RECHTENSTUDENT JOURNAL
Volume 7 Number (2) August 2026, pp. 129-138
DOI: https://doi.org/10.35719/rch.v7i2.413
Published by the UIN KHAS Jember, Indonesia
Available online 1 August 2026
ISSN: 2723-0406 | E-ISSN: 2775-5304

Legal Certainty of Criminal Responsibility for Artificial Intelligence Scam through Electronic Communications in Indonesia

Nabila Fajrin*
University of Jember, Indonesia
Ade Irma Suryani
University of Jember, Indonesia
Dominikus Rato
University of Jember, Indonesia
Y.A Triana Ohoiwutun
University of Jember, Indonesia
Corresponding Author's Email: nnabila004@gmail.com

Article	Abstract
How to cite: Nabila Fajrin, et al., **'Legal Certainty of Criminal Responsibility for Artificial Intelligence Scam through Electronic Communications in Indonesia'** (2026) Vol. 7 No. 2 Rechtenstudent Journal Sharia Faculty of KH Achmad Siddiq Jember State Islamic University. **DOI:** 10.35719/rch.v7i2.413 **Article History:** Submitted: 08/03/2026 Reviewed: 15/03/2026 Revised: 08/04/2026 Accepted: 19/04/2026 **ISSN:** **2723-0406 (printed)** **E-ISSN:** **2775-5304 (online)**	Sexual violence, particularly sexual intercourse with children, is a serious crime that causes deep trauma, material and immaterial losses, and threatens the victim's future. In 2024, Indonesia recorded 8,674 cases. Children, as the weaker party, often become targets, so perpetrators are frequently given severe punishments, including the death penalty. In Islamic law, sexual intercourse with children is equated with the crime of *hirabah* because it forcibly violates a child's honor; therefore, harsh punishment, including death, is considered consistent with *maqashid shariah* in protecting religion, life, intellect, lineage, and property. This study examines the urgency of the death penalty for perpetrators of sexual intercourse with children, the characteristics of this crime, and the future concept of capital punishment within the framework of *maqashid shariah*. Using a normative juridical method with statutory, conceptual, case, and comparative approaches, the study finds that such acts violate the protection of life, intellect, and lineage, and therefore the death penalty is considered legitimate as protection, prevention, and public benefit, in line with Indonesian law and as a deterrent to this extraordinary crime. **Keywords:** *Artificial Intelligence, Legal Certainty, Criminal Liability.* **Abstrak** Kekerasan seksual, khususnya hubungan seksual dengan anak-anak, adalah kejahatan serius yang menyebabkan trauma mendalam, kerugian materiil dan non-materiil, serta mengancam masa depan korban. Pada tahun 2024, Indonesia mencatat 8.674 kasus. Anak-anak, sebagai pihak yang lebih lemah, sering menjadi sasaran, sehingga pelaku sering diberi hukuman berat, termasuk hukuman mati. Dalam hukum Islam, hubungan seksual dengan anak-anak disamakan dengan kejahatan hirabah karena secara paksa melanggar kehormatan anak; oleh karena itu, hukuman berat, termasuk hukuman mati, dianggap sesuai dengan maqashid syariah dalam melindungi agama, kehidupan, akal budi, keturunan, dan harta benda. Studi ini meneliti urgensi hukuman mati bagi pelaku hubungan seksual dengan anak-anak, karakteristik kejahatan ini, dan konsep hukuman mati di masa depan dalam kerangka maqashid syariah. Dengan menggunakan metode yuridis normatif dengan pendekatan hukum, konseptual, kasus, dan komparatif, penelitian ini menemukan bahwa tindakan tersebut melanggar perlindungan terhadap kehidupan, akal budi, dan keturunan, dan oleh karena itu hukuman mati dianggap sah sebagai bentuk perlindungan, pencegahan, dan kepentingan umum, sejalan dengan hukum Indonesia dan sebagai pencegah terhadap kejahatan luar biasa ini.

Kata Kunci: *Artificial Intelligence, Kepastian Hukum, Pertanggungjawaban Pidana.*

Introduction

Current technological developments have brought significant changes to social, economic, and legal aspects. One of the most noticeable technological developments is the use of Artificial Intelligence, hereinafter abbreviated as AI. AI is a technology found in computer systems. This technology is capable of developing systems and machines that are typically performed by human intelligence. AI is a field of science that involves several disciplines and aims to automate tasks that require human intelligence. With AI, humans and machines can collaborate in making decisions that are less influenced by personal values.[1] Currently, AI is increasingly sophisticated and is already being used in various fields such as public services, industry, healthcare, and the security sector. However, this technological development also opens up opportunities for new crime modes, one example being fraud or scams that use AI technology through electronic communication media.

Crimes that exploit AI typically involve perpetrators using deepfakes to deceive victims by conducting video calls with faked faces or voices. Perpetrators use AI to impersonate public figures or people close to the victim, thus inducing trust and then willingly providing personal data or transferring funds. For example, in the case of the "Prabowo & Sri Mulyani" Deepfake Video for Social Assistance Fraud, a man in Lampung with the initials JS used a deepfake video resembling President Prabowo Subianto and Finance Minister Sri Mulyani. The video was edited to appear as if they were offering social assistance.[2] Korban yang tertarik lalu diminta mentransfer sejumlah uang sebagai biaya Assistance registration administration. Then, a video uploaded to the TikTok account @/depianadepi showed a fraudulent video call using AI, depicting Raffi Ahmad. In the video, the fraudster impersonated Raffi Ahmad and claimed the woman had received Rp. 100,000,000 (one hundred million rupiah).

AI fraud operates by using artificial intelligence to copy a person's voice. Using machine learning algorithms, it's very easy for fraudsters to mimic a person's voice, making the fake call appear real. Fraudsters exploit this technology to trick victims into providing sensitive information or sending money.[3]

From a criminal law perspective, the crime of fraud through electronic communications is regulated in Law Number 1 of 2023 concerning the Criminal Code (hereinafter abbreviated as the KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter abbreviated as the ITE Law), and Law Number 27 of 2022 concerning Personal Data Protection (hereinafter abbreviated as the PDP Law). However, these regulations are often considered inadequate to address the increasingly complex challenges posed by AI technology. The main issues that arise relate to legal certainty and criminal liability, both for perpetrators who utilize AI and for the platforms or systems that enable these crimes.

---

[1] Afifah Ayu Nurjannah & Herry Liyus, "Perlindungan Hukum Bagi Korban Penyalahgunaan Artificial Intelligence (AI) Terhadap Serangan Malware dalam Perspektif Peraturan Perundang Undangan", *PAMPAS: Journal of Criminal Law*, Vol. 6, No. 2 (2025): 232-233.

[2] Shela Octavia &Ardito Ramadhan, "Warga Lampung Ditangkap akibat Sebar Video "Deepfake" Prabowo untuk Penipuan", Compas.com, 2025.

[3] David Jeremy Lengkey, Altje Agustin Musa, dan Ronald Elrik Rorie, "Kajian Hukum Mengenai Pertanggungjawaban Pidana oleh Pelaku Penipuan Melalui Media Komunikasi Seluler," *Lex Privatum: Jurnal Fakultas Hukum Unsrat* Vol. 15, No. 5 (2025),. 2

Therefore, it is important to conduct a more in-depth study of how the Indonesian criminal law system responds to crimes involving AI, as well as how legal guarantees can be applied to prosecute perpetrators and prevent the recurrence of similar crimes in the future.

Research Method

This research falls under normative legal research, focusing on applicable legal norms and serving as the primary basis for analyzing the issues discussed.

The approach employed consists of several components: a statutory approach and a conceptual approach, which analyzes legal principles and theories. The analytical technique employed is qualitative analysis, interpreting and constructing the meaning of positive legal provisions and then connecting them with relevant legal theories and principles to obtain a comprehensive answer to the problem under study.

Result and Discussion

Legal Regulations in Indonesia Regarding AI-Based Scam Crimes Through Electronic Communications

The phenomenon of AI-based scams, one of the loopholes of current technological advancements, involves using deepfakes to deceive victims with false identities. Deepfakes are a combination of "deep learning" and "fake" videos, involving digitally altering videos to create hyperrealistic depictions of individuals saying and doing things that never actually happened.[4] Misuse of deepfakes can cause various legal problems such as fraudulent theft, easy dissemination of fake news, the risk of personal data leaks, violation of user privacy, and various other problems that can harm and endanger society.[5]

In this context, legal regulations governing the protection of personal data and electronic information are crucial as a tool to prevent and address crimes involving AI technology. Several Indonesian regulations have already established laws that can be used to address this issue, including the Criminal Code, the Electronic Information and Transactions Law, and the Privacy and Personal Data Protection Law.

Digital Fraud from the Criminal Code Perspective

Regarding AI-based scams, Article 492 of the Criminal Code regulates classic fraud, but this article remains relevant to addressing digital fraud by using a broader approach to the elements contained in the article. With a more detailed explanation[6]:

Elements of Article 492	AI Based Scam
"Any individual who aims to gain profit for himself or others by breaking the law"	The perpetrator used AI to trick the victim into getting money by requesting a transfer.

[4] Sami Alanazi & Seemal Asif, "Exploring deepfake technology: creation, consequences and countermeasures", *Human Intelligent Systems Integratio***n**, (2024), 49.

[5] Silvia Mah arani Iskandar Putri, Nashwa Salsabila, & Asmak UI Hosnah, "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum", *Jurnal Hukum Legalita*, Vol. 6, No. 2 (2024), 84.

[6] Law Number 1 of 2023 concerning the Criminal Code, Article 492.

"Using a fake identity or incorrect status"	The perpetrator fakes his face and voice, for example claiming to be the president, artist or public figure.
"Taking advantage of deception and falsehood"	Using sentences that victims will receive social assistance, gifts, and so on via AI-based video calls.
"Encourage others to give something, provide a loan, make a statement of debt, or cancel a debt obligation."	The victim gave money and personal data because the victim believed the perpetrator who claimed to be the president, artist or public figure.

Based on the explanation above, it can be concluded that the elements of Article 492 of the Criminal Code regarding AI-based scams have been fulfilled because this action is classified as an act of fraud based on the Criminal Code even though it is carried out digitally.

ITE Law: Manipulation of Electronic Information

AI-based scams, because they utilize technology to commit crimes, fall under the realm of cybercrime, and the ITE Law provides legal certainty for addressing crimes in the digital space. Cybercrime encompasses various ways of using computer networks, information systems, and digital technology to commit crimes that can harm individuals, groups, organizations, or the state.[7]

Article 28 paragraph 1 of the ITE Law explains that any individual who intentionally disseminates electronic information containing false news or false information that results in consumer losses in electronic transactions.[8] AI-based scams meet all the requirements because the perpetrators spread false information via video calls or electronic media to deceive consumers into believing in social assistance or prizes, resulting in the loss of money or personal data.

AI-based scams also violate Article 35 of the Electronic Information and Transactions (ITE) Law, which defines any individual who intentionally violates the law by manipulating electronic information or electronic documents with the intention of making the information appear to be true,[9] Because AI-based scammers fake their digital identities by using the faces or voices of officials, celebrities, or public figures to pretend they're real. The perpetrators' goal is to convince victims that their identities and information are genuine.

PDP Law: Privacy Violations & Data Falsification

The Personal Data Protection Law (PDP) is a tool to protect the public's digital rights in this AI-based scam, as the perpetrators have illegally used victims' personal data. The data frequently misused includes ID card numbers, contact information and addresses, photos or videos on social media, and facial and voice recordings. These personal data violations

[7] Yoan Shevila Kristiyenda, Jasmine Faradila, Christina Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang", *ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 3 No. 2 (2025), 150.

[8] Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Article 28 paragraph 1.

[9] Law Number 11 of 2008 concerning Electronic Information and Transactions, Article 35

demonstrate the weakness of digital security systems and leave users feeling unable to engage in digital activities due to perceived privacy threats.[10]

Article 65 paragraph 1 explains that every individual who illegally collects other people's personal data with the aim of benefiting themselves or another party which could be detrimental to the subject of the personal data.[11] AI-based scams often begin with the perpetrator illegally collecting other people's personal data, such as facial, voice, or phone number data, from social media, through hacking, or other illegal means, harming the victims whose personal data is misused.

Article 65 paragraph 3 also states that no individual is permitted to use another person's data illegally.[12] In the context of AI-based scams, perpetrators use the faces and voices of officials, celebrities, or public figures to deceive victims into thinking they are the ones contacting them. The perpetrators also misuse the victim's phone number, which constitutes the illegal use of another person's personal data. Article 66 of the PDP Law also stipulates that individuals are prohibited from falsifying their personal data for the purpose of benefiting themselves or another party, or harming othersAI-based scams fulfill this element because the perpetrators pretend to be officials, celebrities, or other figures to obtain money transfers from victims.

AI-based scam perpetrators can be punished under Article 67 paragraph 1, which states that individuals who illegally collect another person's personal data for the purpose of benefiting themselves or another party, which could be detrimental to the personal data subject as referred to in Article 65 paragraph 1, shall be subject to a maximum imprisonment of 5 years and/or a maximum fine of 5 billion rupiah.[13]

For perpetrators of AI-based scams, they can also be punished based on Article 67 paragraph 3, namely every individual who uses other people's data illegally as per Article 65 paragraph 3 shall be punished with a maximum of 5 years imprisonment and/or a maximum fine of 5 billion rupiah.[14] The criminal penalty for perpetrators of AI-based scams based on Article 68 is that every individual who intentionally falsifies his/her personal data with the aim of benefiting himself/herself or another party that is detrimental to other people in accordance with what is meant by Article 66 shall be punished with a maximum prison sentence of 6 years and/or a maximum fine of 6 billion rupiah.

Legal Certainty Regarding the Accountability of AI Scam Perpetrators Through Electronic Communications

According to Radbruch, legal certainty is defined as a condition in which the law can function as a regulation that must be obeyed. The law's role is to create legal certainty because it aims to create order in society.[15] Legal certainty essentially guarantees that applicable regulations can be used as a guideline for action. Legal certainty in criminal law enforcement

---

[10] Noval bin usman & Satria Unggul Wicaksana Prakasa, "Perlindungan Hukum Data Pribadi dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP", *Doktrina : Journal of Law*, Vol. 7, No. 2 (2024), 179-180.

[11] Law Number 27 of 2022 concerning Protection of Personal Data, Article 65 paragraph 1.

[12] Law Number 27 of 2022 concerning Protection of Personal Data, Article 65 paragraph 3.

[13] Law Number 27 of 2022 concerning Protection of Personal Data, Article 67 paragraph 1.

[14] Law Number 27 of 2022 concerning Protection of Personal Data, Article 67 paragraph 3.

[15] Siti Halilah, "Asas Kepastian Hukum Menurut Para Ahli," *Siyasah: Jurnal Hukum Tata Negara*, Vol. 4, No. 2, (2021), 60.

requires that every act deemed unlawful be accompanied by a clear legal basis, so that criminal liability is imposed only on those who are legally capable of being held responsible and are truly guilty of their actions.

Criminal liability in Dutch is called torekenbaarheid, while in English it is called criminal responsibility or criminal liability. Criminal liability is the imposition of punishment for an act that violates a prohibition or creates a prohibited situation. Criminal liability therefore involves the process of transferring the punishment for a criminal act to the perpetrator.[16] Moeljatno stated that criminal responsibility is not sufficient if a criminal act is committed, but in addition there must be a mistake, or an attitude of mind that can be blamed, it also turns out that in the unwritten legal principle there is no punishment if there is no mistake (green straf zonder schuld, ohne schuld keine strafe).[17] The elements contained in criminal responsibility consist of three things, namely:[18]

Able to be responsible

In his book, Amir Ilyas entitled Principles of Criminal Law, explains about being able to be responsible, citing the opinion of E.Y. Kanter and S.R. Sianturi, which consists of elements of mental state and mental ability. Mental state means that the perpetrator is not disturbed by a continuous or temporary illness, is not disabled in growth (mute, idiot, imbecile, and so on), and is not disturbed by shock, hypnotism, overflowing anger, subconscious influence/reflexe bewenging, melindur/slaapwandel, delirium due to fever/koorts, nyidamdan so on. In other words, he is in a conscious state. Meanwhile, mental ability means that the perpetrator can realize the nature of his actions, can determine his will for the action, whether to carry it out or not, and can know the reprehensibility of the action.[19]

Thus, if the condition of the perpetrator in this case is not included in one explanation regarding mental condition and mental abilities being disturbed, then the condition of the perpetrator has fulfilled one of the elements to be responsible for the crime of AI using deepfakes to deceive.

Schuld

A mistake, which in foreign languages is called schuld, is a person's psychological condition related to an action he or she has committed in such a way that based on that condition, the perpetrator can be blamed for his or her actions.[20] According to Moeljatno, a person's mistakes and negligence can be measured by whether the perpetrator of the crime is capable of being responsible, namely if the action contains 4 (four) elements, namely committing a criminal act (unlawful in nature), being over a certain age and capable of being responsible, having a form of error in the form of intent (dolus) and negligence/negligence (culpa), and there is no reason to forgive.[21]

In this case, the perpetrator could be considered a criminal offense for committing fraud by making a video call with a fake face or voice, with the goal of obtaining personal data or obtaining money. Furthermore, such acts are also regulated by Indonesian law.

---

[16] Aryo Fadlian. "Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis," *Jurnal Hukum Positum* Vol. 5, No. 2, (2020) 13.

[17] Moeljatno, *Asas-asas Hukum Pidana*, PT. Rineka Cipta, Jakarta, 1993, 73.

[18] Amir Ilyas, *Asas-asas Hukum Pidana,* Rangkang Education Yogyakarta & PuKAP-Indonesia, Yogyakarta, 2012, 75.

[19] *Ibid*, 76.

[20] Afridus Darto. et. al. "Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pembunuhan Pengidap Gangguan Kejiwaan Dalam Prespektif Hukum Pidana", *jurnal ilmu hukum Wijaya putra,* Vol. 1, No. 2, 2023, 260.

[21] Moeljatno, *op. cit*. h. 164.

Regarding the age of legal responsibility in Indonesia, there are differences, but if according to Article 40 of Law No. 1 of 2023 concerning the Criminal Code (KUHP) it states "Criminal responsibility cannot be imposed on children who at the time of committing a crime were not yet 12 (twelve) years old." If referring to this regulation, then a person can be punished if they are 12 (twelve) years old or older. And if in a deepfake case the perpetrator is 12 (twelve) years old or older, then they can be punished for their actions.

Meanwhile, the ability to take responsibility in this case means that the perpetrator is not in a state of imperfect reason (idiot) or suffering from mental disorders.[22] The element of responsibility means the perpetrator understands the consequences of their actions and has free will in operating the technology. Therefore, the fault in cases of AI scams through electronic communication is not only related to the technical aspects of AI use, but also concerns the perpetrator's legal awareness in using the technology illegally, which harms the victim's rights and interests.

Von Hipel and Simons define intent as intent when someone has the intention to commit the crime and is prepared to bear the consequences.[23] From the intentional (dolus) perspective, the perpetrator consciously designs and uses AI technology with the aim of misleading others and gaining profit. The perpetrator knows that their actions are prohibited and have the potential to harm others, but they still carry them out for personal gain. Meanwhile, negligence (culpa) focuses more on the perpetrator's psychological aspects in carrying out the act.[24] From a negligence (culpa) perspective, an error can arise if the perpetrator fails to control the AI system used, resulting in a loss.

There is also the element of lack of excuse within the element of error, meaning there are no circumstances that can eliminate the perpetrator's guilt even though they have committed a criminal act. Because the perpetrator's actions are regulated by Indonesian regulations, the perpetrator cannot escape responsibility for their actions.

There is no excuse

The absence of a justification (including a justification) as an element of criminal responsibility, which is more appropriately termed the elimination of criminal responsibility. The elimination of criminal responsibility means that the perpetrator is not held responsible.[25] The reason for forgiveness is an exception from criminal liability due to the psychological condition of the perpetrator.[26]

In criminal law, a justification for forgiveness may apply if the perpetrator acted under duress, excessive self-defense, a legitimate official order, or mental disorder. In the case of deepfake fraud, the perpetrator was not under duress, was not defending himself, was not carrying out an official order, and was not insane. Therefore, no circumstances can eliminate his guilt, and in this case, the perpetrator must be held accountable for his actions.

On the other hand, the accountability of Artificial Intelligence (AI)-based scam perpetrators through electronic communication can also be carried out by imposing criminal penalties as stipulated in Law Number 1 of 2023 concerning the Criminal Code (KUHP), Law

---

[22] Vania Sulistiano dan Bambang Arwanto, "Analisis Hukum Mengenai Pertanggungjawaban Pidana Bagi Pembuat Aplikasi Game Online Yang Memuat Unsur Perjudian", *Aladalah*, Vol. 3, No. 2, 2025, 100.

[23] *Ibid*, 100.

[24] *Ibid*, 101.

[25] Yohanis Pasaribu, "Tanggung Jawab Pengemudi Mobil Yang Lalai Dan Akibat Hukumnya Ditinjau Dari Pasal, 359 Dan 360 Kitab Undang-Undang Hukum Pidana", *Lex et Societatis*, Vol. 5, No. 1, 2017, 109.

[26] *Ibid*, h. 109.

Number 1 of 2024 concerning the Second Amendment to Law Number I1 of 2008 concerning Electronic Information and Transactions (ITE Law), and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). One of the rules that ensnare AI scam perpetrators is stated in Article 492 of the Criminal Code, which reads: "Any person who with the intention of unlawfully benefiting himself or another person by using a false name or false position, using trickery or a series of lies, inducing people to hand over goods, giving debt, making acknowledgment of debt, or writing off receivables, shall be punished for fraud, with a maximum imprisonment of 4 (four) years or a maximum fine of the category."

When linked to Artificial Intelligence (AI)-based scams through electronic communications, this article is relevant because perpetrators often use false identities or manipulation to deceive victims. The elements of "trickery" and "a series of lies" in this article can be fulfilled when perpetrators use AI to gain the victim's trust and hand over money or personal data. Therefore, Article 492 of the Criminal Code provides a clear legal basis for prosecuting AI scammers. The article also emphasizes that even though the method uses sophisticated technology, the act is still punishable.

Apart from that, the rules regarding perpetrators of Artificial Intelligence (AI) based scams via Electronic communication are also stated in Article 28 of the ITE Law, which reads: "Any person who intentionally and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that results in material losses for consumers in Electronic Transactions."

The criminal threat from Article 28 of the ITE Law is stated in Article 45A of the ITE Law, which reads: "Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that results in material losses for consumers in Electronic Transactions as referred to in Article 28 paragraph (1) shall be punished with imprisonment of up to 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah)."

If Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) is associated with Artificial Intelligence (AI)-based scam practices through electronic communication, then the act has fulfilled the elements of disseminating misleading information that causes harm. Thus, the existence of Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) provides legal certainty that even though the fraud method is carried out using artificial intelligence, criminal responsibility still attaches to humans as legal subjects who control or utilize the technology. This is in line with the objective of the ITE Law, which is to provide legal protection to the public from the harmful misuse of information technology.

The rules regarding perpetrators of Artificial Intelligence (AI)-based scams through electronic communication are also stipulated in Article 66 of the PDP Law, which states: "Every person is prohibited from creating false Personal Data or falsifying Personal Data with the intention of harming themselves or others that could result in harm to others.."

Criminal liability is regulated in Article 68 of the Privacy and Personal Data Law, which states: "Any person who intentionally creates false Personal Data or falsifies Personal Data with the intent to benefit themselves or another person, which may result in harm to that person as referred to in Article 66, shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 6,000,000,000.00 (six billion rupiah)."

When linked to perpetrators of AI scams through electronic communications, Article 68 of the Privacy and Personal Data Law becomes relevant when the scam is carried out by an individual or business entity that utilizes AI technology to unlawfully obtain, use, or disseminate the victim's personal data. Article 68 of the Privacy and Personal Data Law provides legal certainty that misuse of personal data through AI scams not only ensnares individual perpetrators but can also implicate corporations that systematically use the technology for unlawful purposes.

The creation of the aforementioned laws is essentially aimed at providing legal certainty for the public. If someone persists in committing an act prohibited by law, they must be held legally accountable for their actions. Criminal liability for AI scammers is upheld based on the principle of no crime without fault (Geen Straf Zonder Schuld). This means that a person will not be punished unless it can be proven that their actions are prohibited by law.[27]

In cases of AI-based scams through electronic communications, perpetrators who intentionally design, operate, or utilize AI systems to commit fraud through electronic communications can still be held accountable. The use of AI does not eliminate human error, as AI is merely a tool (instrument) controlled by the perpetrator. With the enactment of Law Number 1 of 2023 concerning the Criminal Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number I1 of 2008 concerning Electronic Information and Transactions (UU ITE), and Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), this certainly provides legal certainty for perpetrators of AI-based scams through electronic communications.

Conclusion

Indonesia's legal framework for AI-based scams through electronic communications has a strong foundation under the Criminal Code (KUHP), the Electronic Information and Transactions (ITE) Law, and the Personal Data Protection (PDP) Law. Although these crimes utilize modern technology such as deepfakes, the element of fraud as outlined in Article 492 of the Criminal Code remains intact, as the perpetrators use false identities to unlawfully obtain profits. Furthermore, the ITE Law provides legal certainty against the manipulation and dissemination of false electronic information, while the PDP Law strengthens protection of victims' personal data and digital privacy. Thus, these three complementary legal instruments are capable of ensnaring perpetrators of AI-based scams, while also demonstrating the state's responsibility to provide legal certainty and protection for the public in the digital age.

Legal certainty regarding the accountability of perpetrators of AI-based scams through electronic communications confirms that the use of technology does not eliminate human error. Perpetrators can still be held criminally responsible for knowingly and intentionally violating the law. With the new Criminal Code, the ITE Law, and the Privacy and Privacy Law, the law provides a clear basis for prosecuting perpetrators and guarantees protection for the public from the misuse of AI technology.

Bibiliography

Book

Ilyas, Amir. *Asas-Asas Hukum Pidana*. Yogyakarta: Rangkang Education & PuKAP-Indonesia, 2012.

Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: PT Rineka Cipta, 1993.

[27] Ahda Muttaqin. et. al. *Telaah Asas Geen Straf Zonder Schuld terhadap Pertanggungjawaban Pidana Penipuan melalui Modus Ritual*. University of Bengkulu Law Journal, Vol. 8, No. 1, 2023, h. 37.

Journal Articles

Alanazi, Sami, dan Seemal Asif. "Exploring Deepfake Technology: Creation, Consequences and Countermeasures." *Human Intelligent Systems Integration* (2024).

Darto, Afridus, et al. "Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana Pembunuhan Pengidap Gangguan Kejiwaan dalam Perspektif Hukum Pidana." *Jurnal Ilmu Hukum Wijaya Putra* 1, no. 2 (2023).

Fadlian, Aryo. "Pertanggungjawaban Pidana dalam Suatu Kerangka Teoritis." *Jurnal Hukum Positum* 5, no. 2 (2020).

Halilah, Siti. "Asas Kepastian Hukum Menurut Para Ahli." *Siyasah: Jurnal Hukum Tata Negara* 4, no. 2 (2021).

Iskandar Putri, Silvia Maharani, Nashwa Salsabila, dan Asmak Ul Hosnah. "Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum." *Jurnal Hukum Legalita* 6, no. 2 (2024).

Kristiyenda, Yoan Shevila, Jasmine Faradila, dan Christina Basanova. "Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang." *Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora* 3, no. 2 (2025).

Lengkey, David Jeremy, Altje Agustin Musa, dan Ronald Elrik Rorie. "Kajian Hukum Mengenai Pertanggungjawaban Pidana oleh Pelaku Penipuan melalui Media Komunikasi Seluler." *Lex Privatum* 15, no. 5 (2025).

Muttaqin, Ahda, et al. "Telaah Asas *Geen Straf Zonder Schuld* terhadap Pertanggungjawaban Pidana Penipuan melalui Modus Ritual." *University of Bengkulu Law Journal* 8, no. 1 (2023).

Nurjannah, Afifah Ayu, dan Herry Liyus. "Perlindungan Hukum bagi Korban Penyalahgunaan Artificial Intelligence (AI) terhadap Serangan Malware dalam Perspektif Peraturan Perundang-Undangan." *PAMPAS: Journal of Criminal Law* 6, no. 2 (2025).

Pasaribu, Yohanis. "Tanggung Jawab Pengemudi Mobil yang Lalai dan Akibat Hukumnya Ditinjau dari Pasal 359 dan 360 Kitab Undang-Undang Hukum Pidana." *Lex et Societatis* 5, no. 1 (2017).

Sulistiano, Vania, dan Bambang Arwanto. "Analisis Hukum Mengenai Pertanggungjawaban Pidana bagi Pembuat Aplikasi Game Online yang Memuat Unsur Perjudian." *Al-Adalah* 3, no. 2 (2025).

Usman, Noval bin, dan Satria Unggul Wicaksana Prakasa. "Perlindungan Hukum Data Pribadi dan Pertanggungjawaban Otoritas terhadap Keamanan Siber Menurut Tinjauan UU PDP." *Doktrina: Journal of Law* 7, no. 2 (2024).