International Journal of Educational Review, Law & Social Sciences (IJERLAS)

International Journal of Educational Review, Law And Social Sciences (IJERLAS Journal) | ISSN (e): 2808-487X
Volumes 5 No. 6 (2025)

POLICY ON THE LEGAL REGULATION OF CRIMINAL ACTS INVOLVING THE MISUSE OF ARTIFICIAL INTELLIGENCE DEEPFAKES

Amalia Andayani Nugraha, Faizin Sulistio, Patricia Audrey Ruslijanto
Master of Law Program, Faculty of Law / Brawijaya University, Malang
Faculty of Law / Universitas Brawijaya, Malang
Faculty of Law / Universitas Brawijaya, Malang
e-mail: amalianugraha@student.ub.ac.id, faizin@ub.ac.id, patricia@ub.ac.id

Received	: 15 September 2025	Published	: 17 November 2025
Revised	: 10 October 2025	DOI	: https://doi.org/10.54443/ijerlas.v5i6.4416
Accepted	: 31 October 2025	Link Publish	: https://radjapublika.com/index.php/IJERLAS

Abstract

The development of artificial intelligence (AI) technology has brought significant advances in various areas of human life, but on the other hand, it has also created new challenges in the legal field, especially through the emergence of deepfake technology. Deepfake technology utilizes AI to manipulate images, videos, and voices of individuals to appear realistic, which in practice is often misused for purposes such as fraud, pornography, spreading hoaxes, and damaging reputations. Indonesia currently has no specific regulations governing the misuse of deepfake technology, so law enforcement still relies on general provisions such as the Criminal Code, the Electronic Information and Transaction Law, the Personal Data Protection Law, and the Sexual Violence Criminal Law. This legal vacuum or incompleteness causes legal uncertainty and potential violations of the principle of legality. Through a criminal law policy approach, adaptive legal reforms are needed to keep pace with developments in digital technology. Efforts that can be made include revising the Electronic Information and Transaction Law as lex specialis that regulates provisions on deepfakes or formulating specific regulations on artificial intelligence (AI) that comprehensively regulate ethical aspects, responsibility, and criminal liability. This policy is expected to provide certainty, justice, and protection of individual rights in facing the legal challenges of the digital era in Indonesia.

Keywords: Artificial Intelligence, Deepfake, Legal Policy

INTRODUCTION

Society continues to evolve along with changes in all aspects of life, including economic, political, legal, social, cultural, and technological dimensions, which continue to move toward progress. One of the things that drives change is innovation in the field of information technology, with many new discoveries aimed at increasing effectiveness and performance. Artificial intelligence technology, hereinafter referred to as AI, has developed in such a way as to facilitate human work. The focus of AI development is based on the paradigm that the future of industry lies in automation.[1] Automation is implemented because many routine tasks that do not require human hard or soft skills can be delegated to AI. Additionally, AI is expected to increase productivity by eliminating human error and physical fatigue, which are inherent weaknesses of humans.

After this AI technology was applied, many negative impacts emerged that were not previously anticipated. Instead of helping humans become more productive and reducing technical work that is less meaningful to humans, AI has become humans' main competitor in obtaining jobs. Now, AI can even perform human jobs that are actually creative, analytical, or managerial in nature. While humans need time, training, and certification to become experts in a field, artificial intelligence can master these skills in a short period of time. On the other hand, there is criticism

[1] Yudo Devianto and Saruni Dwiasnati, Framework of Artificial Intelligence Systems in Improving the Competence of Indonesian Human Resources, InComTech: Journal of Telecommunications and Computers 10, No. 1 (2020), 19–24, http://dx.doi.org/10.22441/incomtech.v10i1.7460

directed at the creative work of AI, which is considered to have limited meaning or to only produce something that is beautiful from an industrial perspective but lacks vision and mission.[2]

Social changes in the field of information technology have led to the emergence of deepfake technology, which is an advancement of AI technology. The function of deepfake is to create a visual illusion that someone is doing something. Deepfake is done by selecting biometric data such as a video of someone speaking, then reconstructing or replacing the face in the video with another person's face by following the facial movements and voice of the person in the original video. The function of deepfake is actually to assist the film industry and other creative works.[3] However, deepfake is often used to commit various crimes, causing concern because it can damage a person's reputation and demean human dignity. Deepfake can have a negative impact because it encourages the emergence of deviations from values and norms in society, which will affect the functioning of the law. Other negative things that can be realized with deepfakes are pornography and fraud. There are even content creators who edit using deepfake technology unwisely for the sake of economic gain and commercialization. In addition to the content creators, those who broadcast the content should also be held accountable for the act of distribution. Although deepfake products that are misused are quickly distributed in the virtual environment, victims often do not realize that their data has been used until someone else informs them.

Private documents such as photos or videos, when uploaded to the internet, open up opportunities for misuse by various parties.[4] Although technology to detect deepfakes has now been developed, preventing the adverse effects of deepfakes is not easy. For example, even when deepfake videos have been widely distributed and official statements have been issued by both the police and the prosecutor's office, this does not prevent people from believing what they see through deepfake technology. The subject who is the source of the data is certainly the party who suffers the loss because their data has been stolen without permission and illegally. Moreover, the content is distributed rapidly.

The Electronic Certification Authority (PSrE) at the Ministry of Communication and Digital Affairs, namely PT Indonesia Digital Identity or VIDA, noted that there was a 1,550% increase in deepfake fraud cases in Indonesia from 2022 to 2023.[5] In just one year, there was a very significant increase. There is an urgent need for legislation to ensure that everyone's rights are protected and to prevent people from becoming victims of deepfakes. Given the current situation, advocacy and public communication approaches are not really suitable as a means of preventing the circulation of deepfakes. A legal approach is considered far more realistic, as it can minimize the negative impact, whereas advocacy, education, and public communication approaches require more time and have yet to deliver the desired results.

In addition, demands for legal change arise when there is a discrepancy between the situation in society and the regulations currently in force. Faced with social change, the product of law in the form of legislation seems slower than the social changes in society, which move more quickly.[6] Legal change can come from two things. First, there are changes in society, and then the law comes to legitimize those changes. Second, the law acts as a means of engineering to lead society in a more positive direction.[7] The relationship with AI technology is more related to the first type because AI technology already exists, and specific regulations in Indonesia are not yet available.

Law as a tool of social engineering views law not as something autonomous but rather as intertwined with other instruments such as culture, economics, religion, and politics.[8] In Indonesia, regulations related to AI deepfake cybercrime are still only regulated in a few regulations but do not yet accommodate increasingly developing and varied criminal acts. Currently, there are no specific provisions addressing this issue. In light of this, the author was motivated to conduct further research through this article entitled "The Political Law of Criminal Regulation of Artificial Intelligence Deepfake Abuse."

---

[2] Sean Cao et al., From Man vs. Machine to Man+ Machine: The Art and AI of Stock Analyses, Journal of Financial Economics 160, 2024, 103910
[3] Md Shohel Rana et al., "Deepfake Detection: A Systematic Literature Review," IEEE Access 10 (2022): 25494–513
[4] Suhendra, Dedy et al. 2024. The Concept of Legal Change in Facing Technological Developments, Muqoddimah Scientific Journal 8 No. 1
[5] "VIDA Records 1,550 Percent Surge in 'Deepfake' Fraud in Indonesia" accessed November 8, 2024, https://www.antaranews.com/berita/4437365/vida-catat-penipuan-deepfake-di-indonesia-melonjak-1550-persen
[6] Kartika, Shahnaz and Nurhayati, Hate Speech on Social Media in the Context of Law and Social Change (Case Study on the Community of Medan City). Mercatoria Journal 16 No.1 (2023): 101-102
[7] Sinaga, Niru Anita, The Readiness of the Indonesian Legal System in the Transformation of Society from 4.0 to 5.0, Krtha Bhayangkara Journal 17 No. 1 (2023): 120, https://doi.org/10.31599/krtha.v17i1.2111
[8] Ridwan. Law and Social Change: A Two-Polar Debate Between Law as Social Control and Law as Social Engineering. 2016. Jurisprudence Journal 6 No. 1

METHOD

This study uses a normative juridical approach with a focus on analyzing positive legal norms that apply in Indonesia and abroad, as well as the need for legal reform in dealing with the misuse of AI technology, especially deepfakes. This research is descriptive and analytical in nature, systematically describing relevant laws and regulations and analyzing their effectiveness in combating criminal acts involving the misuse of deepfakes. The research was conducted by examining the relationship between criminal law political theory, criminal law principles, and their implementation in the context of modern digital technology.

POLITICAL ANALYSIS OF CRIMINAL LAW

According to Sudarto, criminal law policy refers to efforts to establish sound regulations in accordance with current circumstances and situations. He argues that state policy, through authorized bodies, is to establish desirable regulations that are expected to express the values of society and achieve its aspirations.[9] Criminal law policy can basically be understood as a policy approach in the criminal justice system that aims to combat crime.[10] One important aspect of this approach is reflected in efforts to reform criminal law.

The criminal act of deepfake AI abuse is basically covered in the ITE Law and other laws, but due to its development, this criminal act has become more widespread in its modus operandi and has developed faster than the speed of legislative development, so there is no legal definition of deepfake in the regulations currently in force. In addition, law enforcement officials still lack the capacity to understand AI-based electronic evidence in the trial process. This has created an urgent need to reform the law to regulate AI deepfake crimes more specifically.
Basically, according to Gustav Radburch, there are three components that must be fulfilled in order to achieve justice, namely fairness, certainty, and usefulness. Fairness can be understood in several ways:

1. Fairness can be seen as a personal characteristic or trait. This form of subjective justice, also known as secondary justice, reflects a person's attitude, perspective, and beliefs aimed at achieving objective justice, which is considered primary justice;
2. justice derived from positive law and legal ideals; and
3. justice rooted in the principle of equality.[11]

The law is also required to bring benefits because its essence is to ensure the happiness of the people. The law does not arise from a vacuum but rather from the dynamics of human interaction as a response to or solution for the limitations and negative tendencies inherent in human nature. The existence of the state and the legal system is essentially intended to serve the greater good and promote the welfare of the majority. The principle of certainty guarantees that the law is positive, applies with certainty, and must be obeyed by society. This certainty is necessary in order to know what actions are permissible and what are not, as well as to protect against arbitrary actions by the government in enforcing the law. Ideally, every regulation should be certain, without any doubt, and there should be no potential for vague or ambiguous provisions. This is related to the consistency of legal certainty.

As explained above, there is an uncompleted norm that causes a legal vacuum or a lack of laws regulating deepfake crimes. An incomplete norm refers to a legal norm that has deficiencies, which can take the form of a lack of a clear definition of the offense or prohibited acts, a lack of clear criminal sanctions, a lack of clear procedures or mechanisms for law enforcement, and language that is too broad or ambiguous, leading to various interpretations and legal uncertainty. For example, there is no specific definition or legal provision regarding the misuse of deepfakes in the ITE Law, even though there have been many crimes committed using this method. Incomplete norms can lead to a legal vacuum, making it difficult for judges and law enforcement officials to prosecute perpetrators due to the absence of applicable criminal provisions. In addition, there is also the potential for violations of the principle of legality (nullum crimen sine lege), whereby individuals cannot be punished for acts that are not explicitly defined as crimes. Other impacts that may occur are also related to legal uncertainty and the potential for abuse of power. The public does not know clearly what is permissible and what is not, and unclear norms can be exploited by the government as the authority to impose punishment based on subjective interpretation alone.

Criminal law policy plays an important role in developing new legal norms that are clear and comprehensive, minimizing ambiguity and preventing legal loopholes. Enacting responsive and forward-looking laws, especially in relation to technological advances, and encouraging the revision of unclear or incomplete laws is considered

[9] Sudarto. 1983. Criminal Law and Social Development. Bandung: Sinar Baru
[10] Hanafi Amrani. 2019. Politics of Criminal Law Reform. Yogyakarta: UII Press
[11] Dino Rizka Afdhali and Taufiqurrohman Syahuri. 2023. The Ideality of Law Enforcement Reviewed from the Perspective of Legal Purpose Theory. Collegium Studiosum Journal, Vol. 6 No. 2, December 2023

necessary, such as through the revision of the Electronic Information and Transactions Law. In its formulation, criminal law policy must ensure the involvement of experts from multiple disciplines, primarily law, technology, and human rights, in the drafting process to align regulations with the current needs of society.

Currently, the ITE Law does not specifically address deepfake technology, so law enforcement agencies only rely on general provisions such as defamation, articles related to hoaxes, personal data protection, pornography, sexual violence crimes, and fraud. These matters concern the interests of individuals that must be protected by the state. Threats to public order also haunt the life of the nation and state. There are also no regulations regarding whether AI can be considered a legal entity, and what about criminal liability, both for content creators and AI technology developers themselves. This shows that the legal norms are incomplete, because they don't consider key aspects like the role of AI, the intent of the perpetrator, and the scope of digital harm. So, there's an urgent need for progressive legal policies that support the creation of well-defined new criminal norms that are adapted to the realities of the digital age as an effort to maintain national stability.

EVALUATION OF POLICY IMPLEMENTATION

Article 28D of the 1945 Constitution reflects the state's guarantee of recognition, protection, and certainty of fair law, as well as the guarantee of equal treatment before the law for everyone. In its implementation, there are several positive laws that can be used as a reference for enforcement in dealing with deepfake cases. First, of course, is the latest Criminal Code, which is embodied in Law Number 1 of 2023, which includes discussions on defamation and libel through social media, namely in Articles 310 and 311. In addition, there are also other positive laws that can be used as a reference, namely Law Law Number 1 of 2024 concerning Electronic Information and Transactions in Article 27 paragraph 1, which states that there are prohibitions and penalties for anyone who deliberately and without rights broadcasts, displays, distributes, transmits, and/or makes accessible electronic information and/or electronic documents that contain content that violates decency for public knowledge.

Next is the Personal Data Protection Law contained in Law Number 27 of 2022, namely Article 65, which states that personal data may not be used outside the interests of the owner of the personal data and that there are clear restrictions on how personal data may be used. Personal data may not be used for purposes that are against the law, including defamation or character assassination. Furthermore, Law Number 12 of 2022 concerning Sexual Violence Crimes, specifically Article 14, emphasizes that the act of distributing or transmitting visual products, including videos, that contain sexual harassment can result in criminal penalties.

Criminal acts of fraud that use deepfake AI technology as their modus operandi are often prosecuted under Article 51 paragraph (1) in conjunction with Article 35 of the ITE Law and Article 378 of the Criminal Code. Any person who manipulates, creates, alters, deletes, or destroys ITE or electronic documents with the intention of making them appear to be authentic data shall be punished with a maximum imprisonment of 12 (twelve) years and a maximum fine of twelve billion rupiah. Furthermore, any person who, with the intention of benefiting themselves or others unlawfully, uses a false name, false identity through deception or a series of lies, to induce another person to hand over goods to them or to grant a loan or cancel a debt, shall be punished for fraud with a maximum penalty of 4 (four) years' imprisonment.

In general, the ITE Law has not been effective in dealing with the misuse of deepfake technology because it does not have specific provisions regarding the nature, methods, and impacts of such violations in the context of modern technological developments. This law does not explicitly refer to or regulate deepfakes, which are AI-based digital manipulations that alter a person's identity through falsified images, audio, or video. The articles that are usually applied are very broad and lack technological context, failing to consider the use of AI as a tool for crime, or the intent or purpose behind the creation of deepfake content, whether for fraud, harassment, other criminal purposes, or even for entertainment alone. This poses challenges in law enforcement, especially if the victim is not a public figure or cannot demonstrate clear damages. Law enforcement and judicial authorities may interpret the law differently, increasing the risk of subjective or arbitrary criminalization. Another challenge is that digital forensics is known to be difficult to identify, especially without the support of infrastructure and human resources, the anonymity of perpetrators or the deliberate concealment of their identities, and the lack of ethical and legal standards regarding the use of AI itself.

CASE ANALYSIS

A frequently cited case is that of Alwi Husen Maola.[12] Alwi Husen Maola was sentenced to six years in prison and had his internet access revoked. This punishment can be considered a new breakthrough because it turns out that perpetrators who disseminate information without permission can be charged with an article that revokes their internet access rights. The revocation of internet access rights is considered a breakthrough because internet access rights have recently been promoted as a new human right in the modern world.[13] Internet access rights as human rights are based on the understanding that the internet is an important platform for various fundamental rights, including the right to freedom of expression, access to information, education, and participation in social and economic life.

The internet allows individuals to search for, receive, and disseminate information more easily and quickly. Therefore, internet access not only supports freedom of expression, but also opens up opportunities for economic and educational empowerment. This right to internet access is also supported by many international institutions, including the United Nations (UN), which has emphasized that internet access should be considered a human right, as disconnecting access or restricting internet use can have a significant impact on other basic rights. In this case, the right to internet access means that everyone should have the same opportunity to use the internet without discrimination.

Disproportionate restrictions on internet access, such as excessive blocking or censorship, can be considered a violation of human rights because they hinder a person's freedom to obtain and share information. Therefore, punishment in the form of restricting internet access rights is considered to have a deterrent effect on parties who have malicious intentions to spread harmful information. For this reason, parties who have spread information irresponsibly can be punished by restricting their internet access rights so that they will not repeat the same mistake in the future.

In 2022, there was a similar incident involving deepfake AI technology, namely the viral spread of a pornographic video resembling the artist Nagita Slavina. The victim of the deepfake appeared to be involved in activities that she did not actually do, which certainly caused the victim to suffer losses, mainly to her reputation. The Central Jakarta Police Criminal Investigation Unit stated that it had coordinated with the Metro Jaya Regional Police, which handles cybercrime issues, and found that the visual was edited and manipulated.[14] In early 2025, a criminal act of fraud using the face and audio of President Prabowo Subianto spread widely on Instagram and TikTok. The video shows President Prabowo Subianto asking the public for help. As a result of the circulation of this video, there were people who believed that the video was real and then contacted the person listed and paid an "administrative fee," even though it was a scam. The Cybercrime Directorate of the National Police's Criminal Investigation Agency revealed this criminal incident and successfully arrested the perpetrator in Central Lampung in January 2025.[15] The perpetrator was charged under Article 51(1) in conjunction with Article 35 of the Information and Transactions Law (ITE) and Article 378 of the Criminal Code (KUHP).

The actions of perpetrators who produce or distribute false content with the intention of gaining personal profit are in line with the definition of electronic data manipulation, which is creating the illusion that the information is accurate or comes from a legitimate source. When deepfake content is used to influence public opinion or deceive individuals for personal gain, such as through identity fraud, reputation attacks, or disinformation, then such content constitutes criminal fraud. These actions cause tangible and intangible losses to the victims. Article 35 of the ITE Law regulates digital manipulation and the technological dimensions of such crimes, while Article 378 of the Criminal Code covers the elements of fraud and losses incurred by victims. The application of this article is currently the most ideal legal framework for prosecuting perpetrators in cases involving sophisticated digital crimes that are not explicitly regulated in newer laws.

COMPARISON OF DEEPFAKE AI REGULATIONS WITH OTHER COUNTRIES

[12] "Defendant in 'Revenge Porn' in Banten Sentenced to Six Years in Prison and Internet Access Revoked, Victim's Family: "The Punishment Does Not Match the Victim's Suffering" - BBC News Indonesia," accessed October 30, 2024, https://www.bbc.com/indonesia/articles/cd1w0lydg9eo

[13] Rita Rubin, "Internet Access as a Social Determinant of Health," Jama 326, no. 4 (2021): 298

[14] Galuh Putri Riyanto and Wahyunanda Kusuma Pertiwi. Examining the "Deepfake" Technology Behind the Video Allegedly Resembling Nagita Slavina. Accessed April 13, 2025. https://tekno.kompas.com/read/2022/01/18/15490077/menilik-teknologi-deepfake-di-balik-video-diduga-mirip-nagita-slavina?page=all

[15] Hukmana. Fraud Using AI Deepfake Prabowo's Face, Residents Deceived by Government Aid Offers. Accessed April 13, 2025. https://mediaindonesia.com/politik-dan-hukum/741824/penipuan-dengan-ai-deepfake-wajah-prabowo-warga tertipu-tawaran-bantuan-pemerintah?#goog_rewarded

China

China has enacted regulations on AI contained in the Cybersecurity Law of the People's Republic of China, also known as the Generative AI Measures. The purpose of these regulations is to ensure that the use of artificial intelligence continues to prioritize ethics and morality. This indicates that the Chinese government is seeking to create a legal protection structure that ensures the responsible use of technology. Article 3 paragraph (3) of the New Generation Artificial Intelligence Code of Ethics states that the protection of privacy rights requires all activities carried out by AI to comply with established ethical standards, such as maintaining privacy and security. This includes fully respecting the right of individuals to obtain information about their personal information and consent to its use. AI must not violate personal rights or interests, nor may it collect or use personal information illegally. In addition, AI must not sacrifice or disclose and disseminate individual privacy rights.

Generative AI Measures include regulations related to deepfake technology. Previously, China implemented a draft law entitled "Provisions on the Administration of Synthesis in Internet-Based Information Services." This regulation provides a more detailed framework that specifically addresses the use of deepfake technology and media manipulation, including focusing on the risks and potential for misuse. China is at the forefront of AI regulation, having established a comprehensive set of rules governing Generative AI, Recommendation Algorithms, and AI Innovation.[16]

In addition, China is one step ahead because it has enacted special regulations governing deepfakes since January 10, 2023, through the "Provisions on the Administration of Deep Synthesis of Internet-based Information Service." This regulation acts as a watchdog on the use of synthesis technology that can generate or edit text, images, audio, and even videos that are prone to misuse. This regulation requires service providers to verify the identity of service users, obtain permission and approval to edit data, and filter content and information that is against the law. In addition, personal data is the most important object to be protected. The Chinese government has the authority to enforce the law by imposing sanctions on violators of the above regulations. The existence of these regulations shows that the Chinese government is working hard to maintain cyber security and combat cyber abuse or crime in its territory.

European Union

The EU AI Act has come into effect in European countries, and it is the first regulation governing the use of AI technology. On December 9, 2023, the Council and Parliament of the European Union reached an agreement on the final draft of the EU AI Act. This law establishes a comprehensive regulatory framework for artificial intelligence that is uniform across all sectors that use AI technology in their operations. The EU AI Act officially came into force on March 13, 2024, specifically addressing the regulation of artificial intelligence. The main objective of the EU AI Act is to promote the development and deployment of safe and reliable AI systems for the public and private sectors. In addition, this law also aims to uphold human rights, encourage investment, and promote innovation in the AI landscape.[17] According to Article 3 Paragraph 60 of the EU AI Act, deepfake refers to content that refers to images, audio, or video that has been created or altered using artificial intelligence. This content imitates real people, objects, places, or events and can mislead viewers into thinking it is authentic or true. There is also an obligation for people who create content containing deepfakes, namely the obligation of transparency. Transparency is achieved by attaching a statement if the content created and disseminated is created and altered or manipulated using deepfake AI technology, in accordance with Article 50 Paragraph 4 of the EU AI Act.

RECOMMENDATIONS

The existence of lex specialis for deepfake cases can be achieved by revising the ITE Law. The reason why revising the ITE Law is a more realistic response to the deepfake phenomenon is the fact that not all deepfake crimes involve elements of pornography. It should be taken into consideration that deepfakes can also be used to make it appear as if a political figure is giving misleading statements or inciting hatred towards that figure. Deepfakes can even be used to assassinate someone's character. Placing details about deepfake technology solely in the context of sexual crimes diminishes the reality of the dangers of deepfake technology, while the potential for deepfake crimes is considerable. Even if deepfakes can one day pass the Turing test or reality test that blurs the line between human and machine interaction, it is possible that deepfakes could be used as instruments of financial crime. With this in

[16] Adnasohn Aqilla Respati. Reformulation of the ITE Law on Artificial Intelligence Compared to the European Union and China AI Act Regulation. USM Law Review Journal Vol. 7 No. 3, 2024. P. 1752
[17] Norma Kinanty. Legal Protection for Victims of Artificial Intelligence Abuse in the Form of Deepfake Pornography from a Criminal Law Perspective. 2024. https://doi.org/10.59890/ijsr.v2i4.1992

mind, strengthening the regulation of deepfakes is actually more appropriately placed in the revised Electronic Information and Transactions Law. The second solution is to create specific legal products to address AI. These regulations should govern the procedures or mechanisms for the effective use of AI and legal accountability and its consequences.[18] By applying the principle that the law continues to evolve in line with reality, specific laws governing deepfakes are also regulated to keep pace with developments in society.[19] On the other hand, when drafting regulations on AI, it is important to emphasize that over-criminalization should be avoided. Therefore, the drafting process must be carefully designed and involve various relevant stakeholders. With this understanding, the principle of proportionality will be achieved in the future. Consistency and unity in regulations are needed to address ethical and privacy challenges and to increase the principle of prudence in the use of AI. As a reference, the Indonesian government can emulate other countries that have enacted AI laws.

CONCLUSION

The development of AI, particularly deepfake technology, has posed significant challenges for the legal system. The misuse of this technology highlights regulatory gaps, as there are currently no specific regulations governing these issues. Currently, law enforcement relies on general provisions in the Criminal Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and other relevant laws, which are insufficient to manage the complexity of AI-driven digital crimes. Legal reform is needed to ensure that regulations can keep pace with technological advances. One possible measure is to revise the ITE Law by including provisions on the regulation of AI deepfakes or, further still, by introducing a specific law on AI.[20] This aims to strengthen justice, legal certainty, and the overall effectiveness of the law in addressing the challenges posed by the digital age.

REFERENCES

Books:

Hanafi Amrani. 2019. Politik Pembaruan Hukum Pidana. Yogyakarta: UII Press

Sudarto. 1983. Hukum Pidana dan Perkembangan Masyarakat. Bandung: Sinar Baru

Journals:

Adnasohn Aqilla Respati. Reformulasi Undang-Undang ITE terhadap Artificial Intellegence Dibandingkan dengan Uni Eropa dan China *AI Act Regulation*. Jurnal USM Law Review Vol 7 No 3Tahun 2024. Hlm. 1752

Cahya, Ayuni Nilam et al. (2024) Transformasi Budaya Hukum dalam Era Digital (Implikasi Penggunaan AI dalam Perkembangan Hukum di Indonesia). Jurnal Ikraith Humaniora 8 No. 2

Dino Rizka Afdhali dan Taufiqurrohman Syahuri. 2023. Idealitas Penegakkan Hukum Ditinjau dari Perspektif Teori Tujuan Hukum. *Collegium Studiosum Journal*, Vol. 6 No. 2, Desember 2023

Izzy Al Kautsar and Danang Wahyu Muhammad, "Sistem Hukum Modern Lawrance M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat Dari Industrial Ke Digital," SAPIENTIA ET VIRTUS 7, No. 2 (2022): 84–99, https://doi.org/10.37477/sev.v7i2.358

Kartika, Shahnaz dan Nurhayati, Ujaran Kebencian (*Hate Speech*) di Media Sosial dalam Konteks Hukum dan Perubahan Sosial (Studi Kasus pada Masyarakat Kota Medan). Jurnal Mercatoria 16 No.1 (2023): 101-102

Kurniarullah, Muhammad Rizki et al, Tinjauan Kriminologi Terhadap Penyalahgunaan *Artificial Intelligence: Deepfake* Pornografi dan Pencurian Data Pribadi, Jurnal Ilmiah Wahana Pendidikan 10 No. 10 (2024): 539, https://doi.org/10.5281/zenodo.11448814

Md Shohel Rana et al., "*Deepfake Detection: A Systematic Literature Review*," IEEE Access 10 (2022): 25494–513.

Norma Kinanty. Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence Berupa

[18] Kurniarullah, Muhammad Rizki et al, A Criminological Review of Artificial Intelligence Abuse: Deepfake Pornography and Personal Data Theft, Wahana Pendidikan Scientific Journal 10 No. 10 (2024): 539, https://doi.org/10.5281/zenodo.11448814

[19] Izzy Al Kautsar and Danang Wahyu Muhammad, "Lawrence M. Friedman's Modern Legal System: Legal Culture and Social Change from Industrial to Digital Society," SAPIENTIA ET VIRTUS 7, No. 2 (2022): 84–99, https://doi.org/10.37477/sev.v7i2.358

[20] Cahya, Ayuni Nilam et al. (2024) Transformation of Legal Culture in the Digital Age (Implications of AI Use in Legal Development in Indonesia). Ikraith Humaniora Journal 8 No. 2

Deepfake Porn dalam Perspektif Hukum Pidana. 2024. https://doi.org/10.59890/ijsr.v2i4.1992

Ridwan. Hukum dan Perubahan Sosial: Perdebatan Dua Kutub Antara Hukum Sebagai *Social Control* dan Hukum Sebagai *Social Engineering*. 2016. Jurnal Jurisprudence 6 No. 1

Rita Rubin, "Internet Access as a Social Determinant of Health," Jama 326, no. 4 (2021): 298;

Sean Cao et al., *From Man vs. Machine to Man+ Machine: The Art and AI of Stock Analyses, Journal of Financial Economics* 160, 2024, 103910

Sinaga, Niru Anita, Kesiapan Sistem Hukum Indonesia dalam Transformasi Masyarakat dari 4.0 Menuju 5.0, Jurnal Krtha Bhayangkara 17 No. 1 (2023): 120, https://doi.org/10.31599/krtha.v17i1.2111

Suhendra, Dedy et al. 2024. Konsep Perubahan Hukum dalam Menghadapi Perkembangan Teknologi, Jurnal Ilmiah Muqoddimah 8 No. 1

Yudo Devianto and Saruni Dwiasnati, Kerangka Kerja Sistem Kecerdasan Buatan dalam Meningkatkan Kompetensi Sumber Daya Manusia Indonesia, InComTech: Jurnal Telekomunikasi dan Komputer 10, No. 1 (2020), 19–24, http://dx.doi.org/10.22441/incomtech.v10i1.7460

Articles:

"Menilik Teknologi "*Deepfake*" di Balik Video Diduga Mirip Nagita Slavina". Accessed 13 April 2025. https://tekno.kompas.com/read/2022/01/18/15490077/menilik-teknologi-*deepfake*-di-balik-video-diduga-mirip-nagita-slavina?page=all.

"Penipuan dengan *AI Deepfake* Wajah Prabowo, Warga Tertipu Tawaran Bantuan Pemerintah". Accessed 13 April 2025. https://mediaindonesia.com/politik-dan-hukum/741824/penipuan-dengan-ai-deepfake-wajah-prabowo-warga-tertipu-tawaran-bantuan-pemerintah?#goog_rewarded

"Terdakwa "Revenge Porn" Di Banten Dibui Enam Tahun dan Dicabut Hak Akses Internet, Keluarga Korban: "Hukuman Tidak Setimpal Dengan Penderitaan Korban" - BBC News Indonesia," accessed October 30, 2024, https://www.bbc.com/indonesia/articles/cd1w0lydg9eo.

"VIDA Catat Penipuan "*Deepfake*" di Indonesia Melonjak 1.550 Persen" accessed November, 8, 2024, https://www.antaranews.com/berita/4437365/vida-catat-penipuan-deepfake-di-indonesia-melonjak-1550-persen