WORLD CLASS ISLAMIC CYBER UNIVERCITY
UNISSULA
SULTAN AGUNG ISLAMIC UNIVERSITY
Master of Law Program (S2)
Faculty of Law
Collaboration International Program with Doctoral of Law – UNISSULA 2024
Proceeding of International Conference on The Law Development For Public Welfare
ISSN 2798-9313
Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Legal Analysis of the Use of Deep Fake Artificial Intillegence; Criticism and Solutions for Future Regulatory Improvements

Andriyanto [1)]

[1)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: masbroandriyanto@gmail.com

Abstract. *The use of AI deepfake technology in recent years has become a serious concern in various fields, including law, privacy and security. This article analyzes the legal aspects of using deepfakes. Through a descriptive qualitative approach, this article explores the relevant legal provisions in the Information and Electronic Transactions Law (UU ITE), Personal Data Protection Law (UU PDP), Criminal Code (KUHP) to ensnare the use of deepfakes and regulatory projections for the future. The findings of this research show that several laws can be used as a basis for dealing with deepfake cases, but there is still a need to update regulations related to deepfakes. Apart from that, it is hoped that the government will need to draft special laws to overcome the phenomenon of AI deepfakes.*

Keywords: *AI; Deepfake; Law; Regulation.*

1. Introduction

In an era where technology is advancing at an incredible pace, advances in artificial intelligence (AI) have provided tremendous potential, but have also raised unexpected challenges. One contemporary phenomenon that raises serious questions about ethics, privacy, and the law is “deepfakes.” Deepfake, is an AI technology for creating video or audio that appears genuine but is actually fake Deepfake is a technology that uses artificial intelligence (AI), specifically deep learning techniques, to create fake multimedia content that appears authentic and real.[1]

[1] Aiken, Malaika, & Greenstadt, Rachel. (2020). The Illusion of Personalization: The Need for Algorithmic Awareness and Accountability in Pornography Consumption. Yale Journal of Law & Technology, 22(1), p. 33-80.

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

The term "deepfake" itself is a combination of "deep learning" and "fake". This technology is generally used to create video or audio that shows someone actually doing or saying something they have never done or said. The process of creating a deepfake begins with collecting visual or audio data from a target person.[2]

This data can take the form of video and audio recordings taken from various sources, such as interviews, films, or television shows. Then, deep learning technology is used to analyze and study patterns in the data, including facial expressions, lip movements and voice intonation. After learning these patterns, the deep learning model can then generate fake content that depicts the target in a different situation or context. For example, an actor may be replaced in a movie scene, or a person may "speak" in a video that appears authentic.[3]

According to Statistia data, in 2021 AI users will reach 1.76 billion. This data shows that society is aware of the presence of AI as a utility, just like the existence of computers and the internet. The use of deepfakes has raised various concerns, especially regarding their potential misuse in politics, pornography and crime. Deepfakes can be used to create fake videos that mislead or damage someone's reputation, spread hoaxes or political propaganda, or even create fake pornographic content involving people without their permission.[4]

Deepfake techniques open the door to potential fraud, falsification and manipulation of information that can disrupt the social and political order.[5] Many cases in Indonesia and other countries have been harmed by deepfake technology. First, in 2022 there will be the case of the famous artist Nagita Slavina.

In early 2022, Indonesian people were shocked by a horrendous incident, namely the distribution of a 61-second pornographic video showing a face similar to Nagita Slavina. After being investigated by the Polda Metro Jaya Cyber Team, it turned out that the video was the result of manipulation by deepfake technology, where Nagita Slavina's face was replaced by another person's face through the use of AI.[6]

---

[2] Citron, Danielle Keats, & Chesney, Robert. (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, p. 107.

[3] Ibid

[4] Ibid

[5] Wang, Y., & Farid, H. (2019). Exposing DeepFake Videos by Detecting Face Warping Artifacts. Proceedings of the IEEE International Conference on Computer Vision (ICCV), p. 3230-3238.

[6] Pertiwi, WK (January 18, 2018). Taking a look at the "deepfake" technology behind the video allegedly similar to Nagita Slavina Page all. KOMPAS.com. available at

A similar case also happened to the famous actress Emma Watson, where her face was used in an application advertisement that displayed pornographic-like content. An NBC News article in March 2023 reported that there were dozens or even hundreds of similar advertisements circulating on social media platforms such as Instagram, Facebook and Messenger. While the ads do not show explicit sexual activity, they begin with an intro sound that references pornographic content, showing how deepfakes can be used to damage reputations and violate human rights.[7] Apart from being used for pornographic purposes, deepfakes are also used to spread hoax video content, especially during the 2024 presidential candidate general election (Pemilu) in Indonesia.

The Ministry of Communication and Information handled 203 fake news related to the election that spread on social media from the end of 2023 to the beginning of 2024. previously. The total amount of information dissemination reached 2,882 pieces of content. Of this number, the most hoax findings were found in Meta's subsidiaries, namely Facebook and Instagram, with 1,325 content, and 198 hoax content related to the election. Another platform that also contributed a large number of election- related hoaxes was X/Twitter with a total of 947 content. Next, there is TikTok with 342 content, Snack Video with 36 content, and YouTube with 34 hoax content.[8]

From the case examples described previously, deepfakes can also be categorized as a form of online gender-based violence (KBGO) if they are used for pornographic purposes. Deepfakes used for pornography can be a criminal act because they can harm both individuals and the social structure of society as a whole. Meanwhile, if it is related to the purpose of spreading hoaxes, it can include various criminal acts, such as theft of personal data, dissemination of information that violates moral norms, as well as falsification or manipulation of data.

Currently, the public can only rely on four applicable national regulations, namely the Information and Electronic Transactions Law (UU ITE), the Personal Data Protection Law (UU

https://tekno.kompas.com/read/2022/01/18/15490077/menilik-technology-deepfake-di-baik-video-diduga-mirip-nagita-slavina?page=all

[7] Tenbarge, K. (2023, March 7). Sexual Deepfake ads using Emma Watson's face ran on Facebook, Instagram. NBCNews.com. available at https://www.nbcnews.com/tech/social-media/emma-watson-deep-fake-scarlett-johansson-face-swap-app-rcna73624

[8] Bestari, P., March 5, 2023, "203 2024 Election Hoaxes Circulating on Social Media, Many Are Still Viral" available athttps://www.cnbcindonesia.com/tech/20240105080338-37-502925/203-hoaks-pemilu-2024- beredar-di-medsos-besar-yang-masih-viral.

PDP), the Pornography Law (UU Pornography), and the Indonesian Civil Code. Criminal Law (KUHP). The following is a brief explanation:

1. Electronic Information and Transactions Law (UU ITE)

The ITE Law is a law that regulates the use of information technology and electronic transactions in Indonesia. This law covers various aspects, including electronic data security, privacy protection, as well as regulation of various criminal acts that occur in the digital space, such as fraud, dissemination of misleading information, and defamation.

2. Personal Data Protection Law (UU PDP)

The PDP Law is a law that aims to protect individuals' personal data from misuse and unlawful processing. This law establishes personal data protection standards that organizations or entities that collect, store and process personal data must comply with, and provides individuals with rights to control and access their personal data.

3. Pornography Law (Pornography Law)

The Pornography Law is a law that regulates the production, distribution and consumption of pornographic material in Indonesia. This law sets clear boundaries regarding the types of pornographic material that are considered illegal, as well as providing legal sanctions for violations of the specified provisions.

4. Criminal Code (KUHP)

The Criminal Code is a law that regulates various criminal acts and legal sanctions imposed on law violators in Indonesia. This Criminal Code covers various aspects of crime, ranging from crimes against state security, crimes against morality, to crimes against public and individual interests. It includes a number of relevant articles in the context of deepfake abuse, such as document falsification, defamation and the dissemination of false information.[9]

In a legal context, the implications of deepfakes are complex, threatening the integrity of evidence in the justice system and creating new challenges in defining the boundaries of

[9] Maharini, A. et al, December 1, 2023, "Deepfake artificial intelligence (AI): A new method of manifesting Online Gender-Based Violence (KBGO)" available athttps://hopehelps-ugm.medium.com/deepfake-artificial-intelligence-ai-method-baru-dari-wujud-kekerasan-berbasis-gender-online-431c92948306

privacy and truth. So, what is the legal analysis of the use of deepfake AI and is it necessary to create new regulations to regulate it?

2. Research Methods

This research tries to conduct an analysis of the legal use of deepfake AI. This article aims to analyze criticism, solutions and projections of future legal regulations in regulating the use of AI deepfakes. This research uses a qualitative descriptive analysis approach, a research method to describe and describe phenomena or data in a detailed and in-depth way.

In qualitative descriptive analysis, data is collected through various techniques, such as interviews, participant observation, or document analysis. Then, the data is analyzed systematically by identifying themes, patterns, or categories that emerge from the data. This analysis was carried out using an inductive approach, where the researcher allowed the findings to emerge from the data itself, without forcing a previous conceptual framework.[10]

Using qualitative descriptive analysis, researchers looked for cases of deepfake use and reviewed existing legal regulations in Indonesia to find out whether existing regulations were sufficient or needed new legal regulations, specifically to regulate the use of AI deepfakes so as not to cause various problems related to sexual crimes and human rights violations.

3. Results and Discussion

The use of deepfakes invites serious consideration regarding the ethics and regulations governing them. Although this AI technology has the potential to bring useful innovations, its misuse in the context of sexual crimes and human rights violations emphasizes the need for a firm response in terms of the law, responsive public policy, and advances in the technology itself.

Existing regulations, such as the Information and Electronic Transactions Law (UU ITE) in Indonesia, need to be updated to face the challenges arising from the deepfake phenomenon. There are only 4 regulations in Indonesia that can be used to ensnare deepfake users themselves, but each still has criticism or shortcomings. The 4 regulations are:

1. ITE Law:

[10] Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. Sage Publications, p. 115.

It should be emphasized that the ITE Law does not actually directly regulate the use of AI, especially in the context of deepfakes. However, article 1(8) explains that deepfakes have the same characteristics as electronic agents. An electronic agent can be defined as "a device that is produced from an electronic system and used to carry out actions on certain electronic information automatically by people." The word "automatic" in this article means working alone, whose characteristics are almost the same as AI.

If anyone is harmed by deepfake, then you can refer to article 27(1) in the ITE Law which reads "Every person intentionally and without right distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that have content that violates decency."[11]

In this article, people who use deepfakes and harm other people can be charged under Article 27 (1) of the ITE Law, namely imprisonment for 6 years or a maximum fine of IDR 1 billion.

2. PDP Law

Law enforcement in deepfake cases can also refer to the Personal Data Protection Law (PDP Law) because the use of deepfakes involves falsifying personal data for personal or other people's interests. Therefore, the provisions in Article 66 of the PDP Law which states that, ""everyone is prohibited from creating false personal data or falsifying personal data with the intention of benefiting themselves or others which may result in harm to others" can also apply in this context.[12] The legal consequences arising from this violation are imprisonment with a maximum sentence of 6 years or a fine of IDR 6 billion.

3. Pornography Law

Deepfakes can also produce media in accordance with the characteristics of pornography as written in Article 1(1) of the Pornography Law which defines pornography as, "images, sketches, illustrations, photos, writing, sounds, sounds, moving images, animations, cartoons, conversations, movements." body, or other forms of messages through various forms of communication media and/or public performances, which contain obscenity or sexual exploitation that violates the norms of decency in society." Referring to this article, deepfake

[11] Republic of Indonesia Law number 19 of 2016, available thttps://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20 Tahun%202016.pdf.

[12] Law number 27 of 2022, BPK, 17 October 2022, "Law (UU) Number 27 of 2022 Personal Data Protection" is available athttps://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

users can be punished with a minimum prison term of 6 months and a maximum of 12 years, as well as/or a minimum fine of IDR 250 million and a maximum of IDR 6 billion.[13]

4. Criminal Code (Law 1/2023)

The latest Criminal Code (KUHP), which will come into force in 2026, regulates the misuse of deepfakes containing pornographic material with heavier criminal sanctions, and cancels the provisions in Article 27(1) of the ITE Law and Article 45(1) Law 19/2016.

In cases of deepfake abuse related to online gender-based violence (KBGO), a person can file a lawsuit under the above-mentioned articles.

Although some of the laws mentioned have relevant provisions to address deepfake cases, they are not necessarily sufficient to comprehensively address all aspects of this phenomenon. Most existing laws do not yet specifically address the use of deepfakes, so there is a need to update and strengthen existing regulations or even draft new laws that specifically address this issue.

Some solutions that can be proposed to regulate the use of deepfakes from a legal perspective are:

1. Renewal of Existing Laws

Carry out updates and improvements to existing laws, such as the Information and Electronic Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and the Criminal Code (KUHP), by adding provisions - provisions that specifically regulate the use of deepfakes.

2. Special Law on Deepfakes

Create new laws that specifically regulate the use of deepfakes, including their creation, distribution, and use in harmful contexts, such as fake pornography, fraud, or invasion of privacy.

3. Increasing Awareness and Educating the Community

Carry out education and outreach campaigns to increase public awareness about the dangers and consequences of using deepfakes, as well as how to identify them and protect yourself from potential misuse.

[13] Law number 44 of 2008, BPK, 26 November 2022, "Law (UU) Number 44 of 2008 concerning Pornography"

4. Collaboration between Government and Technology Industry

Encourage cooperation between the government and the technology industry to develop more advanced deepfake detection technologies, and implement strict security and privacy standards in the development and use of artificial intelligence.

It is hoped that the implementation of these regulatory solutions and projections will be able to handle AI deepfake cases so that they do not harm other people and thus be able to provide better protection for society from the potential negative impacts of deepfakes.

4. Conclusion

In an era when technology continues to develop rapidly, the use of deepfake AI has presented significant new challenges in various aspects of life, especially in the realms of law, privacy and security. Cases of misuse of deepfakes, which are often used for detrimental purposes such as fraud, counterfeiting, fake pornography, as well as human rights violations, highlight the urgency to address this phenomenon through appropriate and effective regulation. Although several existing laws, such as the Information and Electronic Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), provide a legal basis for dealing with deepfake cases, there are still gaps and shortcomings in regulations. at this time so there is a need for new rules. Recommendation: As for recommendations for further research: As for further research, it is recommended to examine the comparison of deepfake regulations in Indonesia with other countries to provide additional insight into different legal approaches to this problem. Or you can do an in-depth case study about deepfake cases that occurred in Indonesia and the context of use, impact and legal response to this phenomenon.

5. References

Journals:

Aiken, Malaika, & Greenstadt, Rachel. (2020). The Illusion of Personalization: The Need for Algorithmic Awareness and Accountability in Pornography Consumption. Yale Journal of Law & Technology, 22(1), 33-80.

& Chesney, Robert. (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107.

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. Sage Publications.

Wang, Y., & Farid, H. (2019). Exposing DeepFake Videos by Detecting Face Warping Artifacts. Proceedings of the IEEE International Conference on Computer Vision (ICCV), 3230-3238.

Pertiwi, WK (January 18, 2018). Examining the "deepfake" technology behind the video allegedly resembling Nagita Slavina. KOMPAS.com. Available at: https://tekno.kompas.com/read/2022/01/18/15490077/menilik-technology-deepfake-di-baik-video-diduga-mirip-nagita-slavina?page=all

Bestari, P. (March 5, 2023). "203 2024 Election Hoaxes Circulating on Social Media, Many Are Still Viral." Available at: https://www.cnbcindonesia.com/tech/20240105080338-37-502925/203-hoaks- pemilu-2024-beredar-di-medsos-besar-yang-masih-viral Citron, Danielle Keats,

Tenbarge, K. (2023, March 7). Sexual Deepfake ads using Emma Watson's face ran on Facebook, Instagram. NBCNews.com. Available at: https://www.nbcnews.com/tech/social-media/emma-watson-deep-fake-scarlett-johansson-face-swap-app-rcna73624

Maharini, A. et al (1 December 2023). “Deepfake artificial intelligence (AI): A new method of online gender-based violence (KBGO).” Available at: https://hopehelps-ugm.medium.com/deepfake-artificial-intelligence-ai-method- baru-dari-wujud-kekerasan-berbasis-gender-online-431c92948306

Regulation:

Republic of Indonesia. (2016). Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Available at: https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf

Republic of Indonesia. (2008). Law Number 44 of 2008 concerning Pornography. Available at: https://peraturan.bpk.go.id/Details/39740

Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Protection of Personal Data. Available at: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022