azzaman)." *Indonesian Journal of Shariah and Justice* 2, no. 2 (2022): 141–61. https://doi.org/10.46339/ijsj.v2i2.22.

Yusuf, Moh. "Kekosongan Hukum pada Penyiaran di Media Sosial." *Tadulako Master Law Journal* 8, no. 3 (2024): 243, https://garuda.kemdiktisaintek.go.id/documents/detail/5718110.

This page is intentionally left blank