Criminal Legal Aspects Of The Use Of Artificial Intelligence (AI) As A Means Of Fraud From The Perspective Of ITE Law

Rudi Salam Tarigan [*1] **Mhd. Azhali Siregar** [*2] **Rahmayanti** [*3]
[123] Universitas Pembangunan Panca Budi
E-mail: tariganrudi21@gmail.com, azhalisiregar@dosen.pancabudi.ac.id, Rahmayanti@dosen.pancabudi.ac.id

Article Info
Article History
Received: 2025-08-25
Revised: 2025-08-29
Published: 2025-09-10

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

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 of the study 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 defraud. Furthermore, 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 in detecting and handling cybercrimes involving AI.

I. INTRODUCTION

The development of digital technology in the Industrial Revolution 4.0 era has brought rapid progress in the field of artificial intelligence (AI). This technology enables machines or computer systems to perform tasks that previously required human intelligence, such as recognizing faces, understanding language, making decisions, and generating new content that closely resembles human creation. AI has become an integral part of modern society and makes significant contributions to the economic, education, health, communications, and security sectors. However, along with its benefits, AI also brings new, complex challenges and risks, particularly in the legal and security aspects.

One phenomenon that deserves attention is the misuse of AI technology as a tool to commit crimes, particularly fraud. In this context, AI is not merely used as a supporting tool but has transformed into a primary instrument in carrying out criminal modus operandi. For example, fraudsters can use deepfakes to fake videos of the faces or voices of public figures to persuade or deceive victims; use AI-based chatbots to mimic human communication in phishing or fraudulent investment schemes; and even apply natural language processing techniques to craft highly persuasive fraudulent emails that are difficult to distinguish from genuine messages.

This phenomenon raises new concerns in law enforcement practices. Fraud committed with the help of AI has specific characteristics: it is sophisticated, difficult to detect, can be carried out across jurisdictions, and often leaves no clear digital footprint. In fact, in some cases, perpetrators can completely disguise their identities behind automated AI systems, thus complicating the process of identification and proof in court. In Indonesia, fraud is generally regulated by Article 378 of the Criminal Code, which is a product of Dutch colonial law from 1918. Meanwhile, Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), which was updated through Law No. 19 of 2016, serves as the legal basis for ensnaring perpetrators of crimes using electronic media and digital systems. However, neither the Criminal Code nor the ITE Law explicitly regulates or anticipates the development of AI technology as a means or subject of criminal acts. As a result, there is a potential legal vacuum and legal uncertainty in handling cases of AI-based fraud.

Important questions arise: Can AI be classified as a tool in a criminal act, like a weapon or other means in conventional criminal law? How can the concept of mens rea (evil intent) be applied if some actions are carried out automatically by a machine? Who can be held criminally responsible when AI acts on orders, under training, or even autonomously? And is the current Indonesian criminal law system sufficiently adaptive and progressive to face these challenges? The regulatory gap and limited positive legal instruments are urgent matters that cannot be ignored. On the other hand, the development of criminal law must be able to keep up with the dynamics of technology, so as not to be left behind and continue to guarantee legal protection for the public. Therefore, an in-depth legal study is needed regarding the criminal law aspects of the use of Artificial Intelligence in fraud crimes, 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 the public from all forms of detrimental acts, including fraud. The Criminal Code (KUHP), as Indonesia's positive criminal law, regulates fraud through Article 378, which emphasizes the element of trickery or a series of lies to obtain unlawful benefits. In addition, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), which was updated through Law Number 19 of 2016, provides an additional legal basis for ensnaring fraud crimes committed through electronic media. However, in practice, developments in information technology, particularly Artificial Intelligence (AI), have created significant legal loopholes. AI technology enables criminals to commit fraud in highly sophisticated ways, such as through the use of deepfakes, voice cloning, automated chatbots, and other digital data manipulation. These tools are capable of deceiving victims more convincingly, even on a wider scale and in a very short time.

Problems arise when existing legal theories are insufficiently adaptive to these new methods. Neither the Criminal Code nor the Electronic Information and Transactions Law explicitly regulate the use of AI in fraud crimes, resulting in weak enforcement or even legal confusion. For example, in some cases, law enforcement officials have struggled to prove intent and the role of human perpetrators when AI is used as the primary tool of a crime. Yet, in classical criminal law theory, criminal liability is directed at human legal subjects, not technological entities. This situation demonstrates a discrepancy between prevailing criminal law theory and criminal practice in practice. Criminal theory emphasizes responsibility on human actors and the element of will, while in practice, AI can operate automatically or semi-autonomously based on algorithms without direct intervention. This raises fundamental questions: who should be held responsible when crimes are committed by self-operating tools? How can law enforcement officials identify and prove criminal acts committed through AI?

One example of the use of Artificial Intelligence (AI) as a means of fraud occurred in Indonesia, specifically in January 2025, a case of Indonesian deepfake-based fraud occurred, causing losses of up to tens of millions of rupiah. The modus operandi of this crime was a manipulative video showing President Prabowo Subianto as if announcing a financial assistance program from the government, which read: "Assalamualaikum, people of Indonesia, as President of Indonesia, I want to share with people in need. This is official from me personally, I will send each family Rp. 50 million, you must be honest about what it is for," said the voice heard in the video. In reality, Prabowo never made such a statement.

The perpetrator, identified as AMA, included a telephone number in the video and asked the victims to transfer money as an initial administration fee. The requested amount varied, ranging from Rp 250,000 to Rp 1 million. After receiving the payment, the perpetrator disappeared without providing any assistance. After an investigation, AMA was arrested at his home in Central Lampung, Lampung Province, on January 16, 2025. He was charged with the Electronic Information and Transactions Law (UU ITE) and Article 51 Paragraph 1 in conjunction with Article 35 of Law Number 1 of 2024. The law is a revision of Law No. 11 of 2008 concerning ITE.

If found guilty, AMA faces a maximum prison sentence of 12 years and a fine of up to IDR 12 billion. Another example is in East Java, where the East Java Regional Police uncovered a case of AI deepfake fraud involving regional heads, with the perpetrators pocketing profits of up to IDR 87 million. The perpetrators created several fake accounts impersonating the Governor of East Java, Khofifah Indar Parawansa. They utilized deepfake technology to manipulate videos and distribute them to the public with the aim of defrauding. In addition to the Governor of East Java, a similar method was also used to impersonate the

Governor of West Java and the Governor of Central Java.

This phenomenon demonstrates the urgency of updating or reinterpreting criminal law concepts to accommodate the development of digital technology. Without such updates, a gap between theory and practice will emerge, hampering the process of justice and protecting the public from new and increasingly complex forms of crime. Therefore, this study aims to critically examine how Indonesian criminal law, specifically the Criminal Code (KUHP) and the Electronic Information and Transactions (ITE) Law, regulates, understands, and responds to the use of Artificial Intelligence as a means of fraud, and to explore forms of criminal accountability relevant to the challenges of modern technology.

Based on the background description above, the author is interested in studying and understanding more deeply about this problem in a scientific work in the form of a thesis with the title "Criminal Law Aspects of the Use of Artificial Intelligence (AI) as a Means of Fraud Crimes from the Perspective of the ITE Law"

From the background above, the author formulates the problem as follows:

1) What are the forms and modus operandi of using Artificial Intelligence (AI) in fraud crimes in Indonesia?
2) How Does Indonesian Criminal Law Arrange to Address the Use of Artificial Intelligence (AI) as a Means of Fraud Crimes in Indonesia Fraud in the Perspective of the ITE Law?
3) What is the Criminal Liability of Perpetrators in Online Fraud Cases Involving Artificial Intelligence Assistance?

II. RESEARCH METHODS

This study uses a normative legal research method, which is part of the doctrinal research typology. The research approach employed is a conceptual and legislative approach. The data sources obtained in this study are secondary data obtained indirectly through literature studies and secondary data. These data are divided into several sections: primary legal materials, secondary legal materials, and tertiary legal materials.

Primary legal materials are data that have legal force such as statutory regulations, while secondary and tertiary legal materials are supporting data on primary legal materials such as previous studies that discuss the research being written and those that have been published and related books. The legal materials that have been obtained are then analyzed using descriptive-qualitative analysis to obtain conclusions that can be scientifically accounted for regarding the comparative analysis of the Criminal Law Aspects of the Use of Artificial Intelligence (AI) as a Means of Fraud Crimes in the Perspective of the ITE Law.

III. RESULTS AND DISCUSSION

A. Form and Modus Operandi of Use*Artificial Intelligence*(AI) In Fraud Crimes in Indonesia

a. Understanding Artificial Intelligence (AI)

Artificial Intelligence(AI) or artificial intelligence is a branch of computer science that aims to create systems or machines that are able to imitate human intelligence, such as learning, solving problems, recognizing patterns, and making decisions. In the context of cybercrime, AI is often used to automate and refine fraud methods, including in the form of data manipulation, deepfakes, voice cloning, and social engineering. Meanwhile, John McCarthy, known as one of the pioneers of AI, defines AI as "the science and engineering of making intelligent machines, especially intelligent computer programs." In a simple context, AI can be understood as a technology designed to imitate human thought processes, including learning, reasoning, and decision-making, both independently and through interaction with users.

AI is generally divided into three main categories based on its capabilities:

1) *Artificial Narrow Intelligence*(ANI)
   AI is designed to perform a specific task, such as virtual assistants (Siri, Alexa), recommendation systems, and facial recognition. ANI is already widely used today.
2) *Artificial General Intelligence*(AGI)
   AI that has the ability to think and learn on par with humans. AGI is still in the research stage and has not yet been widely used.
3) *Artificial Super Intelligence*(breast milk)
   A future form of AI that surpasses human intelligence, ASI remains speculative and subject to ethical and legal debate.

Several studies have shown that AI can be a very dangerous tool if it falls into the wrong hands. In their report, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," they state that AI can be used to expand the reach and scale of digital crimes, such as:

1) Automated phishing that is difficult to distinguish from genuine communications.
2) Deepfake to spread false information.
3) Voice cloning for identity fraud.
4) Intelligent chatbot based fraud.

b. Forms and Modes of AI Use in Fraud Crimes

Artificial Intelligence (AI) not only brings benefits to society but also poses new challenges due to its frequent misuse in fraudulent activities. Its use patterns are increasingly diverse, ranging from audio and video manipulation, voice imitation, the use of fraudulent chatbots, AI-enhanced phishing, and social engineering based on victim data analysis. Generative AI is now even capable of generating fake documents that resemble official documents. This phenomenon demonstrates that digital crime is evolving in line with technological advances. Although Indonesian positive law does not specifically regulate the use of AI, law enforcement can still be carried out through general criminal law instruments and cyber law. This underscores the need for regulatory updates and increased capacity of law enforcement officers to be able to deal with increasingly sophisticated crime modes.

Table of Forms and Modes of Using AI in Fraud

Form	Explanation	Example of Mode / Case
Deepfake (Audio & Video Manipulation)	AI creates fake audio/video content that resembles a specific person. It's used to mimic the face/voice of a famous figure or someone close to the victim.	Deepfake video of a boss requesting an urgent funds transfer.
Voice Cloning	AI mimics a person's voice with just a short recording. The perpetrator can then call the victim as if they were a family member.	The caller pretended to be a child who had been in an accident and asked for hospital bills.
Fraudulent Chatbots (AI-Based Chatbots)	AI is used for automated, responsive, and convincing chat.	Chatbots pretend to be customer service or investment agents to trick victims into providing personal/payment data.
AI-Enhanced Phishing	AI composes personal, convincing, and linguistically neat emails/messages.	Fake emails from banks/e-commerce request account verification to steal victim's login data.
AI-Based Social Engineering	AI analyzes the victim's social media data to design a psychological approach, such as contact time or language style.	Victims are manipulated into voluntarily providing sensitive data or making money transfers.
Fraud with Generative AI (Fake Documents/Evidence)	AI creates fake documents: ID cards, driving licenses, agreements, proof of transfer.	Deceiving officials/victims with fake documents as if they were genuine.

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

The development of information and communication technology in the era of the industrial revolution 4.0 has given birth to various innovations based on artificial intelligence (AI). This technology has had a positive impact on many aspects of life, from education, health, finance, to public services. However, on the other hand, this technological advancement has also created new loopholes that cybercriminals exploit to commit digital-based fraud. One of the biggest challenges currently faced is the emergence of new fraud modes carried out by exploiting the sophistication of AI, such as the use of deepfake videos and voices, fraudulent chatbots (scam bots), and phishing personalized by intelligent algorithms. These crimes are very difficult for the general public to recognize because they appear

realistic and convincing, so that many victims are deceived and suffer both material and immaterial losses.

In the legal context in Indonesia, the crime of fraud has been regulated in the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) which has been updated by Law No. 19 of 2016. However, these regulations have not specifically addressed the issue of fraud committed through AI systems, both in terms of the perpetrator's responsibility, proof, and punishment. The absence of specific regulations governing the misuse of AI in criminal acts raises its own legal issues, both in terms of legal substance, law enforcement, and protection of victims. Therefore, an in-depth review is needed regarding the extent to which Indonesian criminal law is able to address fraud crimes that use AI as a means, especially from the perspective of the ITE Law as the basis for national cyber law.

Fraud using electronic media is regulated in: Article 28 paragraph (1) of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law No. 19 of 2016, which reads: "Any person who intentionally and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions." Article 45 A paragraph (1) states the sanctions: "Any person who intentionally and without the right to spread false and misleading news as referred to in Article 28 paragraph (1) shall be punished with imprisonment of a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00."

This article contains the core elements of digital fraud, namely:

a. The act of spreading false and misleading news,
b. Done intentionally and without rights,
c. Resulting in consumer losses,
d. Occurs in the context of electronic transactions.

The use of AI in deepfake videos to fake the identities of officials, fake chatbots offering fictitious investment products, or AI-based phishing campaigns to mislead consumers falls within the scope of this article. Even if the perpetrator uses an AI tool, legal responsibility remains with the human legal entity controlling it. Indonesia currently lacks specific legislation governing AI-related crimes. Therefore, it is necessary to formulate a Draft Artificial Intelligence Law that regulates:

a. Ethics and prohibitions on using AI for crime.
b. AI technology oversight standards.
c. Protection of personal data from AI-based systems.
d. Criminal sanctions for misuse of AI.

The sophistication of AI in supporting human life is undeniable, but its misuse for fraudulent acts poses a real threat. The Indonesian criminal law system, through the Criminal Code (KUHP) and the Electronic Information and Transactions (ITE) Law, has provided a normative basis for combating these crimes. However, more specific legal reforms, strengthened digital law enforcement, and comprehensive regulations regarding AI are still needed to address future challenges. Although the ITE Law does not explicitly mention AI, the legal substance in the articles above covers elements of fraud committed through AI systems, including spreading lies, misleading the public, and manipulating electronic information. Therefore, the ITE Law remains a relevant and applicable legal framework for combating AI-based fraudulent crimes, although more comprehensive regulatory reforms are needed in the future.

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

Criminal liability is a fundamental concept of criminal law that asserts that a person can only be punished if they meet the requirements of an unlawful act (actus reus), fault or malicious intent (mens rea), and the absence of justification or excusal. This principle is intended to maintain justice, provide a deterrent effect, and ensure that only those who deserve to be punished are punished.

In the context of AI-based online fraud, the methods used are far more sophisticated than conventional fraud. AI enables large-scale automation, personalized messages, the use of deepfakes, and highly targeted spear phishing. Fake digital identities and the difficulty of tracking perpetrators add to the complexity of these crimes.

The legal basis for prosecuting online fraudsters is already in place, although it does not specifically mention AI. The Criminal Code, through Article 378, regulates fraud in general, while Article 55 provides scope for action not only against the main perpetrator but also against any parties who participate or assist. Furthermore, the ITE Law specifically regulates fraud in the

realm of electronic transactions through Article 28 paragraph (1) and Article 45A, with the threat of imprisonment of up to 6 years and a fine of up to 1 billion rupiah.

Criminal liability for perpetrators involving AI can range from the direct perpetrator who designed and operated the system, the instigator or intellectual actor, the assistant who provided the means, to the negligent supervising party. In certain circumstances, vicarious liability can even apply if a superior fails to prevent a subordinate from misusing AI. Essentially, even though AI plays an active role, it is merely a tool, and legal responsibility remains with humans as legal subjects.

Sub-Topic Summary Table

Sub-Topic	Essence	Example / Relevance
Understanding Criminal Responsibility	A person can be convicted if there is actus reus, mens rea, and no justification/excuse. The goal is to maintain justice and provide a deterrent effect.	Perpetrators who are aware of committing fraud remain responsible.
Characteristics of AI-Based Online Fraud	More sophisticated methods: large-scale automation, personalized messages, deepfakes, spear phishing, and fake digital identities. These are difficult to detect and track.	Fake chatbots, voice cloning, fake social media accounts.
Legal basis	Criminal Code Article 378 (fraud), Article 55 (involvement), and ITE Law Article 28 paragraph (1) and Article 45A (electronic fraud).	Phishing emails, fake accounts, misleading electronic transactions.
Form of Accountability	Dader (direct perpetrator), doenpleger (orderer), medepleger (assistant), culpa (negligent), to vicarious (indirect).	Programmers, server providers, managers who neglect to supervise subordinates.

IV. CONCLUSIONS AND RECOMMENDATIONS

Based on the results of research related to "Criminal Law Aspects of the Use of Artificial Intelligence (AI) as a Means of Fraud Crimes from the Perspective of the ITE Law", the following conclusions can be drawn:

The use of Artificial Intelligence (AI) as a means of fraudulent crimes poses new challenges in criminal law enforcement in Indonesia. From the perspective of the Electronic Information and Transactions Law (ITE Law), AI-based fraudulent acts can be categorized as a violation of Article 28 paragraph (1) and Article 45A paragraph (1) of the ITE Law, which regulates the dissemination of false and misleading information that is detrimental to consumers in electronic transactions. AI can be used by perpetrators to manipulate information, impersonate other parties (deepfake, voice clone), or create false communications that convince victims to hand over personal data or carry out detrimental transactions. Although the ITE Law does not explicitly mention the use of AI, the criminal elements in these articles can still be used as a basis for ensnaring perpetrators, as long as the elements of intent and the losses incurred are met. However, existing regulations are not yet fully able to accommodate the complexity of AI-based crimes. Therefore, legal updates and interpretative approaches are needed by law enforcement officials to be able to respond to developments in digital technology effectively. In addition, strengthening public digital literacy and collaboration between institutions are also important elements in preventing and overcoming fraudulent crimes that use AI as a tool.

SUGGESTION

1. The government should immediately update and harmonize regulations related to digital technology, particularly the use of Artificial Intelligence (AI), to prevent the misuse of AI as a means of fraud. Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE) and its amendments require special emphasis

or additional legal norms related to AI-based cybercrime.

2. Law enforcement, particularly the police and prosecutors, should develop adaptive legal interpretations of the articles in the ITE Law to be able to address AI-based digital crimes. For example, Article 28 paragraph (1) of the ITE Law concerning misleading information can be used to ensnare perpetrators who use AI in deepfake-based fraud schemes or intelligent chatbots.
3. The government, along with legislative bodies and academics, is advised to begin formulating a draft special criminal law on Information Technology and Artificial Intelligence, which includes substantive, procedural, and institutional criminal provisions for addressing AI-based cybercrimes. This is crucial to avoid a legal vacuum in the future.

REFERENCE LISTAN

Ayunil Qurrahman, and Rahim, Jakarta, "The Position and Concept of Accountability of Artificial Intelligence in Indonesian Positive Law.", Gramedia

Asman, 2019. Electronic Transaction-Based Fraud Crimes, Guepedia, 2019 Edition Bambang Waluyo, Victimology: Protection of Victims & Witnesses, Sinar Grafika, 1st Edition, Jakarta

The East Java Regional Police and Communications Agency (Diskominfo) uncover a case of AI deepfake fraud involving a regional head. The perpetrator pocketed profits of up to IDR 87 million. Accessed via https://kominfo.jatimprov.go.id/berita/poldajatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87- juta, June 15, 2025, at 11:00 a.m. WIB.

Eka Nanda Ravizki and Lintang Yudhantaka, "Artificial Intelligence as a Legal Subject: Conceptual Review and Regulatory Challenges in Indonesia," Notaire 5, no. 3 (October 31, 2022).

Hamzah Andi, 2015, Certain Offenses (Speciale Delicten) in the Criminal Code, Second Edition, Sinar Grafika, Jakarta

Muhammad Rizki Kurniarullah et al., "Criminological Review of Artificial Intelligence Abuse: Deepfake Pornography and Personal Data Theft," Wahana Pendidikan Scientific Journal 10, no. 10 (June 3, 2024): 535,https://doi.org/10.5281/zenodo.11448814.

Mhd Azhali Siregar, 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) Volume I, Number II, September 2024 (285-291).

Mhd Azhali Siregar, Tracing the Journey of the Birth of the Concept of the Criminal Law System and Criminal Law in Indonesia, Cv Tahta Media Group, Medan, 2023, p. 44.

Projodikoro Wirjono, 2013, Principles of Criminal Law in Indonesia, Refika Aditama, Bandung

Rahmayanti, Juridical Analysis of the Accountability of Perpetrators of Corruption Crimes Carried Out Jointly, Cahaya Keadilan Journal Volume 8 Number 1 April 2020 ISSN: 2339-1693.

Rahmayanti, 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 https://jishup.org| PT. Radja Intercontinental Publishing Volume 2 No. 2 (2024).

Rahmayanti, Ismaidar, 2023, Legal Protection for Children as Victims of Domestic Violence, Cv. Eureka Media Aksara, Medan, p. 44.

Shofika Hardiyanti Qurrahman, Safira Ayunil, and Tsabita Aurelia Rahim, "The Position

and Concept of Accountability of Artificial Intelligence in Indonesian Positive Law," UNES Law Review 6, no. 4 (June 2024), p. 21.

Syafrida, 2021, Legal Research Methods, Medan Area University Repsytory

Sampur Dongan Simamora & Mega Fitri Hertini, 2015, Criminal Law in the Chart, FH Untan Press, Pontianak

Verihubs, Deepfake in Indonesia: Prabowo and Jokowi are the Victims, accessed via https://verihubs.com/blog/kasus-deepfake-indonesia, June 15, 2025 at 11:00 WIB.

Yurizal, 2018, Law Enforcement of Cyber Crime in Indonesia, MNC, First Edition, Medan.