CONSENSUS
JURNAL ILMU HUKUM
https://consensus.stihpada.ac.id/
E-ISSN: 2962-2395
Volume 3 Nomor 2 November 2024 Page : 37-44

Alamat:
Jl. Kol. H. Animan Achyad (d/h. Jl. Sukabangun II) KM. 6,5 No. 1610
Kelurahan: Sukabangun. Kecamatan: Sukarami, Palembang.
Telp & Fax: 0711-418873/email: jurnalconsensus@gmail.com

Analysis Of The Influence Of Artificial Intelligence Deepfakes From The Perspective Of Legal Science

Inka Verandera Nugraha
Sumpah Pemuda School of Law, E-mail: inkeyverandera@gmail.com

Abstract

In its urgency, AI itself has developed rapidly with the aim of facilitating the acquisition of information by humans in a more expeditious and succinct manner. However, the creation of a system entails a duality of positive and negative consequences. The benefits of AI include the potential to streamline human workflows, provide assistance, and address queries. However, as with any technology, there are also risks and challenges. One such challenge is the emergence of deepfake, a phenomenon where artificial intelligence is used to create realistic fake videos. Deepfake is a video that employs artificial intelligence to portray a person saying and doing things that did not occur in real life. To illustrate, a face swap can be performed in a way that leaves minimal evidence of manipulation on the video. Accordingly, the author investigates the potential for leveraging existing legal frameworks to hold perpetrators of deepfake criminally liable. The research method employed is the normative legal research method. This involves the collection and discussion of positive legal rules in Indonesia and the European Union as a source of primary legal material, as well as related literature as a source of secondary legal material. The results demonstrate that, given that deepfake is an AI that uses electronic data or information, the PDP Law and GDPR are pertinent to the examination of regulations pertaining to the prohibition of AI manipulation for the purpose of misinformation, disinformation, or fraud and the creation of fake news in the cyber world.

Keywords : Artificial Intelligence, Law, Deepfake.

INTRODUCTION

Technology is a collective term used to describe the means used to provide goods and services necessary for human survival and comfort. Technology is ubiquitous in human life, helping in various activities and ventures. In the contemporary era, technology has undergone a period of accelerated development, encompassing a wide range of innovations that have become an integral part of human life and work. These include the Internet of Things (IoT), blockchain technology, big data analytics, and artificial intelligence (AI). The technologies mentioned above play an important role in human life today and have even triggered the emergence of the Fourth Industrial Revolution (Laza & Karo, 2023:136).

However, the accelerating pace of development also raises concerns and potential losses. One of the significant legal issues associated with the misuse of AI is the proliferation of deepfakes, which have gained considerable traction on the internet. Deepfakes are products generated by artificial intelligence that combine, sew, replace, and superimpose images and video clips to create fake videos that look like they are real and spoken by people who don't actually say the words or perform the action. The technology has the potential to produce a variety of videos, including those that are comedic, erotic, or political, that feature a person saying a specific phrase or statement without the consent of the person whose image and voice are used (Budianto, 2020:1339-46).

Microsoft President Brad Smith has identified the potential dangers of AI as a significant concern. Among them, he has identified the development of AI deepfake technology as a very worrying area of research. This technology has the potential to manipulate and spread misinformation and disinformation within a community, as well as misuse personal data. This raises questions regarding the security of consumer data, as well as the potential for the significant spread of misinformation as a consequence of these AI effects. The use of deepfake technology for the purpose of impersonating influencers, artists, public figures, or politicians or presidents is a growing phenomenon. This is done by obtaining personal data or data that already exists in the public domain with the aim of damaging an individual's reputation and providing false information (Amboro, 2021:193-217).

The advent of deepfake technology in 2017 marks a very important turning point in the trajectory of artificial intelligence. Former US President Barack Obama became the first prominent figure to be targeted by this new phenomenon, with a video claiming that he made a statement he never made circulated online. A similar phenomenon also occurred to President Joko Widodo, as evidenced by a video that was widely spread on the social media platform TikTok, where the president was seen singing the song "Cupid" from the South Korean girl group, Fifty-Fifty. The video is the result of artificial intelligence technology that replaces the voice of the original singer with the voice of the president. The end result is as if the president is actually singing the song. Although there have been no high-profile cases of deepfakes in Indonesia, the potential for misinformation and disinformation still exists, especially in the context of the upcoming 2024 general election.

It is undeniable that the detrimental impact of AI deepfakes will violate the fundamental right to privacy inherent in all humans. The philosophical basis of the internationally existing right to privacy is contained in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which states: "No one can be arbitrarily interfered with for their privacy, family, home, or correspondence, or an attack on their honor and reputation. Every individual has the right to legal protection against such interference or attack."

This right guarantees that every individual has the right to, in essence, "hide" or shut off a part of their life from public view, which is one of the most basic human rights. In Indonesia, the philosophical basis regarding privacy is found in Article 28G paragraph (1) of the 1945 Constitution, which states that:

(1) Everyone has the right to the protection of themselves, their families, their honor, their dignity, and the property under their power. In addition, they are entitled to a sense of security and protection from threats which is a human right.
(2) These rights include, but are not limited to, the right to choose whether or not to act in a certain way.

The right to personal protection is not limited to the physical world; This right also includes the virtual realm. This ensures that individuals' rights to their personal selves can be enforced in cyberspace. Violations of the right to privacy can occur when individuals, companies, or even AI take data belonging to individuals without their consent and then

process it for the purpose of spreading misinformation and/or disinformation through the use of deepfake tools. In addition, legal theories related to this subject include the Theory of Legal Protection.

The concept of the state of law underlines the importance of legal protection as an inseparable element of a fair and correct legal system. This includes the recognition and protection of fundamental human rights for all individuals. In addition, legal protection reflects the important role of law in providing justice, order, certainty, and benefits to society. The legal system provides a framework within which individuals or groups who feel there is a threat to their rights or a violation of those rights can seek redress and obtain appropriate redress or compensation.

Therefore, legal protection is a fundamental principle of the legal system, with the aim of protecting individual rights, upholding the rule of law, and ensuring justice in society. Based on the above, researchers propose to conduct further research on the prevention of deepfakes as part of AI. This will include a comparative study between the EU and Indonesia on existing laws and their adequacy in protecting legal subjects from potential violations of the law committed by the emergence of deepfakes. In addition, the question of whether there is an urgency to create a new law internationally regarding AI as a whole will also be discussed. Based on these considerations, this study aims to examine the existing legal framework related to the regulation of AI deepfakes in the context of the General Data Protection Regulation (GDPR) and the Personal Data Protection Law (PDP) in Indonesia. How are the regulations in terms of legal science for legal protection against AI deepfakes reviewed from the General Data Protection Regulation (GDPR), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

RESEARCH METHODS

The research method used is a normative legal research method. Positive legal rules in Indonesia and the European Union are collected and discussed as a source of primary legal material, as well as related literature as a source of secondary legal material.

DISCUSSION

Reviewed from the perspective of Law

The advancement of artificial intelligence has been an inseparable aspect of the evolution of contemporary global society. As a developing country, Indonesia cannot be separated from the impact of artificial intelligence (Radavoi Ciprian N, 2020:107). Artificial intelligence has had a significant impact on various aspects of life, including the legal field. Advances in artificial intelligence have played a crucial role in the evolution of the legal landscape in Indonesia. Artificial intelligence technology has made a significant contribution in facilitating access to legal information. The application of natural language processing algorithms and data analysis enables fast and precise processing of diverse legal sources (Budhijanto, 2002:134-150).

The impact of artificial intelligence on the progress of Indonesia's legal system presents a number of significant challenges (Budhijanto, 2002:134-150). Issues of privacy, data security, and the role of humans in legal decision-making have become significant topics of debate. In addition, it is crucial to implement comprehensive regulations

governing the utilization of artificial intelligence technology in a legal context, in order to prevent potential injustice or abuse (Connell, 2019). In addition, AI technology has the potential to improve the efficiency of the judicial system in Indonesia. Automation of the legal administration process, the use of chatbots to provide basic legal information to the public, and data analysis to predict the development of legal cases are examples of AI implementations that have the potential to reduce the workload of law enforcement officials and judges (Puaschunder, 2017). As a result, this can increase access to justice and accelerate the resolution of legal cases (Rissland et al., 2003; Atkinson et al., 2020).

a. Legal Policy in the European Union regarding *Deepfakes*

In the era of contemporary information technology, data has become a very valuable commodity. The world is increasingly data-centric, with all human information currently being processed and converted into data. Next, data is collected to form what is known as "big data". The term "big data" is used to describe very large, high-speed, or complex data sets, making them challenging or impossible to process using conventional techniques. Based on the study's findings, the volume of data generated globally is growing rapidly, increasing from 33 zettabytes in 2018 to about 175 zettabytes by 2025 (Zulfikar, 2023: 10716-22).

Data serves as "fuel" for artificial intelligence (AI) to move and grow, because all learning processes carried out by AI are data-centric. Without data, AI would not be able to function, similar to a vehicle that cannot operate without fuel. In this context, the role of the General Data Protection Regulation (GDPR) is to filter the data that will be the object of processing. The GDPR applies to all 27 member states of the European Union (EU). In addition, this regulation also applies to all countries in the European Economic Area (EEA), which includes Iceland, Norway, and Liechtenstein. While GDPR does not directly regulate artificial intelligence (AI), it indirectly affects AI because AI relies on data to stay operational. Data supply settings allow for the regulation of AI development.

The potential for deepfake applications is very diverse. They can be used for satirical purposes, artistic expression, or harmless entertainment. However, they can also be used to spread disinformation, produce adult content, expose political scandals, create fake news, and even as a tool in modern warfare. The creation of deepfakes is not a criminal act in itself. However, if it violates the subject's personal rights or is used for malicious purposes, then there are legal consequences. In accordance with the regulations set by the General Data Protection Regulation (GDPR) regarding deepfakes, the processing of personal data is only allowed under certain conditions (Article 67 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection). This is because every individual has the right to privacy and protection of their personal data.

It should be emphasized that the word '*processing'* is a word that has a broad meaning, which includes all possibilities related to the use of personal data in the *lifecycle of deepfakes*. This broad scope has implications for technology developers and deepfake creators themselves, because personal data is not only used to create certain *deepfakes*, but also to train the software used to create *deepfakes*, so that the device can be more sophisticated. As a result, the operation of application services that make it possible to create *deepfake* videos, requires *a Data Protection Impact Assessment* (DPIA), from the

authorities, where the personal controller itself must actively seek the authorities, and together use systematic and extensive evaluation to ensure that processing using new technologies does not have a significant risk of violating rights and freedom of individual legal subjects. Thus, it can be said that the GDPR applies and provides substantive protection for the development of *deepfake software* and applications, as well as for the creation and distribution *of deepfakes* themselves (Article 20 paragraph (2) letters (a) and (f) of Law Number 27 of 2022 concerning Personal Data Protection).

The GDPR stipulates that a legal basis is always required before processing personal data. Only "informed consent" and "legitimate interest" are appropriate in the context of deepfakes, although there are six legal bases in the GDPR. When the creator of a deepfake, or the creator of a deepfake, declares that they have a legitimate intention to carry out the processing of a person's personal data, such intention must not conflict with the interests or fundamental rights and freedoms of the person involved in the deepfake. For example, a deepfake creator can upload a video that ironically depicts a famous person using deepfake depictions. In such situations, the creator of a deepfake can claim freedom of speech for the purpose of satirizing or making political comments.

Nevertheless, the use of personal data for the use and spread of deepfakes requires the explicit consent of the people depicted in the video if the legitimate purpose is unattainable or unattainable. Since their personal data will be processed, consent must be obtained from the person in the original video and the person who will appear in the edited deepfake video. This is important to underline. If the creator of the deepfake fails to get permission from both parties before doing so, they will be in violation of the GDPR (Article 4 paragraph (2) of Law Number 27 of 2022 concerning Personal Data Protection).

So, the GDPR deals with deepfake content that violates the law. This gives victims the right to verify incorrect data information or even request that the video be removed. In each member state, there is at least one independent supervisory authority responsible for ensuring and enforcing applicable laws and regulations. However, the legal path for victims can be more difficult in deepfake cases. Victims are often unable to identify the perpetrator who often acts anonymously. Victims are also often vulnerable to deepfakes because they may not have the necessary resources to initiate the judicial process.

b. Legal Policies in Indonesia related to *Deepfakes*

Indonesia finally issued Law Number 27 of 2022 concerning Personal Data Protection. The PDP Law is derived from the GDPR, which is the most comprehensive law on personal data protection. In terms of deepfakes, the regulations regulated in the PDP Law in Indonesia are the same as those regulated in the GDPR. The PDP Law does not regulate AI or deepfakes directly, but because AI uses data, the PDP Law also indirectly protects deepfakes created by people who use AI.

Specific personal data-usually a person's face and voice-is taken by the creator of the deepfake in this case and incorporated into another image or video for a specific purpose. In general, the creator of a deepfake must meet the criteria between the legitimate interests and/or prior consent of the person depicted in the deepfake, so that they can avoid the possibility of violating the applicable law in this case, the PDP Law (Priowirjanto, 2022:254-72).

To avoid violations of the PDP Law, this valid consent must be clearly given by the personal data subject. Every person is legally prohibited from obtaining or collecting personal data that does not belong to him because, according to Article 65 paragraph (1) of the PDP Law, "Every Person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him or herself with the intention of benefiting himself or others that may result in the loss of the Personal Data Subject." In other words, everyone is prohibited from doing anything that is prohibited by law.

In addition to the PDP Law, Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) (Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions). Indonesia also defames artists, influencers, and politicians as well as content that violates morals, such as a picture of a woman with a porn star changing her face. The ITE Law also stipulates that people who create deepfakes must be held responsible.

The Creator may not disseminate or transmit information and electronic documents that contain insults, gambling, insults, defamation, extortion, or threats. This is in accordance with the protection provided by deepfakes, because the negative effects that deepfakes usually cause include featuring a woman who has never even done immoral acts to defame, violating decency.

With the existence of the PDP Law and the ITE Law, it can protect Indonesia citizens from the adverse effects of *deepfakes*. However, as previously explained, the victim also often experiences difficulties. In this case, the legal path for the victims can become more difficult. Victims are often unable to identify the perpetrator who often acts anonymously. Victims are often vulnerable to *deepfakes* because they may not have the necessary resources to initiate the judicial process.

c. The Urgency to Regulate AI

Artificial Intelligence has brought many social benefits, such as medical advances and the fight against climate change. For example, AI technology developed by United Kingdom AI company DeepMind can now predict the structure of almost every protein known to science. It has the ability to accelerate scientific research up to several times. Thus, scientists have been able to develop life-saving drugs, and these advances have helped scientists in the fight against antibiotics, malaria, and plastic waste to very high levels (Jufri & Putra, 2021:31-57).

AI can also help mitigate climate change, for example by improving energy efficiency or reducing emissions from industry, transportation, and agriculture. AI can also help us adapt to the impacts of climate change by improving our ability to predict extreme weather and providing decision-supporting tools to help us make better decisions.

Although AI seems to be revered for its potential to help humans, the results of which are already beginning to be seen, anxiety about AI is still present. This can be seen from the signing of an open letter signed by more than 2,600 leading leaders and researchers in the tech industry in recent times, including Tesla CEO Elon Musk and Apple co-founder Steve Wozniak. This open letter asks for a temporary halt to AI development. The petition states that the competitive intelligence of humans possessed by AI can pose a great danger to society and humanity. This means that all artificial intelligence companies must

"immediately halt" the development of artificial intelligence systems more powerful than Generative Pre-trained Transformer4 (GPT-4) for at least six months (Prashant Jha, 2023).

CONCLUSIONS

There is no doubt that AI has developed and developed very quickly and massively in this era of globalization. Every day new technologies and applications based on AI are appearing that are getting smarter, which makes human life easier and more efficient. However, with all these positive advances, of course, there will be legal issues related to AI. One of these legal problems is the emergence of deepfake technology.

Deepfakes are used to imitate a person's face, voice, or body that doesn't even belong to the person themselves, so they are often used to carry out disinformation and fraud. For example, they can imitate someone's voice to take money at an ATM, resulting in personal losses and even threatening large institutions, so they must be more careful when granting permission for someone. Therefore, there are existing legal protections and certainties that govern these deepfakes. The GDPR and the PDP Law in Indonesia protect data subjects from deepfakes because data is the "fuel" of AI, so AI will not be able to do things it would normally do without.

Article 65 paragraph (1) of the PDP Law clearly states that it is illegal to obtain or collect Personal Data that does not belong to him for the purpose of benefiting himself or others. However, this is clearly not enough. There is a need for sharper and more specific regulations on artificial intelligence, such as the Artificial Intelligence Act in the European Union, which provides a risk-based approach to their approach to regulating artificial intelligence. This is intended to maintain a balance between regulation and development, where existing arrangements must not be excessively restrictive so as to hinder development.

REFERENCE

Amboro, Komarhana. "The Prospect of Artificial Intelligence as a Subject of Civil Law in Indonesia." *Law Review* XX, no. 2 (2021): 193–217.

Budianto, Agus. “Legal Research Methodology Reposition in Research on Social Science.” *International Journal of Criminology and Sociology* 20, no. 9 (2020): 1339–46. https://doi.org/10.6000/1929-4409.2020.09.154.

Budhijanto, D. (2002). The Role of Telecommunication Law on the Implications of ICT Convergence. Journal of Legal Dynamics, 14(1), 134–150. https://dinamikahukum.fh.unsoed.ac.id/index.php/JDH/article/view/283/275

Connell, B. W., & Black, M. H. (2019). Artificial Intelligence Artificial Intelligence and Legal Education. The Computer & Internet Lawyer, 36(5).

Jufri, Muhammad Ariq Abir, and Akbar Kurnia Putra. "Aspects of International Law in the Use of Deepfake Technology for Personal Data Protection." *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 31–57. https://doi.org/10.22437/up.v2i1.11093.

Laza, Jeremiah Maximillian, and Rizky Karo Karo. “Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP Dan GDPR [Legal Protection of Artificial Intellegence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR].” *Lex Prospicit* 1, no. 2 (2023): 136. https://doi.org/10.19166/lp.v1i2.7386.

Michaels, A. C. (2020). Artificial Intelligence, Legal Change, and Separation of Powers' (2020) 88(4) University of Cincinnati Law Review 1083 MLA 9th ed. Michaels, Andrew C. Artificial Intelligence, Legal Change, 88(4), 1083–1104. https://heinonline.org/HOL/License

Prashant Jha, "Elon Musk-led Petition to Halt AI Development Divides Tech Community," CoinTelegraph, March 31, 2023, https://cointelegraph.com/news/elon-musk-led-petition-to-halt-ai-development-divides-tech-community.

Priowirjanto, Enni Soerjati. "The urgency of regulation regarding Artificial Intelligence in the online business sector during the Covid-19 pandemic in Indonesia." *Journal of Bina Mulia Hukum* 6, no. 2 (2022): 254–72. https://doi.org/10.23920/jbmh.v6i2.355.

Zulfikar, P. "The Influence of Artificial Intelligence (AI) Technology on the Development of Legal Education in Indonesia." *Journal on Education* 06, no. 01 (2023): 10716–22.https://www.jonedu.org/index.php/joe/article/view/4855%0Ahttps://www.jonedu.org/index.php/joe/article/download/4855/3800.

Legal Regulations:

Article 67 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection

Article 20 paragraph (2) letters (a) and (f) of Law Number 27 of 2022 concerning Personal Data Protection

Article 4 paragraph (2) of Law Number 27 of 2022 concerning Personal Data Protection

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.