Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volumes 6 No. 4 (2026)

LEGAL ANALYSIS OF CRIMINAL RESPONSIBILITY FOR PERPETRATORS OF MISUSE OF FACIAL AND VOICE FORGERY TECHNOLOGY IN CYBER FRAUD CRIMES IN INDONESIA

Arnold Anugerah Maharatino[1], Rizky Setyobowo Sagalang[2], Eny Susilowati[2], Aris Toteles[4]
[1,2,3] Universitas Palangka Raya, Indonesia
Email : rizkisetyobowo@law.upr.ac.id[2], enysusilowati.plk78@gmail.com[3], aristoteler@law.upr.ac.id[4]

Received	: 20 March 2026	Accepted	: 17 April 2026
Revised	: 30 March 2026	Published	: 16 May 2026

Abstract

This study aims to analyze the forms of criminal liability for the misuse of *deepfake technology* in cyber fraud crimes in Indonesia. The widespread use of *deepfakes* in the context of fraud raises legal issues because it touches on aspects of information authenticity, identity, and victim protection. The research method used is normative juridical with a statutory, conceptual, and case-based approach. The results show that the misuse of *deepfakes* can be qualified as a criminal act of fraud under Article 378 of the Criminal Code, and can be prosecuted under the provisions of Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments. Criminal liability of the perpetrator is based on intent, the use of digital media as a means, and the occurrence of harm to the victim. In conclusion, existing regulations still have legal gaps specifically regarding *deepfakes* , so normative reforms are needed to strengthen legal certainty and protect the public.

Keywords: Criminal Liability, Deepfake , Cyber Fraud, Criminal Law, It.

A. INTRODUCTION

1.1. Background of the Problem

In the digital era entering ERA 4.0, technological development is so rapid that the development of crime will experience a renewal of types of crime motives. Currently, the hottest crime mode is the use of AI, or Artificial Intelligence, technology. Artificial Intelligence (AI) is the science and engineering to create intelligence in machines, especially intelligence in computer programs. However, as time goes by, AI technology is also increasingly developing and can mimic human intelligence through data processing, speech recognition, and vision. The term AI was first popularly coined by a computer scientist named John McCarthy in 1956. At that time, he argued that AI technology, as machine intelligence, should be able to be used to understand human intelligence. [1]This development can be misused in criminal acts. One example of a case is the Social Assistance Fraud Case Using Deepfake technology videos that used the face and voice of President Prabowo Subianto and other government officials. In the video, AI Deepfake Prabowo Subianto stated that they were providing free social assistance on the condition that prospective recipients must submit their ID cards and family cards. The video successfully deceived 100 people from 20 provinces.[2]

According to Tempo, the suspect, identified as JS, has successfully ensnared approximately 100 people from 20 provinces, with the majority coming from East Java, Central Java, and Papua. This raises concerns about Artificial Intelligence technology, which could help humans solve unimaginable problems, becoming a new tool for fraud. Before going deeper, we need to know first what Artificial Intelligence is? Artificial Intelligence (AI) is a multidisciplinary field that aims to automate activities that require human intelligence, where artificial intelligence and humans can work together in making decisions that are less influenced by personal values. Abuse of *Artificial Intelligence* (AI) has various types, including: *carding* (stealing other people's credit card numbers), *defacing* (redirecting the original website to another website), *hacking* and *cracking* (entering someone else's computer or

[1]Fathia Nurul Haq, 2023, *AI Technology and Its Benefits in Using AI Technology* , https://pluang.com/id/pwa/blog/news-analysis/ai-adalah , accessed September 13, 2025,
At 13:40 WIB.

[2]Alfitriana Nefi, 2025, Social Assistance Fraud Case Using Deepfake Videos, Public Considered Not Yet Recognizing This Mode, There Are 11 Victims in the Deepfake Video Fraud Case of Prabowo and Other Public Figures | tempo.co , accessed September 13, 2025, at 1:52 PM WIB.

electronic system without permission), *phishing* (fraud on websites that have names that are almost similar to the original website), *malware* (malicious programs or *software* that infiltrate computers or *systems* on computers), spamming (sending news repeatedly), and many more forms of crime that can be accessed through the sophistication *of Artificial Intelligence* (AI).[3]Abuse of *Artificial Intelligence* (AI) has various types, including: carding (stealing other people's credit card numbers), defacing (redirecting the original *website* to another *website), hacking and cracking* (entering another person's computer or electronic system without permission), *phishing* (fraud on *websites* that have names that are almost similar to the original *website), malware* (malicious programs or *software* that infiltrate computers or computer systems), *spamming* (sending news repeatedly), and many other forms of crime that can be accessed through the sophistication of Artificial Intelligence (AI).

The misuse of *Artificial Intelligence* (AI) in Indonesia has become a concern for the government and various stakeholders, particularly regarding how regulations governing the use of *Artificial Intelligence* (AI) are still limited and have not been specifically regulated regarding the potential dangers of the misuse of *Artificial Intelligence* (AI) to human rights. Artificial Intelligence *(* AI) is currently classified as an "Electronic Agent" as regulated in Article 1 Number 8 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Article 1 Number 8 of Law Number 19 of 2016 concerning Electronic Information and Transactions classifies *Artificial Intelligence* (AI) as an Electronic Agent because AI has the ability to automate the process of retrieving information and system devices that are capable of performing every action on electronic information automatically and in an organized manner.

deepfake phenomenon has also garnered global attention. For example, in 2019, a UK energy company *CEO was duped by a deepfake -based phone call* impersonating his boss, resulting in losses of approximately €220,000. This case demonstrates that *deepfake -based crimes* not only cause financial losses but also threaten public trust in the authenticity of digital information. In Indonesia, legal loopholes related to *deepfakes* remain wide open, as existing regulations do not explicitly address the misuse of this technology. This contrasts with several countries, such as China and South Korea, which have enacted specific regulations regarding the distribution and creation of deepfake content. Therefore, this research is important for analyzing the forms of criminal liability that can be imposed, while also contributing to the development of Indonesian law to be more adaptive to technological developments.[4]

Based on the background of the problems described above, the author is interested in raising the title " **JURIDICAL ANALYSIS OF CRIMINAL RESPONSIBILITY AGAINST PERPETRATORS OF DEEPFAKE TECHNOLOGY MISUSE IN CYBER FRAUD CRIMES IN INDONESIA".**

1.2. PROBLEM FORMULATION

Based on the description of the background of the problem above, the author can formulate the problem as follows:

1. *deepfake* technology abuse in fraud crimes in Indonesia?
2. How are the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE) adequate in regulating the misuse of *deepfakes* in fraud crimes?

METHOD

Research Methodology

In an effort to resolve the issue of fraud using Deepfake technology, the author employed a normative juridical research method. The research was conducted by examining primary legal materials, including the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, as well as secondary legal materials, including literature, scientific articles, and relevant academic perspectives. Tertiary legal materials, such as legal dictionaries and legal encyclopedias, were used as supporting materials. The approaches used are legislative and conceptual. The legislative approach is used to examine the extent to which the provisions of the Criminal Code and the Electronic Information and Transactions Law (UU ITE) can regulate the misuse of deepfake technology in fraud crimes. Meanwhile, the conceptual approach is used to examine criminal law doctrine and theory in relation to the development of artificial intelligence technology, as well as to analyze the urgency of establishing specific legislation regarding AI and the adequacy of existing regulations.

[3]Afifah Ayu Nurjanah, Herry Liyus, 2025, Legal Protection for Victims of Artificial Intelligence (Ai) Abuse Against Malware Attacks from the Perspective of Legislation, *Legal Protection for Victims of Artificial Intelligence* (Ai) Abuse Against Malware Attacks in the Perspective of Legislation.pdf , 20:17 WIB.

[4]*iZOOlogic , 2020, Voice Phishing to scam $243000 out of a UK energy firm* , accessed 22 September 2025, at 13:21 WIB.

Type of Research

The type of research used is normative legal research, with a focus on examining applicable laws and regulations relevant to the problem.

Research Approach

In this research, several approaches were used, namely:

- **Statute approach:** to examine the provisions in **the Criminal Code** , **the ITE Law** , and other laws relevant to the misuse of *deepfakes* .
- **Conceptual approach:** by referring to doctrine, criminal theory, and criminal responsibility theory that have developed in criminal law.
- **Case approach:** by analyzing examples of *deepfake cases* in Indonesia and abroad as comparative material for the application of norms.

Legal Materials

- **Primary legal materials:** Criminal Code, Law Number 11 of 2008 concerning Electronic Information and Transactions and other related regulations.
- **Secondary legal materials:** books, literature, legal journals, scientific articles, and the views of criminal law experts regarding cybercrime and *deepfakes* .
- **Tertiary legal materials:** legal dictionaries, legal encyclopedias, and other supporting sources that provide additional understanding.
- **Legal Material Collection Techniques**
  The technique used is library research *by* examining laws and regulations, doctrines and legal literature.
- **Legal Material Analysis**
  Legal materials are analyzed using a descriptive-analytical method, namely systematically describing the applicable legal regulations, then analyzing them with criminal theory and criminal responsibility theory to find legal conformity or gaps related to the *deepfake phenomenon.*

DISCUSSION

The Concept of Deepfake Technology and Its Characteristics

Deepfake is a controversial form of *Artificial Intelligence (AI) due to its ability to create fake content that appears incredibly realistic. The term is derived from a combination of the words "deep learning"* and *"fake* ." So, *a deepfake* is essentially the manipulation of images, videos, or audio using AI algorithms to appear authentic.[5]

The term deepfake itself emerged around 2017 on the Reddit forum, when an anonymous user with the handle *"Deepfakes"* uploaded a video of celebrity faces manipulated into explicit content. From there, the term spread widely, and the technology began to gain public awareness. Initially *, deepfakes were primarily used for entertainment, parody, or creative experimentation, but concerns quickly arose about their misuse. As deepfake* -making software became more accessible, even people without technical expertise could create fake videos with just a few steps. From this point on, deepfakes began to enter the realm of cyber fraud.[6] *deepfake* use in cyberfraud began to become apparent around 2018–2019. One highly publicized case occurred in Europe in 2019, when an energy company CEO received a phone call with a voice that sounded remarkably like his boss at the parent company. The fake voice, generated using *deepfake* audio technology, asked him to transfer over two hundred thousand euros to a specific account. Because the instructions sounded convincing, he followed them, and the money disappeared. This case served as early evidence that deepfakes were not just a reputational threat, but also a viable tool for financial crime. Since then, reports of deepfake-based fraud have become increasingly common, ranging from investment scams involving fake videos of company executives to personal blackmail using manipulated videos of victims' faces.

[5]Marsha Bremanda, Yudha Pratomo, 2025, What Is Deepfake? Explanation, Meaning of Deepfake, and the Dangers of This Technology, https://tekno.kompas.com/read/2025/06/30/19030077/apa-itu-deepfake-penjelasan-arti-deepfake-dan-bahaya-teknologi-ini , accessed September 25, 2025, at 4:28 PM WIB.

[6]Muhammad Afif , 2025, **Deepfake Cybercrime in the Era of Artificial Intelligence,** https://marinews.mahkamahagung.go.id/artikel/kejahatan-siber-deepfake-di-era-kecerdasan-buatan-0hb , accessed September 25, 2025, at 16:39 WIB

As it has evolved, *deepfakes* are no longer used solely to imitate a person's voice or face in business contexts, but also in broader fraud schemes. For example, in modern phishing practices, fraudsters no longer rely solely on fake emails but also include authentic-looking voice recordings or videos to convince victims. There have also been cases where a person's face has been superimposed onto an indecent video for blackmail purposes, a form of crime known as *sextortion.* Even in the political realm, deepfakes are used to spread disinformation, create false narratives, and manipulate public opinion. All of this shows that since their inception, deepfakes have evolved from a mere technological experiment into a dangerous cyber fraud tool.

Definition of Cybercrime According to Indonesian Law

In the Indonesian legal system, cybercrime does not yet have an explicit definition in legislation. However, an understanding of cybercrime can be traced back to Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which was amended by *Law* No. 19 of 2016. The ITE Law serves as the primary basis for handling crimes involving information and communication technology. Cybercrimes in the ITE Law can be classified into two broad categories. The first category includes crimes targeting the technology itself, such as hacking (Article 30), illegal interception (Article 31 paragraphs 1 and 2), website defacement (Article 32), electronic data theft (Article 32 paragraph 2), system interference (Article 33), facilitation of criminal acts (Article 34), and digital identity theft (Article 35). These crimes are considered contemporary crimes stemming from the development of digital technology and are not yet recognized in conventional criminal law. The second category includes crimes that use technology to disseminate illegal content, such as pornography (Article 27 paragraph 1), gambling (Article 27 paragraph 2), defamation (Article 27 paragraph 3), extortion (Article 27 paragraph 4), consumer fraud (Article 28 paragraph 1), hate speech (Article 28 paragraph 2), and threats of violence (Article 29).[7] Crimes in this category are actually old forms of crime modified through digital media. Therefore, the ITE Law has redefined these crimes to accommodate technological and social media developments. In practice, violations of the ITE Law mostly occur in the form of publishing and distributing illegal content through social media and other digital platforms.

Meanwhile, according to Josua Sitompul in his review in Hukumonline, cybercrime broadly encompasses all crimes committed using electronic systems. This means that even conventional crimes such as murder or human trafficking can be categorized as cybercrimes if committed through digital means. Therefore, the definition of cybercrime in Indonesian law is dynamic and contextual, depending on the means and objects used in the crime.[8] The position *of deepfakes* within the category of cybercrime under Indonesian law can be explained as the misuse of artificial intelligence technology to produce or manipulate visual and audio content that imitates a person's identity in a highly realistic manner, thereby causing legal harm to dignity, privacy, and the public interest. In the construction of criminal law, *deepfakes* are viewed through two lenses simultaneously: as objects of criminal acts (when the content itself violates moral norms, damages reputation, deceives, or causes harm) and as tools or means *used* by perpetrators to commit other cybercrimes recognized by positive law. This "dual" conception aligns with law enforcement practices in Indonesia that prosecute *deepfakes* based on existing norms, particularly the ITE Law and the Pornography Law, while recognizing the absence of *lex specialis* that explicitly regulates AI technology, so that *deepfakes* are placed within the framework of cybercrimes that utilize electronic systems for unlawful purposes.

Theory of Criminal Acts and Criminal Responsibility

Theory of Criminal Acts

A crime is an act that meets the elements specified in criminal law and can be subject to sanctions by the state. ***According to Moeljatno, a crime is an act prohibited by a legal regulation, a prohibition accompanied by the threat of punishment for those who violate it*** .[9]

In the case of cyber fraud that uses deepfake technology to manipulatively portray public figures such as Prabowo Subianto in a video promising free social assistance, the perpetrator has carried out a series of lies and deceptions that fulfill the elements of the crime of fraud as regulated in:

[7] Vidya Prahassacitta, 2019, The Concept of Cybercrime in the Indonesian Legal System, https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/ , accessed September 26, 2025, at 13:01 WIB.

[8]Josua Sitompul, 2018, Legal Basis for Handling Cybercrime in Indonesia, https://www.hukumonline.com/klinik/a/landasan-hukum-penanganan-icybercrime-i-di-indonesia-cl5960/ , accessed September 26, 2025, at 1:30 PM WIB

[9]Moeljatno. Principles of Criminal Law. Volume 1 Jakarta: Rineka Cipta, 2002, p. 54.

• Article 378 of the Criminal Code: "Anyone who, with the intention of unlawfully benefiting himself or another person, by using a false name or false dignity, by means of deception, or a series of lies, induces another person to hand over something to him, or to grant a loan or write off a debt, is threatened with a maximum prison sentence of four years for fraud."

The use of *deepfakes* to create false images is a highly complex form of digital deception. Perpetrators leverage technology to deceive the public by spreading false information purportedly from official figures, thus inducing victims to provide personal data or engage in harmful behavior.

Apart from the Criminal Code, this act also violates the provisions in:

• Article 35 of the ITE Law:

"Any person who intentionally and without authority manipulates, creates, changes, deletes and/or destroys electronic information and/or electronic documents with the aim of making the electronic information and/or electronic documents appear to be authentic data."

Article 66 of the PDP Law:

"Everyone is prohibited from falsifying Personal Data with the intention of benefiting themselves or others which could result in harm to others."

Article 68 of the PDP Law:

"Regulates criminal sanctions for falsifying personal data. Perpetrators who intentionally create false or fabricated data for personal or other gain are subject to a maximum prison sentence of six years and/or a maximum fine of IDR 6 billion. Furthermore, perpetrators of falsifying personal data may be subject to additional penalties, such as confiscation of profits or compensation to the victim."

Theory of Criminal Responsibility

Criminal liability concerns whether the perpetrator can be held responsible for the crime they committed. In Indonesian criminal law, criminal liability requires fault, either intentional (*dolus*) or negligence (*culpa*).

Simons states that **errors (*schuld*)** consist of:

1. **Ability to take responsibility** ,
2. **Intentional or negligent** ,
3. **There is no reason to delete the error** .

According to Simons, without these three elements, a person **cannot be punished** , even if his actions fulfill the elements of a crime.

Van Hamel states that criminal responsibility is moral and legal responsibility for unlawful acts committed with free will.

In this case, the perpetrator knowingly and deliberately created deepfake content with the intention of deceiving the public. The element of intent is clearly evident, as the perpetrator knew the content was fake and continued to distribute it for profit. Therefore, the perpetrator qualifies for criminal liability.

Criminal liability may also be imposed on parties involved in the production, distribution or promotion of such content, in accordance with:

• Article 55 of the Criminal Code:

"Those who commit, who order to commit, and who participate in committing acts, shall be punished as perpetrators of a criminal act."

• Article 56 of the Criminal Code:

"Convicted as an accessory to a crime:

a. those who intentionally provide assistance at the time the crime is committed;
b. those who intentionally provide the opportunity, means or information to commit a crime."

In the context of cybercrime, criminal liability can also be extended to corporations or groups that systematically use technology for criminal purposes, in accordance with the principle of *corporate criminal liability* that is beginning to be recognized in modern criminal law practice.

Urgency Regarding the Regulation of the Law on *Artificial Intelligence* in the Case of Prabowo Subianto's Deepfake Fraud Crime

Regarding the Prabowo Subianto case, in the context of the fraud case using *deepfake technology* that impersonated President Prabowo to promise free social assistance, Indonesia desperately needs a specific law on *Artificial Intelligence* (AI). Currently, the legal instruments used still rely on the Criminal Code and the Electronic Information and Transactions Law, which are general in nature and do not specifically regulate the misuse of AI.

This creates a legal vacuum, as *deepfake technology* is a highly sophisticated form of digital manipulation that is difficult to address with existing legal instruments.

The absence of specific regulations forces law enforcement officials to interpret existing articles extensively, such as Article 492 of the 2023 Criminal Code on fraud or Article 35 of the Electronic Information and Transactions Law (ITE Law) on the dissemination of false information and electronic data manipulation. However, this approach is insufficient to address the complexities of AI-based crimes, particularly when it comes to criminal liability, personal data protection, and the potential involvement of corporations or international networks. With the AI Law, Indonesia could have a clearer legal framework to regulate the ethics, accountability, and limits of AI use, while also providing legal certainty for both the public and technology industry players.

Why is it so important to establish legal regulations regarding AI technology immediately?

Regarding regulations on *Artificial Intelligence,* several countries have already established them, such as China's *EU AI Act* , which was passed in 2024 and will come into effect gradually from 2025 to 2026. [10]It clarifies the levels of risk for AI use, including minimal, limited, and high, and focuses on human rights protection, transparency, and security.[11]

China also has a draft law called *the New Generation AI Development Plan.* And in 2023, the law was officially passed, called *the Measure for the Management of Generation AI Services* . Regulating *Generative AI* requires service providers to conduct security assessments, filter content, and label AI-generated content. The goal of establishing AI Regulation is to maintain national security, social stability, and control over public information.

Of the several countries that have formed and ratified regulations regarding AI by adjusting the needs of the country, Indonesia can also immediately form and ratify the Regulation Law regarding AI. For me, AI itself is not only tools and robots, but they can also slowly have consciousness and even communication between fellow AI exists, and unfortunately it cannot be understood by humans. This has become a concern for me and many people regarding AI.[12]

In Indonesia, this also creates a legal vacuum regarding AI. As of October 2025, Indonesian law does not yet recognize a specific definition of *deepfakes* in legislation; the substance of the offense is still based on acts of "fraud," "spreading false news," "defamation," or "morality," without defining the manipulative nature of AI. As a result:

1. **It is difficult to distinguish AI-manipulative content as a specific crime vs. regular digital media.**
2. **Many articles are open to multiple interpretations and give rise to uncertainty in law enforcement (*legal uncertainty*).**
3. **Perpetrators often exploit legal loopholes *to* escape responsibility.**

This creates challenges in enforcement and proof in court, I give the points as follows:

1. Anonymity and Digital Footprint Engineering: *Deepfake perpetrators* generally operate covertly, using fake accounts, overseas servers, or digital masking techniques, making them difficult for law enforcement to track.
2. Forensic Limitations and Human Resource Capacity: Limited digital forensic infrastructure and the low human resource capacity of the authorities to detect/prove deepfake content exacerbate the slowness in handling this crime.
3. The Difficulty of Proving Intent: The ability of perpetrators to create and distribute *deepfakes* automatically , *especially* in organized crime/ *cybercrime syndicates, makes deepfake* creations and the resulting losses to victims increasingly complex, especially if the distributor or digital platform is only an intermediary.[13]

---

[10] *European Commission* ,2025, *European approaches to artificial intelligence. Retrieved* https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence accessed on October 6, 2025, at 02:30 WIB.

[11]Trisnawati, 2024, *Artificial Intelligence* Governance and Regulation : A Roadmap for Developing Legal Policy for *Artificial Intelligence Applications.* file:///C:/Users/asus71123/Downloads/4+JGAR+Vol+5+No+2++Th+2024+P156-155+-+Trisnawati.pdf , accessed on October 5, 2025, at 22:30 WIB.

[12] *Editors of ScienceNewsToday* , 2025, ***The Secret Language AI Systems Use to Talk to Each Other,*** *Here is a direct link (HTTPS) to the article you requested from* ***the Science News Today website*** , *https://www.sciencenewstoday.org/the-secret-language-ai-systems-use-to-talk-to-each-other* , accessed October 6, 2025, at 7:00 PM WIB

[13] SIP Firm Law, 2025, **Criminal Prosecution for Deepfake Content, New Challenges for Law Enforcement in the AI Era,** https://siplawfirm.id/konten-deepfake/?lang=id , accessed October 7, 2025, at 04:00 WIB

CLOSING

deepfake technology in cybercrime, particularly digital fraud, poses a significant challenge to criminal law in Indonesia. Juridical analysis suggests that such actions constitute fraud under Article 492 of the 2023 Criminal Code and also violate Article 35 of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). Criminal liability for perpetrators is based on the element of intent (*dolus*), because the perpetrators knowingly use *deepfake technology* to deceive the public and obtain unlawful benefits. In addition to individuals, parties who assist or facilitate the creation and distribution of *deepfake content* can also be held accountable under Articles 55 and 56 of the Criminal Code. However, the absence of specific regulations governing the misuse of artificial intelligence (*AI*), such as *deepfakes,* creates a legal vacuum *and* uncertainty in law enforcement. Law enforcement officials still rely on interpretations of general articles in the Criminal Code and the ITE Law, which are not fully able to address the complexity of modern digital crimes. Therefore, Indonesia needs to immediately enact a specific law on *Artificial Intelligence* (AI) that addresses ethics, responsibilities, limitations, and law enforcement mechanisms for the misuse of this technology. Such regulation is crucial for providing legal certainty, protecting the public, and strengthening national legal deterrence against increasingly sophisticated and transnational cybercrime.

REFERENCES

A. Buku

Moeljatno. (2002). Asas-Asas Hukum Pidana (Jilid 1). Jakarta: Rineka Cipta.

Rahardjo, Satjipto.Ilmu Hukum di Tengah Arus Perubahan. Surya Pena Gemilang, 2016.

Raz, Joseph.The Authority of Law. New York, Oxford University Press, 1979.

Royce, Edward. Classical Social Theory and Modern Society: Marx, Durkheim, Weber, Rowman & Littlefield. Lanham–Boulder –New York –London, 2015.

Shklar, Judith N.Legalism: An Essay on Law, Morals and Politics. Cambridge, Massachusetts, Harvard University Press, 1964.

B. Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

UU Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022)

C. Jurnal

Afif, M. (2025). Kejahatan Siber Deepfake di Era Kecerdasan Buatan. Marinews Mahkamah Agung RI. Diakses dari: https://marinews.mahkamahagung.go.id/artikel/kejahatan-siber-deepfake-di-era-kecerdasan-buatan-0hb

Afifah, A. N., & Liyus, H. (2025). Perlindungan Hukum bagi Korban Penyalahgunaan Artificial Intelligence (AI) terhadap Serangan Malware dalam Perspektif Peraturan Perundang-Undangan.

Trisnawati. (2024). Tata Kelola dan Regulasi Artificial Intelligence: Peta Jalan untuk Mengembangkan Kebijakan Hukum untuk Penerapan Artificial Intelligence. Jurnal Governance and Regulation, Vol. 5 No. 2, Hal. 156–155.

D. Artikel Internet

Alfitriana, N. (2025). Kasus Penipuan Bansos Pakai Video Deepfake, Masyarakat Dinilai Belum Kenali Modus Ini. Tempo.co. Diakses dari: https://tempo.co

Editors of Science News Today. (2025). The Secret Language AI Systems Use to Talk to Each Other. ScienceNewsToday.org. Diakses dari: https://www.sciencenewstoday.org/the-secret-language-ai-systems-use-to-talk-to-each-other

European Commission. (2025). European Approach to Artificial Intelligence. Diakses dari: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

Fathia, N. H. (2023). Apa Itu Teknologi AI dan Apa Manfaatnya? Pluang.com. Diakses dari: https://pluang.com/id/pwa/blog/news-analysis/ai-adalah

Josua Sitompul. (2018). Landasan Hukum Penanganan Cybercrime di Indonesia. Hukumonline.com. Diakses dari: https://www.hukumonline.com/klinik/a/landasan-hukum-penanganan-icybercrime-i-di-indonesia-cl5960

Marsha, B., & Pratomo, Y. (2025). Apa Itu Deepfake? Penjelasan, Arti Deepfake, dan Bahaya Teknologi Ini. Kompas.com. Diakses dari : https://tekno.kompas.com/read/2025/06/30/19030077/apa-itu-deepfake-penjelasan-arti-deepfake-dan-bahaya-teknologi-ini

SIP Law Firm. (2025). Pidana atas Konten Deepfake: Tantangan Baru Penegakan Hukum di Era AI. Siplawfirm.id. Diakses dari: https://siplawfirm.id/konten-deepfake/?lang=id

Vidya Prahassacitta. (2019). Konsep Kejahatan Siber dalam Sistem Hukum Indonesia. Binus Business Law. Diakses dari: https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

Ni Kadek Dwi Ika Ardiyani. (2024). *Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif*. Jurnal Kajian Hukum dan Kebijakan Publik. Diakses dari: https://doi.org/10.62379/cs863250