

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

Legal Protection of Artificial Intelligence: Analysis of Deepfake Technology in the Context of the Personal Data Protection Law

Eben E. Silalahi¹⁾, Bambang Tri Bawono²⁾ & Jawade Hafidz³⁾

¹⁾Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: Ebensilalahi1808@gmail.com

²⁾Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: bambang@unissula.ac.id

³⁾Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: jawade@unissula.ac.id

Abstract. *The development of Artificial Intelligence (AI) technology in recent years has had a significant impact on various aspects of life, including the creation of increasingly sophisticated digital content. One of the phenomena that have emerged is deepfake technology, where AI is used to create fake videos that are difficult to distinguish from the real ones. In the context of personal data protection, deepfake technology raises several legal issues related to individual privacy and data security. Personal data protection laws must be able to accommodate protection against the misuse of deepfake technology, which can harm an individual's reputation and privacy. In some countries, efforts have been made to update personal data protection laws to address the challenges posed by deepfake technology. Legal protection for AI, especially in the context of deepfake, is important to safeguard the security and privacy of individuals' personal data. Thus, legal protection for Artificial Intelligence, particularly in the analysis of Deepfake Technology in the context of personal data protection laws, becomes an urgent matter to consider in order to safeguard the security and privacy of individuals' personal data in this digital era.*

Keyword: Artificial; Deepfake; intelligence; Technology.

1. Introduction

The development of technology, the existence of Artificial Intelligence (AI) has become an unavoidable reality. AI, which is a technology capable of mimicking human behavior, has been used in fields such as health, finance, and entertainment. However, with its increasingly

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

sophisticated capabilities, AI can also be used for unethical purposes, one of which is in the production of deepfakes.

Deepfake is a technology that uses AI to create fake video or audio that can trick people into believing that it actually happened. Thus, deepfake can be used for manipulative purposes and cause harm to others. Therefore, strong legal protection is needed against the use of deepfake technology, especially in the context of the Personal Data Protection Law (UU PDP).

The most widely discussed case of deepfake is the video deepfake case that caused chaos in the United States in 2019. The deepfake video features a politician who is making a speech in inappropriate language, when in fact the video is the result of engineering using AI. This case raises concerns about the potential for the spread of false information that could affect public opinion.

In Indonesia, although there have been no similar cases of deepfake, the government has paid attention to the potential dangers that can be caused by deepfake technology. In 2016, the Indonesian government has issued a PDP Law that aims to protect a person's personal data from misuse and takeover by other parties. In this PDP Law, there are provisions regarding the regulation and protection of personal data managed by private and government parties.

In addition to The Rules of PDP Law, there are also other laws and regulations that can be used to protect the public from the spread of deepfake technology. One of them is the Electronic Information and Transaction Act (UU ITE) which regulates the criminal act of unauthorized use of electronic data, including video deepfake that causes harm to others. With these regulations, it is hoped that it can provide adequate legal protection against the use of deepfake technology. However, greater efforts are still needed in monitoring and controlling the use of deepfake technology, especially with the development of AI technology. In addition, it is also necessary to have awareness from the public not to spread video deepfake that can cause harm to others.

By the development of technology, legal protection against the use of deepfake technology is important in order to protect the public from the spread of false information that can affect public opinion. In Indonesia, the PDP Law and the ITE Law can be used as a basis for protection against deepfake technology. However, greater efforts are still needed to monitor and control the use of deepfake technology so as not to cause harm to others. In addition, public awareness also needs to be improved in the use of deepfake technology.

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

2. Research Methods

This research uses a qualitative approach to analyze the legal protection against the use of Deepfake technology in the context of the Personal Data Protection Law. Research data is obtained through literature studies, analysis of legal documents, interviews with legal and technology experts, as well as case studies of the use of Deepfake technology. The results of data analysis will provide a deeper understanding of the legal protection of Artificial Intelligence, especially in the context of Deepfake Technology and the Personal Data Protection Law, as well as provide appropriate policy recommendations to improve the protection of personal data in this era of advanced technology.

4. Results and Discussion

3.1. The Effectiveness of the Implementation of the Personal Data Protection Law in Overcoming the Challenges That Arise Due to the Development of Artificial Intelligence Technology, related to the Prevention and Handling of Cases of Abuse of Deepfake Technology Involving Individual Personal Data

In the increasingly advanced digital era, the development of artificial intelligence (AI) technology has experienced rapid progress. This technology has many benefits, but on the other hand it also poses new challenges, especially related to the protection of individual personal data. The development of artificial intelligence technology has had a significant impact on various aspects of life, including the protection of personal data. With the increasing sophistication of artificial intelligence technology, new challenges are emerging that must be faced by the Personal Data Protection Law in protecting individual personal data from abuse.

One of the challenges that arise due to the development of artificial intelligence technology is the case of Deepfake Technology abuse. Deepfake Technology (audio and video forgery technology) has allowed the creation of fake videos or audio that are very similar to real people, so that they can be misleading and cause harm to the individuals involved. Deepfake Technology cases often involve the intentional or accidental use of individual personal data, which can threaten the privacy and security of individual personal data.

To overcome this challenge, the Personal Data Protection Law (Law No. 11 of 2008) has regulated the protection of personal data, including in terms of the use of personal data by artificial intelligence technology. The law gives individuals the right to know and control the use of their personal data, as well as sanctioning violators who misuse personal data.

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

However, the implementation of the Personal Data Protection Law in addressing the Deepfake Technology case still has several challenges, especially related to applicable regulations and related cases. There are some of the challenges faced:

1. The need for more specific regulatory adjustments related to the use of personal data by artificial intelligence technology, including in the case of Deepfake Technology. This is important so that the use of personal data by artificial intelligence technology can be maximally protected and does not cause harm to the individuals involved.
2. Another challenge is the difficulty of identifying and handling Deepfake Technology cases involving individual personal data. Because Deepfake Technology can manipulate personal data invisibly, it is difficult to know whether the personal data has been misused or not. In addition, Deepfake Technology cases often involve perpetrators who are difficult to identify, making it difficult to follow up on the case.

To overcome this challenge, there needs to be better cooperation between the government, personal data protection agencies, and other stakeholders. In addition, there is also a need to increase public understanding and awareness regarding the importance of protecting personal data and the dangers of the Deepfake Technology case.

In related cases, the implementation of the Personal Data Protection Law has been carried out by various institutions, such as the Corruption Eradication Commission (KPK) which takes legal action against people who fake votes using Deepfake technology to influence regional head elections. In addition, some countries have also adopted more specific regulations related to the use of personal data by artificial intelligence technology, such as the General Data Protection Regulation (GDPR) in the European Union.

Overall, the effectiveness of the implementation of the Personal Data Protection Law in overcoming the challenges that arise due to the development of artificial intelligence technology still needs to be improved. Better cooperation between related parties is needed and increased public understanding of personal data protection. In addition, there needs to be more specific regulatory adjustments related to the use of personal data by artificial intelligence technology, especially in the case of Deepfake Technology. Thus, it is hoped that the protection of personal data can be guaranteed and the public can avoid cases of misuse of Deepfake Technology involving individual personal data.

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

2. The Role of Government Agencies in Supervising and Providing Sanctions Against Violations of the Abuse of Artificial Intelligence of Deepfake Technology According to the Personal Data Protection Law.

Artificial intelligence or artificial intelligence (AI) has become one of the technologies that is increasingly developing rapidly and is used in various areas of life, including in the production of deepfake technology. Deepfake technology is a technology that uses AI to create fake videos or audio that closely resemble real people. This technology is predicted to be used for a variety of purposes, such as entertainment, politics, and even for crime, such as fraud and extortion.

In this context, the protection of personal data becomes very important to prevent the misuse of artificial intelligence in the production of deepfake. This is because deepfakes created using AI can pose very serious risks to the privacy and rights of individuals, such as defamation, fraud, and privacy violations.

Therefore, the government has a very important role in supervising and sanctioning violations of the misuse of artificial intelligence deepfake technology. Here are some of the main roles of government agencies in this regard:

1. Supervision of the use of artificial intelligence and deepfake technology. Government institutions, such as the Ministry of Communication and Information (Kominfo) and the State Cyber and Password Agency (BSSN), have a role in overseeing the use of artificial intelligence and deepfake technology in Indonesia. This can be done by issuing regulations and supervising activities carried out by parties who use this technology.
2. Making regulations related to the protection of personal data. Government agencies also have a role in making regulations related to the protection of personal data, such as the Personal Data Protection Law (PDP Law) which was only passed in 2020. This regulation aims to protect the privacy and personal data of individuals from abuse and infringement, including in the case of deepfake.
3. Prosecution of violations of the PDP Law and other related regulations. The government also has the authority to crack down on violations of the PDP Law and other regulations related to the protection of personal data. This violation can be in the form of collection, processing, to the dissemination of personal data without the legal permission of the individual concerned.
4. Giving sanctions to the perpetrator of the violation. In addition to crackdown, government agencies also have the authority to sanction perpetrators of violations of the PDP Law and other

Legal Protection of Artificial Intelligence: Analysis of Deepfake
(Eben E. Silalahi, Bambang Tri Bawono & Jawade Hafidz)

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

regulations related to the protection of personal data. These sanctions can be in the form of fines, closure of access, to revocation of permits owned by the perpetrator of the violation.

5. Cooperation with related parties. The government can also work with related parties, such as law enforcement agencies, the technology industry, and the public, to increase surveillance and prosecution of violations of the misuse of artificial intelligence deepfake technology. This can be done through training and socialization programs, as well as cooperation in conducting research and technology development to detect and prevent deepfake.

Cases related to deepfake technology and violations of personal data protection have also occurred in various countries, including in Indonesia. In 2019, for example, it was revealed that a number of influencers in Indonesia spread video deepfake to promote products illegally. The case led to a polemic and sparked a debate about the need for stricter regulations on deepfakes.

In the other case, in 2020, it was revealed that the personal data of around 1.3 million Indonesians had been leaked and sold illegally on the internet. This data is then used to create deepfake photos and videos that pose a risk of defamation and privacy violations for the individual concerned.

Things like this show that deepfake technology can be a serious threat to individual privacy and rights if not properly monitored and controlled. Therefore, the role of government agencies in supervising and sanctioning violations of the misuse of artificial intelligence deepfake technology is very important to do in order to protect personal data and public privacy.

4. Conclusion

From the explanation that has been explained by the author of the Personal Data Protection Law, it is a law that aims to protect individual personal data from abuse, including in terms of the development of artificial intelligence technology. This is related to the emergence of cases of misuse of Deepfake technology involving individual personal data. Deepfake is a technology that can mimic a person's face and voice to create fake videos that are difficult to distinguish from the original video. In overcoming the challenges that arise due to the development of artificial intelligence technology, the Personal Data Protection Law has established a number of provisions that must be obeyed by each party that processes individual personal data. One of the relevant provisions is the protection of personal data relating to data processing activities using artificial intelligence technology such as Deepfake. In terms of prevention and handling of cases of Deepfake Technology abuse involving individual personal data, the Personal Data Protection Law provides an obligation for each data holder to ensure that the personal data they

Legal Protection of Artificial Intelligence: Analysis of Deepfake
(Eben E. Silalahi, Bambang Tri Bawono & Jawade Hafidz)

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

hold is not misused, including in the case of misuse of Deepfake technology. Parties involved in the processing of personal data must also take adequate data security measures to prevent unauthorized access or use of personal data by unauthorized parties. In addition, government agencies also have an important role in overseeing and sanctioning violations of the misuse of artificial intelligence of Deepfake Technology according to the Personal Data Protection Law. The government agency responsible in this case is the Personal Data Protection Commission (KPPD) which has the authority to supervise and sanction violations of the Personal Data Protection Law. If there is a violation of the use of Deepfake artificial intelligence technology involving individual personal data, the party who commits the violation may be subject to sanctions stipulated in the Personal Data Protection Law, such as administrative sanctions, civil sanctions, and criminal sanctions. This sanction aims to provide a deterrent effect to parties who commit violations so that they can prevent the misuse of personal data in the future. Overall, the implementation of the Personal Data Protection Law in addressing the challenges arising from the development of artificial intelligence technology has shown its effectiveness in protecting individual personal data from abuse, including in cases of misuse of Deepfake Technology involving individual personal data. The role of government agencies that supervise and sanction is also important in maintaining the security and privacy of individual personal data. Therefore, the application of the Personal Data Protection Law must still be improved to face the development of increasingly sophisticated artificial intelligence technologies in the future. Based on the conclusion above, the author suggests that the implementation of the Personal Data Protection Law is very important in facing the challenges arising from the development of artificial intelligence technology, especially related to the prevention and handling of cases of Deepfake Technology abuse involving individual personal data. For this reason, concrete measures are needed such as strengthening regulations that include cases of Deepfake abuse, increasing education and public awareness about the risks of Deepfake, close collaboration between the government, law enforcement agencies, and technology platforms, strengthening supervision by related agencies, and strict sanctions against violations. With these measures, it is hoped that the protection of individual personal data from misuse of artificial intelligence technology, in particular Deepfake, can be improved in accordance with the provisions of the applicable Personal Data Protection Law.

5. References

Legal Protection of Artificial Intelligence: Analysis of Deepfake
(Eben E. Silalahi, Bambang Tri Bawono & Jawade Hafidz)

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

Journals:

- Al-shamasneh, Alaá Rateb Mahmoud, and Unaizah Hanum Binti Obaidellah. 'Artificial Intelligence Techniques for Cancer Detection and Classification: Review Study.' European Scientific Journal 13, no. 3 (January 2017)
- Amboro, FL. Yudhi Priyo, and Khusuf Komarhana. "The Prospect of Artificial Intelligence as a Subject of Civil Law in Indonesia." Law Review 21, no. 2 (November 2021)
- Aqbir, Muhamad Ariq, and Akbar Kurnia Putra. 'Aspect Of International Law in the utilization of Deepfake Technology for The Protection Of Personal Data.' Uti Possidetis: Journal of International Law 2, no. 1 (2021)
- Borges, Luís, Bruno Martins, and Pável Calado. 'Combining Similarity Features and Deep Representation Learning for Stance Detection in the Context of Checking Fake News.' Journal of Data and Information Quality 11, no. 3 (September 2019)
- Budianto, Agus. 'Legal Research Methodology Reposition in Research on Social.' International Journal of Criminology and Sociology 9, (2020)
- Chairani, Meirza Aulia, Angga Pramodya Pradhana, and Taufiq Yuli Purnama. "The Urgency of developing law as a legal basis for the implementation of artificial intelligence in Indonesia." Law and Justice 7, no. 1 (2022)
- 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 (March 2022)
- Reed, Chris. "How Should We Regulate Artificial Intelligence?" Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376, no. 2128 (September 2018)
- Westerlund, Mika. 'The Emergence of Deepfake Technology: A Review.' Technology Innovation Management Review 9, no. 11 (November 2019)

Books:

Legal Protection of Artificial Intelligence: Analysis of Deepfake
(Eben E. Silalahi, Bambang Tri Bawono & Jawade Hafidz)

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

Secretary of State for Science, Innovation and Technology. A pro-innovation approach to AI regulation. United Kingdom: HH Associates Ltd, 2023.

Regulations:

The Constitution of the Republic of Indonesia in 1945.

Law Number 11 of 2008 concerning Electronic Information and Transactions. State Gazette of the Republic of Indonesia Year 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843.

Law Number 27 of 2022 concerning the Protection of Personal Data. State Gazette of the Republic of Indonesia Year 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820.

Internet:

Edwards, Benj. 'Among AI dangers, Deepfakes Worry Microsoft President Most.' Ars Technica, May 26, 2023. <https://arstechnica.com/information-technology/2023/05/microsoft-president-declares-deepfakes-biggest-ai-concern>.

European Commission. 'The EU AI Act's Risk-Based Approach: High-Risk Systems and What They Mean for Users.' Last modified January 16, 2023. <https://futurium.ec.europa.eu/en/european-ai-alliance/document/eu-ai-acts-risk-based-approach-high-risk-systems-and-what-they-mean-users>.

European Parliament. 'EU AI Act: First Regulation on Artificial Intelligence.' Last modified June 14, 2023. <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.

European Parliament. Tackling Deepfakes in European Policy. LU: Publications Office, 2021. <https://data.europa.eu/doi/10.2861/325063>.