Criminal Legal Aspects of the Use of Artificial Intelligence (Ai) as a Means of Fraud From the Perspective of Ite Law

Muhammad Harimanka S Harahap, Suci Ramadani, Rahmayanti

Abstract

The rapid development of information and communication technology has brought about various innovations, one of which is artificial intelligence (AI). However, despite its benefits, AI also has the potential to be misused as a means to commit crimes, particularly digital fraud. This study aims to analyze the criminal law aspects of the use of AI as a tool for fraud crimes from the perspective of the Electronic Information and Transactions Law (UU ITE). The method used is a normative juridical approach by reviewing relevant laws and regulations, legal literature, and case studies. The results indicate that although the ITE Law does not explicitly regulate the use of AI, criminal provisions in articles related to electronic fraud can be applied to perpetrators who use AI to commit fraud. p, there is an urgency for policymakers to formulate more comprehensive regulations to anticipate AI-based digital crimes. This study recommends the need for national legal updates that are adaptive to technological advances, as well as increasing the capacity of law enforcement officials to detect and handle cybercrimes involving AI.

Keywords: Criminal Law Aspects, Artificial Intelligence (AI), Fraud

Muhammad Harimanka S Harahap [1]
Department of Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: ariharahap1991@gmail.com

Suci Ramadani, Rahmayanti
e-mail: suciramadani@dosen.pancabudi.ac.id , rahmayanti@dosen.pancabudi.ac.id

2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

Introduction

The development of digital technology in the Industrial Revolution 4.0 era has driven rapid advancements in the field of artificial intelligence (AI). This technology enables machines or computer systems to perform tasks that previously required human intelligence—such as facial recognition, language comprehension, decision-making, and the generation of new content that closely mimics human output. AI has become an integral part of modern life, contributing significantly to sectors such as the economy, education, healthcare, communication, and security. However, alongside its benefits, AI brings complex new challenges and risks, particularly regarding legal and security aspects. One phenomenon warranting attention is the misuse of AI technology to commit criminal acts, specifically fraud. In this context, AI is not merely a supporting tool but has transformed into a primary instrument for executing criminal schemes. For instance, fraudsters can use deepfakes to fabricate videos of public figures' faces or voices to deceive victims; employ AI-driven chatbots to mimic human interaction in phishing or fake investment scams; or utilize natural language processing techniques to craft highly persuasive fraudulent emails that are difficult to distinguish from legitimate messages.

This phenomenon raises new concerns regarding law enforcement practices. AI-enabled fraud possesses distinct characteristics: it is sophisticated, difficult to detect, capable of crossing jurisdictional boundaries, and often leaves no clear digital footprint. In some instances, perpetrators can completely mask their identities behind automated AI systems, thereby complicating the processes of identification and evidentiary proof in court. In Indonesia, fraud is generally governed by Article 378 of the Criminal Code (KUHP)—a Dutch colonial-era law dating back to 1918. Meanwhile, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law)—as amended by Law No. 19 of 2016—serves as the legal basis for prosecuting offenders who utilize electronic media and digital systems. Nevertheless, neither the Criminal Code nor the ITE Law explicitly addresses or anticipates the evolution of AI technology as a means or subject of criminal activity. Consequently, there is a potential for a legal vacuum and legal uncertainty when handling AI-based fraud cases.

In Indonesia, fraud in general is regulated under Article 378 of the Indonesian Criminal Code (KUHP), which originated from Dutch colonial legislation enacted in 1918. Meanwhile, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law Number 19 of 2016, serves as a legal basis for prosecuting perpetrators of crimes involving electronic media and digital systems. Nevertheless, neither the Criminal Code nor the ITE Law explicitly regulates or anticipates the development of AI as a means or instrument of criminal offenses. Consequently, there is a potential legal vacuum and legal uncertainty in dealing with AIbased fraud cases.

Important questions therefore arise. Can AI be classified as a means or instrument of a criminal offense in the same manner as weapons or other means recognized in conventional criminal law? How can the concept of *mens rea* (criminal intent) be applied when some actions are performed automatically by machines? Who should bear criminal responsibility when AI acts based on human instructions, training, or even autonomously? Furthermore, is the current Indonesian criminal justice system sufficiently adaptive and progressive to address these challenges? The regulatory gap and limitations of existing positive legal instruments constitute an urgency that cannot be ignored. At the same time, criminal law must be able to keep pace with technological developments so that it does not fall behind and can continue to provide legal

protection for society. Therefore, an in-depth juridical study is required concerning the criminal law aspects of the use of Artificial Intelligence in fraudulent activities, both within the framework of the Criminal Code and within the scope of the ITE Law

Theoretically, criminal law aims to protect the legal interests of society from all forms of harmful conduct, including fraud. The Indonesian Criminal Code, as the positive criminal law of Indonesia, regulates fraudulent acts through Article 378, which emphasizes the elements of deception or a series of false statements intended to obtain unlawful benefits. In addition, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law Number 19 of 2016, provides an additional legal basis for prosecuting fraudulent acts committed through electronic media. However, in practice, developments in information technology, particularly Artificial Intelligence (AI), have created significant legal gaps. AI technology enables perpetrators to commit fraud through highly sophisticated methods, such as deepfakes, voice cloning, automated chatbots, and other forms of digital data manipulation. These tools are capable of deceiving victims more convincingly, on a broader scale, and within a very short period of time.

The problem arises when existing legal theories are insufficiently adaptive to these emerging forms of criminal conduct. The Criminal Code and the ITE Law do not explicitly regulate the use of AI in fraudulent activities, resulting in weaknesses in law enforcement or even juridical uncertainty. For example, in certain cases, law enforcement authorities may face difficulties in proving the element of intent and determining the role of human perpetrators when AI is used as the primary instrument of the crime. Under classical criminal law theory, criminal responsibility is imposed upon human legal subjects rather than technological entities. This condition demonstrates a discrepancy between prevailing criminal law theory and the practical realities of crime. Criminal law theory emphasizes the responsibility of human perpetrators and the element of intent, whereas in practice, AI may operate automatically or semi-autonomously based on algorithms without direct human intervention. This raises fundamental questions regarding who should be held responsible when a crime is committed through a tool that operates independently and how law enforcement authorities can identify and prove criminal acts committed through AI.

One example of the use of Artificial Intelligence (AI) as a means of fraudulent crime occurred in Indonesia in January 2025. A deepfake-based fraud case resulted in losses amounting to tens of millions of rupiah. The modus operandi involved a manipulated video depicting President Prabowo Subianto as if he were announcing a government financial assistance program. The video contained a statement suggesting that each family in need would receive financial assistance of IDR 50 million. In reality, President Prabowo had never made such a statement.

The perpetrator, identified by the initials AMA, included a telephone number in the video and requested victims to transfer a certain amount of money as an initial administrative fee. The requested amounts varied from IDR 250,000 to IDR 1,000,000. After receiving the payments, the perpetrator disappeared without providing any assistance. Following an investigation, AMA was arrested at his residence in Central Lampung, Lampung Province, on January 16, 2025. He was charged under the Electronic Information and Transactions Law (ITE Law) and Article 51 paragraph (1) in conjunction with Article 35 of Law Number 1 of 2024, which amended Law Number 11 of 2008 concerning Electronic Information and Transactions

If convicted, AMA faced a maximum sentence of 12 years of imprisonment and a fine of up to IDR 12 billion. Another example occurred in East Java, where the East Java Regional Police uncovered an AI deepfake fraud case involving a regional government leader, with the perpetrators

reportedly obtaining profits of up to IDR 87 million. The perpetrators created several fake accounts resembling the Governor of East Java, Khofifah Indar Parawansa. They used deepfake technology to manipulate videos and distribute them to the public for fraudulent purposes. Similar methods were also reportedly used by perpetrators who falsely appropriated the identities of the Governors of West Java and Central Java. These phenomena demonstrate the urgency of reformulating or reinterpreting criminal law concepts so that they can accommodate developments in digital technology. Without such reforms, a gap may emerge between legal theory and practical realities, potentially hindering the administration of justice and the protection of society against increasingly complex forms of crime. Therefore, this research aims to critically examine how Indonesian criminal law, particularly the Criminal Code and the ITE Law, regulates, understands, and responds to the use of Artificial Intelligence as a means of committing fraud, as well as to identify forms of criminal responsibility that are relevant to the challenges posed by modern technology.

Based on the foregoing background, the author is interested in conducting a more in-depth study of these issues in a scientific work entitled "Criminal Law Aspects of the Use of Artificial Intelligence (AI) as a Means of Fraudulent Crime from the Perspective of the ITE Law."

Research Methodology

This study employs a normative legal research method, which constitutes a form of doctrinal legal research. The research approaches used are the conceptual approach and the statutory approach. The data used in this study are secondary data, obtained indirectly through library research. The secondary legal materials are divided into several categories, namely primary legal materials, secondary legal materials, and tertiary legal materials.

Primary legal materials are authoritative legal sources that have binding legal force, such as laws and regulations. Secondary and tertiary legal materials serve as supporting sources for primary legal materials, including previous studies that discuss issues relevant to the subject of this research, published scholarly works, and books related to the research topic. The legal materials obtained are subsequently analyzed using a descriptive-qualitative analysis method. This method is employed to formulate scientifically accountable conclusions concerning the comparative analysis of the criminal law aspects of the use of Artificial Intelligence (AI) as a means of committing fraud from the perspective of the Electronic Information and Transactions Law (ITE Law).

Results

1. Forms and Modes of Artificial Intelligence (AI) Use in Fraud Offenses in Indonesia

Artificial Intelligence (AI) is a branch of computer science that aims to develop systems or machines capable of performing functions that normally require human intelligence, including learning, problem-solving, pattern recognition, and decision-making. In the context of cybercrime, AI can be used not only for legitimate purposes but also as a technological instrument to facilitate fraudulent activities. The development of AI has enabled perpetrators to automate various criminal processes, manipulate digital information, and create highly convincing false identities or communications. Technologies such as deepfake, voice cloning, intelligent chatbots, and natural language processing can therefore be exploited to make fraudulent schemes appear authentic and difficult for victims to identify.

The development of AI has also resulted in different levels of technological capability. Artificial Narrow Intelligence (ANI), for example, is designed to perform specific tasks and is already widely implemented in virtual assistants, recommendation systems, and facial recognition technologies. Artificial General Intelligence (AGI), on the other hand, refers to a prospective form of AI capable of performing intellectual tasks at a level comparable to humans, although it remains largely within the research and development stage. Meanwhile, Artificial Super Intelligence (ASI) refers to a hypothetical form of AI that would exceed human intellectual capabilities. Although AGI and ASI remain largely conceptual, the development of existing AI technologies has already created significant challenges for criminal law enforcement, particularly because AI can increase the speed, scale, and sophistication of fraudulent activities.

The misuse of AI in fraud can take various forms. Deepfake technology can be used to manipulate audio and video so that a person appears to say or do something that never actually occurred. Voice cloning can imitate the voice of a family member, colleague, government official, or other trusted individual and subsequently be used to request money or sensitive information. AI-powered chatbots can impersonate customer service representatives, investment agents, or online sellers and interact with victims automatically. In addition, AI-enhanced phishing can generate highly personalized messages that resemble legitimate communications from banks, ecommerce platforms, or other institutions, thereby increasing the likelihood that victims will provide personal information or transfer funds.

Another form of AI-based fraud involves social engineering and generative AI. AI can analyze information obtained from social media and other digital activities to identify a victim's habits, interests, communication style, and appropriate time of contact. This information may then be used to construct psychologically persuasive approaches designed to manipulate victims into transferring money, disclosing sensitive information, or clicking malicious links. Generative AI can also be used to create fraudulent documents, identification cards, agreements, or transaction receipts that appear authentic. Consequently, the use of AI in fraudulent activities represents an evolving form of digital crime that is increasingly sophisticated and difficult to detect, requiring legal enforcement mechanisms and technological capabilities to adapt to these developments.

2. Indonesian Criminal Law Regulations in Addressing the Use of Artificial Intelligence (AI) as a Means of Fraud from the Perspective of the ITE Law

The development of information and communication technology during the Fourth Industrial Revolution has generated significant innovation based on Artificial Intelligence (AI). AI provides substantial benefits in various sectors, including education, healthcare, finance, and public services. However, technological development also creates opportunities for cybercriminals to exploit AI for unlawful purposes. One of the emerging challenges is the use of AI to conduct fraudulent activities through deepfake videos and audio, fraudulent chatbots, and highly personalized phishing schemes. These methods can appear realistic and convincing, making it increasingly difficult for members of the public to distinguish legitimate communications from fraudulent ones and potentially resulting in material and immaterial losses.

Within the Indonesian legal framework, fraud is regulated through the Indonesian Criminal Code (KUHP) and Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016. Nevertheless, the existing regulations do not specifically regulate the use of AI in fraudulent offenses, particularly with regard to the responsibility of perpetrators, evidentiary mechanisms, and the application of criminal sanctions.

This regulatory situation creates legal challenges concerning the substance of the law, law enforcement, and protection of victims. Therefore, an examination is necessary to determine the extent to which Indonesian criminal law can address fraud involving AI as a means of committing the offense, particularly through the perspective of the ITE Law as one of the principal legal frameworks governing electronic activities in Indonesia.

Fraud committed through electronic media is addressed in Article 28 paragraph (1) of Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016. The provision prohibits every person from intentionally and without authorization disseminating false and misleading information that results in consumer losses in electronic transactions. Article 45A paragraph (1) provides criminal sanctions for violations of this provision, namely imprisonment for a maximum of six years and/or a maximum fine of IDR 1 billion. The provision therefore contains several essential elements, including the dissemination of false and misleading information, intentional conduct without authorization, the occurrence of consumer losses, and the existence of an electronic transaction.

The use of AI in deepfake videos to impersonate government officials, fraudulent chatbots offering fictitious investment products, and AI-based phishing that misleads consumers can be examined within the framework of these provisions. Although AI may be used as a technological instrument, criminal responsibility remains attributable to the human legal subject who controls or utilizes the technology for the commission of the offense. At present, the Indonesian legal framework does not specifically regulate AI-related criminal offenses. Therefore, the development of more comprehensive regulation is necessary, including provisions concerning ethical restrictions on the use of AI for criminal purposes, technological supervision, personal data protection, and sanctions for AI misuse. Although the ITE Law does not explicitly refer to AI, its provisions remain relevant to acts involving false and misleading electronic information generated or disseminated through AI, while future regulatory development may provide greater legal certainty in addressing increasingly complex AI-based crimes.

3. Criminal Liability of Perpetrators in Online Fraud Cases Involving Artificial Intelligence

Criminal liability is an essential concept in criminal law concerning the imposition of legal responsibility upon a person for a criminal act that can be attributed to that person. In general, criminal liability requires the existence of a prohibited act and an element of fault on the part of the perpetrator. Within Indonesian criminal law, the fundamental elements relevant to criminal liability include the existence of a criminal act or *actus reus*, the existence of fault or *mens rea* in the form of intent or negligence, and the absence of grounds for justification or excuse. These requirements are important to ensure that criminal sanctions are imposed only upon persons who can legally be held responsible for the acts committed.

The application of criminal liability becomes more complex when AI is involved in the commission of an online fraud offense. AI-based fraud can operate automatically and on a large scale, allowing perpetrators to send large numbers of fraudulent messages, analyze victim data, personalize communications, and create fabricated audio or visual content. Deepfake technology, for example, can imitate the face or voice of another person, while AI-based systems can create highly convincing digital identities and communications. Such characteristics may make it difficult for victims and law enforcement authorities to identify the actual perpetrator, particularly where

the perpetrator uses overseas servers, proxy networks, or other technological means to conceal digital traces.

The legal basis for imposing criminal liability in online fraud can be found in the Indonesian Criminal Code and the ITE Law. Article 378 of the KUHP regulates fraud involving the use of a false name or status, deceitful means, or a series of false statements to induce another person to surrender property, create a debt, or extinguish a receivable. In the context of online fraud, false digital identities, fake accounts, fraudulent websites, electronic messages, and other digital methods may constitute means through which deception is carried out. In addition, provisions concerning participation and assistance may become relevant where the offense involves several individuals performing different roles, including those who design fraudulent systems, control accounts, provide technological infrastructure, or otherwise facilitate the commission of the offense.

The forms of criminal liability in AI-based online fraud depend on the role, intent, and degree of involvement of the individual concerned. A person who personally designs and operates an AI system for fraudulent purposes and benefits from the proceeds may be regarded as a direct perpetrator. Responsibility may also arise where a person instructs another individual to operate an AI system or acts as the intellectual actor behind a fraudulent scheme. In certain circumstances, liability may also concern individuals who knowingly provide technical assistance or infrastructure for the commission of the offense. Furthermore, issues of negligence may arise where a person fails to exercise the necessary care in controlling an AI system that is subsequently misused for fraudulent activities. Accordingly, although AI may perform an active technological role in the commission of online fraud, AI itself functions as a technological instrument, while criminal responsibility under the existing framework remains focused on the human actors who control, direct, facilitate, or negligently supervise its use.

Conclusion

Based on the results of the research entitled *"Criminal Law Aspects of the Use of Artificial Intelligence (AI) as a Means of Fraud from the Perspective of the Electronic Information and Transactions Law (ITE Law),"* it can be concluded that the use of Artificial Intelligence (AI) as a means of committing fraud presents new challenges for criminal law enforcement in Indonesia. From the perspective of the Electronic Information and Transactions Law (ITE Law), AI-based fraudulent activities may be categorized as violations of Article 28 paragraph (1) and Article 45A paragraph (1) of the ITE Law, which regulate the dissemination of false and misleading information resulting in consumer losses in electronic transactions. AI may be utilized by perpetrators to manipulate information, impersonate other individuals through technologies such as deepfake and voice cloning, or create deceptive communications designed to persuade victims to disclose personal data or conduct transactions that cause losses.

Although the ITE Law does not explicitly regulate the use of AI, the criminal elements contained in the relevant provisions may still serve as a legal basis for prosecuting perpetrators, provided that the elements of intent and resulting losses are established. Nevertheless, the existing legal framework has not yet fully accommodated the complexity of AI-based crimes. Therefore, legal reform and adaptive interpretative approaches by law enforcement authorities are necessary to effectively respond to developments in digital technology. In addition, strengthening digital literacy among the public and enhancing inter-agency cooperation constitute important elements in preventing and addressing fraudulent crimes involving AI.

References

[1] Hamzah, Andi. (2015). *Delik-delik tertentu (speciale delicten) di dalam KUHP* (Edisi Kedua). Jakarta: Sinar Grafika.

[2] Hertini, Mega Fitri, & Sampur Dongan Simamora. (2015). *Hukum pidana dalam bagan*. Pontianak: FH Untan Press.

[3] Kurniarullah, Muhammad Rizki, dkk. (2024). Tinjauan kriminologi terhadap penyalahgunaan artificial intelligence: Deepfake pornografi dan pencurian data pribadi. *Jurnal Ilmiah Wahana Pendidikan*, 10(10), 535. https://doi.org/10.5281/zenodo.11448814

[4] Projodikoro, Wirjono. (2013). *Asas-asas hukum pidana di Indonesia*. Bandung: Refika Aditama.

[5] Qurrahman, Shofika Hardiyanti, Safira Ayunil, & Tsabita Aurelia Rahim. (2024). Kedudukan dan konsep pertanggungjawaban artificial intelegence dalam hukum positif Indonesia. *UNES Law Review*, 6(4), 21–23.

[6] Rahim, Tsabita Aurelia, Safira Ayunil, & Shofika Hardiyanti Qurrahman. (2024). *Kedudukan dan konsep pertanggungjawaban artificial intelegence dalam hukum positif Indonesia*. *UNES Law Review*, 6(4), 21–23.

[7] Rahmayanti. (2020). *Analisis yuridis terhadap pertanggungjawaban pelaku tindak pidana korupsi yang dilakukan secara bersama-sama*. *Jurnal Cahaya Keadilan*, 8(1).

[8] Rahmayanti. (2024). *Legal measures to overcome the crime of money laundering committed by the Indonesian National Army (TNI). Journal of International Islamic Law, Human Rights and Public Policy*, 2(2).

[9] Rahmayanti, & Ismaidar. (2023). *Perlindungan hukum terhadap anak sebagai korban kekerasan dalam rumah tangga*. Medan: CV Eureka Media Aksara.

[10] Ravizki, Eka Nanda, & Lintang Yudhantaka. (2022). *Artificial intelligence sebagai subjek hukum: Tinjauan konseptual dan tantangan pengaturan di Indonesia*. *Notaire*, 5(3).

[11] Simamora, Sampur Dongan, & Mega Fitri Hertini. (2015). *Hukum pidana dalam bagan*. Pontianak: FH Untan Press.

[12] Siregar, Mhd Azhali. (2023). *Menelusuri perjalanan lahirnya konsep sistem hukum pidana dan hukum pidana di Indonesia*. Medan: CV Tahta Media Group.

[13] Siregar, Mhd Azhali. (2024). *Integration of restorative justice in medical dispute resolution as a reform to the Indonesian criminal law system*. *International Journal of Synergy in Law, Criminal, and Justice (IJSLCJ)*, 1(2), 285–291.

[14] Syafrida. (2021). *Metode penelitian hukum*. Repository Universitas Medan Area.

[15] Verihubs. (2025). *Deepfake di Indonesia: Prabowo dan Jokowi jadi korbannya*. Diakses pada 15 Juni 2025, dari Verihubs

[16] Waluyo, Bambang. (2019). *Viktimologi: Perlindungan korban & saksi* (Cetakan I). Jakarta: Sinar Grafika.

[17] Yurizal. (2018). *Penegakan hukum tindak pidana cyber crime di Indonesia* (Cetakan I). MNC.