CONTEMPORARY ISSUES IN CRIMINAL LAW, (2024), pp. 107-128
ISSN 3064-3139 (Online)

Available online 19 June 2025
https://doi.org/10.20885/CICL.vol1.iss2.art1

Deepfake: A Review from The Victimology Perspective

Doni Noviantama*

Postgraduate Student at Faculty of Law Universitas Islam Indonesia, Yogyakarta, Indonesia, 23912050@students.uii.ac.id, ORCID ID 0009-0008-1068-7084

Alif Alfani Rahman

Postgraduate Student at Faculty of Law Universitas Islam Indonesia, Yogyakarta, Indonesia, 23912052@students.uii.ac.id

Abstract. This study focuses on deepfake as a result of synthetic media that can change a person's image, speech, or actions by utilizing artificial intelligence, which results in heavily realistic outcomes that make someone seem to be doing something when in fact they are not. Thus, it is detrimental to the victim whose face has been manipulated using the deepfake. This study will analyze the characteristics of deepfake, what crimes are born out of deepfake, and how the regulations for victim protection are related to the use of deepfake. The purpose of this study is to determine the characteristics of deepfake, the crimes that come out of it, and the regulations for victim protection relating to the use of deepfake. The method used is normative legal research with a conceptual approach, a statutory approach, and a case study approach. The results of this study indicate that the first characteristic of deepfake is a synthesis technique created using AI, deepfake is made using a person's face as if the person is doing something, the person's face is manipulated without consent, and the results of the manipulation are highly realistic. Then the crimes that arise from deepfakes are pornography, defamation, spreading fake news, fraud, and using other people's personal data without consent. Meanwhile, the protection of deepfake victims is regulated in the Protection of Witnesses and Victims Law, Human Rights Law, Criminal Procedure Code, Government Regulation No. 7 of 2008 in conjunction with Government Regulation No. 35 of 2020 and Regulation of the Minister of Communication and Information Number 5 of 2020 on the Implementation of Private Electronic Systems (Permenkominfo-PSELP). Where victims have the right to make reports/complaints, submit restitution requests, and request a takedown of the deepfake content.

Keywords: Artificial Intelligence, Deepfake, Victim

Abstrak. *Penelitian ini berfokus pada deepfake sebagai hasil media sintesis yang dapat mengubah citra, ucapan, atau tindakan seseorang dengan memanfaatkan artificial intelligence yang hasilnya sangat realistis yang membuat seseorang seolah-olah sedang melakukan sesuatu padahal aslinya tidak. Sehingga merugikan korban yang wajahnya telah dimanipulasi menggunakan deepfake tersebut. Penelitian ini akan menganalisis tentang bagaimana karakteristik deepfake, tindak pidana apa saja yang lahir dari deepfake dan bagaimana regulasi perlindungan korban dalam kaitannya dengan penggunaan deepfake. Tujuan penelitian ini adalah untuk mengetahui bagaimana karakteristik deepfake, tindak pidana apa saja yang lahir dari deepfake dan bagaimana regulasi perlindungan korban dalam kaitannya dengan penggunaan deepfake. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan konseptual, pendekatan perundang-undangan, dan pendekatan kasus. Hasil penelitian ini menunjukkan bahwa karakteristik deepfake yang pertama yaitu teknik sintesis yang dibuat menggunakan AI, deepfake dibuat menggunakan wajah seseorang seolah-olah orang tersebut sedang melakukan sesuatu, wajah orang tersebut dimanipulasi tanpa izin serta hasil manipulasinya sangat realistis. Kemudian tindak pidana yang lahir dari deepfake adalah tindak pidana pornografi, pencemaran nama baik, penyebaran berita bohong, penipuan dan penggunaan data pribadi orang lain tanpa izin. Sedangkan regulasi perlindungan korban deepfake diatur dalam UU PSK, UU HAM, KUHAP, PP 7/208 jo PP 35/2020 dan Permenkominfo-PSELP. Dimana korban berhak untuk membuat laporan/pengaduan, mengajukan permohonan restitusi dan meminta untuk dilakukan takedown terhadap konten deepfake tersebut.*

Kata kunci: *Deepfake, Kecerdasan Buatan, Korban*

Submitted: 18 November 2024 | Reviewed: 25 February 2025 | Revised: 14 May 2025 | Accepted: 16 June 2025

INTRODUCTION

Deepfake is a synthetic media that changes a person's image, speech, or actions. [1] By utilizing artificial intelligence (AI) to replace a person's face with another person and the results are very realistic.[2] Deepfake is a human image synthesis technique based on AI or which is used to combine and place pre-existing images and videos into other image or video sources using machine learning techniques commonly known as generative adversarial networks or GANs. With this GAN, it is possible for someone to produce an entirely new audio from pre-existing audio or produce an entirely new video from pre-existing videos.

Deepfake is a work of AI that can manipulate a person's facial features by using the help of technology. With the said deepfake, a person is able to make a video using someone's face as if they are conducting something, whilst in fact the person in the deepfaked video never performed the depicted activity. In other words, deepfake is a creation using AI that can then select certain biometric data such as a video of a person talking which then reconstructs the person's face in the video onto another person's face by matching the facial movements and voice of the initial person. Thus, deepfake can produce fake data that is identical or at least alarmingly similar to the original data, as if the fake ones are the original ones instead.[3]

The mention of deepfake to address the said method has only been popularized since 2017. It all started from one of the Reddit application users who uploaded an edited pornographic video wherein the said user developed GAN using TensorFlow, a free search engine software from Google to attach a person's face to another woman's body in a pornographic film. The emergence of such deepfake then resurfaced as a heated public discussion once more when a video from Mark Zuckerberg appeared in June 2019 which addressed the power of Facebook to control all data of its users which turned out to be a heavily edited video when in fact, the original video was uploaded

[1] William Sasse, "Deepfakes and the Courtroom," *Maryland Bar Journal* 2, no. 2 (2020): 1.

[2] Eric Koscis, "Deepfakes, Shallowfakes, and the Need for a Private Right of Action," *Dickinson Law Review* 126, no. 621 (2022): 3.

[3] Thefirstly, Chiquita Noerman and Lukman, Aji Ibrahim, "Kriminalisasi Deepfake di Indonesia Sebagai Bentuk Pelindungan Negara," *USM Law Review* 7, no. 2 (2024): 604–7, https://doi.org/http://dx.doi.org/10.26623/julr.v7i2.8995.

by Zuckerberg himself in September 2017 when he discussed the intervention of Facebook in the general election in Russia.[4]

Deepfake serves as evidence that AI, which is currently developing rapidly, is able to create and manipulate a video as if the video was actually performed by the person(s) involved. In fact, it is but a gigantic lie. Initially, deepfake was only used for entertainment purposes, but in its development, deepfake was misused by irresponsible individuals to commit crimes. Where these individuals freely use deepfake technology to edit images or videos with another person's face according to their wishes, which are usually used to commit crimes such as fraud, pornographic content or the spread of fake news.[5] This certainly causes losses for the victims of deepfake whose biometric data in the form of their faces is misused by other people to commit the crime, both material and immaterial losses.

The idea of the present research evolves around the emergence of several recent studies such as; First, an article entitled "Deepfake Criminalization in Indonesia as a Form of State Protection" which examines the absence of regulations that specifically regulate deepfake in Indonesia which currently Indonesia only regulates general personal data falsification in the Personal Data Protection Law as well as electronic falsification in the IT Law. Second, an article entitled "The Urgency of Legal Regulation for Misuse of Deepfake Applications" which examines the absence of concrete regulations related to deepfake in Indonesia wherein presently the state can only prosecute deepfake perpetrators using other laws such as the IT Law, Pornography Law, Child Protection Law and Personal Data Protection Law. From these studies, the authors emphasize that there are fundamental differences in the present article as the focus of the current study discusses the characteristics of deepfake, criminal acts arising from deepfake, and regulations for protecting victims in relation to deepfake-related crimes. Therefore, to limit the discussion in this study,

[4] Hidayatul, Itsna Khusna and Sri Pangestuti, "Deepfake, Tantangan Baru Untuk Netizen Deepfake, a New Challenge for Netizen," *Jurnal Promedia* 5, no. 2 (2019): 1–24, https://doi.org/https://doi.org/10.52447/promedia.v5i2.2300.

[5] Sarah Amanda, Uly Sijabat, and Diana Lukitasari, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik" 13, no. 2 (2024): 180, https://doi.org/10.20956recidive.v7i2.xxxx.

the authors shape the formulation of the problems, namely as follows: first, what are the characteristics of deepfake? second, what criminal acts arise from deepfake? and third, how are the regulations for victim protection in relation to the use of deepfakes?

METHODOLOGY

This is a normative legal research whose focus is carried out using a conceptual approach to elaborate on what is defined as a deepfake along with its characteristics. In the present study, the authors likewise employed a statutory approach on those which explicitly regulate deepfake, namely Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (IT Law), Law No. 44 of 2008 on Pornography, Law No. 27 of 2022 on Personal Data Protection (PDP Law) and the Criminal Code as well as regulations governing the rights of deepfake victims as regulated in Law No. 8 of 1981 on Criminal Procedure Law, Law No. 31 of 2014 on Amendments to Law No. 13 of 2006 on Protection of Witnesses and Victims (PSK Law), Government Regulation No. 7 of 2018 on Provision of Compensation, Restitution and Assistance to Witnesses and Victims as amended by Government Regulation No. 35 of 2020 and Regulation of the Minister of Communication and Information Number 5 of 2020 on the Implementation of Private Electronic Systems (*Permenkominfo-PSELP*). In addition, this study also utilises a case study approach used in analyzing criminal acts arising from deepfake such as cases of the use of deepfake to commit crimes of pornography, defamation, fraud and misinformation or the spreading of fake news. These three approaches are used in this study because the theoretical aspects of deepfake must first be elaborated conceptually, then continued with its application in various cases of criminal acts arising from deepfake along with its legal basis and subsequently continued with an analysis of victim protection regulations in relation to deepfake and its legal basis. The primary legal materials in this study consist of ITE Law, Law No. 44 of 2008 on Pornography, PDP Law and the Criminal Code, Law No. 8 of 1981 on Criminal Procedure, PSK Law, Government Regulation No. 7 of 2018 on Provision of

Compensation, Restitution and Assistance to Witnesses and *Permenkominfo-PSELP*. Consequently, the study is analyzed using a descriptive-qualitative method.

RESULT AND DISCUSSION

The Characteristics of Deepfake

Crime is growing very rapidly along with the development of technology. At this rate, human civilization has eventually peaked at the industrial era of 4.0, which is marked by the use of digital technology such as the Internet of Things (IoT), big data, augmented reality, and Artificial Intelligence (AI). This very rapid technological development, besides rendering a positive impact on human life, also poses a negative impact on human life. One of the negative impacts is the emergence of new crimes by utilizing technological developments such as AI.[6]

AI is one of the results of technological developments that greatly facilitate human life. AI was originally created by an American mathematician named John McCarthy in 1955 and over time, AI has now reached various sectors of people's lives. In its development, AI technology has sparked a new technology called deepfake. Deepfake is a work of AI that is used to engineer or manipulate images or videos of an event with deep learning techniques that perform comprehensive and basic scanning of human images.[7]

Deepfake was initially only used for entertainment purposes, however in its development, deepfake was misused by irresponsible individuals to commit crimes. These individuals freely use deepfake technology to edit images or videos of a person's face as the perpetrators wish, which are usually used to commit crimes such as fraud, pornographic content or spreading fake news.[8]

Deepfake as a result of AI has several characteristics. First, deepfake is a human image synthesis technique created using AI that is used to combine and place pre-existing

[6] Amanda, Sijabat, and Lukitasari.
[7] Koscis, "Deepfakes, Shallowfakes, and the Need for a Private Right of Action."
[8] Amanda, Sijabat, and Lukitasari, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik."

images and videos into a whole new image or video source using machine learning techniques commonly known as generative adversarial networks or GANs. With the said GAN, it is possible for a person to produce an entirely new audio from the pre-existing audio or produce an entirely new video from the pre-existing videos. The way deepfakes work is by manipulating a person's facial features using the help of AI technology. Where an image or video can be combined with a particular method in a way that makes the results look extremely real.[9]

Whilst in fact, the image or video is the result of manipulation since deepfake technology can manipulate a subject's expression by synthesizing a person's face and expression using AI and facial mapping knowledge and a person's expression using AI and facial mapping knowledge to create edited images and videos that look like the original.[10]

The second characteristic, deepfake technology, can create videos using a person's face as if they are performing a certain activity, where in fact the person in the video never conducted as such. In other words, deepfake is a creation using AI that can cherry-pick biometric data such as a video of a person talking which then reconstructs the face of a person in the video to the face of another person by matching the facial movements and voice of the person. Thus, deepfake can produce fake data that is identical or very similar to the original data as if the fake data is the original data.[11] The example is the infamous Barack Obama video that has been watched by more than 6.4 million YouTube viewers. In fact, the video is a result of engineering from the original Barack Obama video in 2017 which was pasted with a new video from someone using deepfake technology.

The third characteristic of deepfake is that deepfake technology works by manipulating other people's faces without their consent. This occurs due to the fact that deepfake can manipulate facial expressions, identities, or attributes of a subject

[9] Aulia, Meirza Chairani, Yitawati Krista, and Pradhana Pramodya Angga, "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake," *Jurnal Rechtens* 13, no. 1 (June 2024): 88.

[10] Amanda, Sijabat, and Lukitasari, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik."

[11] Noerman and Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara."

by synthesizing a person's face and expressions using AI to make existing images or videos look real or original and the images or videos resulting from deepfake manipulation are very difficult to distinguish from the original content. This is certainly detrimental to the owner of the original face or identity whose images or videos are edited using deepfake technology which is used to spread false information, information with content that violates morality, manipulates or falsifies data, and defames a person's good name. In fact, a good name is something that is very valuable to each individual so it needs to be maintained and preserved. This deepfake phenomenon clearly makes many people feel disadvantaged, especially if the image or video is used to commit a crime.[12]

The fourth characteristic of deepfake is the result of deepfake manipulation that replaces a person's face with another person's face, the results are very realistic and seem real and very difficult to identify if the image or video is the result of deepfake. Since deepfake is heavily difficult to identify, deepfake is currently a very significant threat to individuals, organizations and society.[13] This resulted from the use of synthetic media of photos, images or those created with AI within the scheme of deepfake to convincingly change or completely manipulate a person's appearance and voice.[14] In other words, deepfake is the result of AI in the form of distorted images, videos or audio that are highly convincing thus it seems as if something which did not happen materialized as if it did and it is cruciatingly difficult to identify if the image, video or audio is the result of deepfake, since the said results look real and realistic.[15]

Crimes that Arise from Deepfake

Deepfake is a synthetic media that alters a person's image, speech, or actions.[16] by utilizing artificial intelligence (AI) to replace a person's face with another's.[17] In other

[12] Amanda, Sijabat, and Lukitasari, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik."

[13] Koscis, "Deepfakes, Shallowfakes, and the Need for a Private Right of Action."

[14] Bridget Grathwohl, "Preserving Truth on the Prairie: Navigating Deepfake Challenges to Self-Authenticating Evidence in North Dakota Courts," *North Dakota Law Review* 99, no. 657 (2024): 2.

[15] Bradley Waldstreicher, "Deeply Fake, Deeply Disturbing, Deeply Constitutional: Why the First Amendment Likely Protects the Creation of Pornographic Deepfakes," *Cardozo Law Review* 42, no. 729 (2021): 2.

[16] Sasse, "Deepfakes and the Courtroom."

[17] Koscis, "Deepfakes, Shallowfakes, and the Need for a Private Right of Action."

words, deepfake technology is the result of AI that manipulates videos or photos realistically by combining a person's face with another's.[18] Where the results of manipulation from deepfakes in the form of photos or videos are very difficult to identify because the results are very realistic and it is difficult to distinguish whether the photo or video is genuine or the result of deepfake.[19]

Deepfake was initially used sparingly for the purpose of entertainment, however in its development, deepfake has actually been misused by irresponsible individuals to commit criminal acts. A criminal act is an act that is prohibited by a legal rule that carries its own threat or sanction in the form of a certain criminal penalty for any individual who violates the prohibition.[20] Some of the crimes that arise from deepfakes are as follows:

1. Crimes of Pornography

Pornography is a writing, picture or film designed for a person's sexual needs, satisfaction or pleasure. Pursuant to a Greek word *pornographia*, pornography is a writing or picture that reeks of prostitution.[21] If we look into the provisions of Article 1 paragraph 1 of Law No. 44 of 2008 on Pornography, it is apparent that what is defined as pornography is every image, sketch, illustration, photo, writing, voice, sound, moving image, animation, cartoon, conversation, body movement or other form of message through various forms of communication media and/or public performances that contain obscenity or sexual exploitation that violates moral norms in the society.[22]

Presently, the distribution of pornographic content is increasingly rampant through social media or often referred to as cyberporn. The crime of spreading pornography is categorized as an act that violates morality. Therefore, a person who spreads

[18] Pechenik, Anne Gieseke, "The New Weapon of Choice: Law's Current Inability to Properly Address Deppfake Pornography," *Vanderbilt Law Review* 73, no. 1479 (October 2020): 2.

[19] Dewi, Ivana Kasita, "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19," *Jurnal Wanita Dan Keluarga* 3, no. 1 (July 2022): 18.

[20] Ainuddin, *Hukum Acara Pidana Dari Teori Ke Praktek*, ed. Syahida, Siti Nuraini, 1st Ed. (Yogyakarta: Genta Publishing, 2020).

[21] Yesami, Louisa Krisnalita and Siti Rahayu, "Analisis Yuridis Mengenai Tindak Pidana Pornografi Secara Berlanjut," *Justice Voice* 1, no. 2 (December 2024): 72–73.

[22] "Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi," Pub. L. No. 44 (2008).

cyberporn content can be subject to criminal sanctions. This is as regulated in Article 45 paragraph (1) of the IT Law.[23]

Cyberporn crimes that are currently rampant are not only carried out by perpetrators by spreading original content, but also by spreading pornographic content from deepfake technology. Where the perpetrators can manipulate the victim's face to look like someone else's face, thus they are able to create deepfake porn content.[24] Deepfake porn is a technique for taking and manipulating videos realistically by combining one person's face with another person's real face in the form of a pornographic video to give the impression that the person is actually committing an immoral act.[25]

The emergence of deepfake porn has caused unrest in the civil society as it is heavily detrimental to the person whose face has been manipulated as if they were the actor performing in the pornographic video. The content of deepfake porn is deeply degrading to the dignity of a person, both men and women whose faces have been manipulated through the deepfake application. One of the victims of deepfake porn is a feminist media critic named Anita Sarkeesian, whose face was displayed in a deepfake pornographic video titled "*hardcore*" which has been watched over 30,000 times on the *porn hub* site.[26]

2. Crime of Defamation

Defamation is an act that damages a person's good name or honor or an act that degrades the dignity and honor of another person.[27] Attacks on a person's good name usually occur when the perpetrator says words or a series of words/sentences by accusing the person of something if the person has committed a certain act with the aim of tarnishing the honor and good name of a person in such a way that the person's

[23] "Law Number 1 of 2024 amending Law Number 11 of 2008 on Information and Electronic Transaction," Pub. L. No. 1 (2024).

[24] Utawi, Eva Istia, and Neni Ruhaeni. "Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial." In *Bandung Conference Series: Law Studies*, 3 (2023): 365.

[25] Oktallia, Vika, and I Gede Putra Ariana. "Perlindungan Terhadap Korban Penyalahgunaan Teknik Deepfake Terhadap Data Pribadi." *Jurnal Kertha Desa* 10 (2022): 1254.

[26] Gieseke, "The New Weapon of Choice: Law's Current Inability to Properly Address Deepfake Pornography."

[27] Muchladun, Wildan. "Tinjauan Yuridis Terhadap Tindak Pidana Pencemaran Nama Baik." Tadulako University, 2015.

self-respect or dignity is insulted and tarnished.[28] The crime of defamation is an act that is prohibited and is subject to criminal penalties as regulated in Chapter XVI of the Criminal Code, namely Articles 310 to 321 of the Criminal Code and Article 27A in conjunction with Article 45 paragraph (4) of the IT Law.[29]

The meaning of attack in the act of defamation is not interpreted as a physical attack, but rather as an attack on a person's honor and good name. The meaning of honor is a feeling of dignity that someone has in the eyes of society. Meanwhile, a good name is a self-esteem or dignity that is based on the good views or assessments of society towards someone. Thus, it can be concluded that honor and good name have different meanings, yet both are inseparable since the act of attacking a person's honor will subsequently result in the person's good name being likewise tarnished.[30]

Defamation can also be interpreted as a false statement intended to expose, ridicule, spread hatred, embarrass a person or create a negative view of that person in the minds of the public. Defamation resulting from deepfake content is very different from the form of defamation in general. Basically, the perpetrator makes the deepfake content intended for entertainment only, but in fact the outcomes of the deepfake content actually result in a person's reputation, honor and good name being tarnished.[31]

Defamation through deepfake usually occurs when the perpetrator creates deepfake porn content. The results of deepfake porn content are included in the category of defamation because such outcomes are categorized as acts that attack the honor and good name of others which are carried out by accusing a certain act that makes the person feel embarrassed or degraded, including accusing someone of being involved in pornographic content whereas in fact the video is the result of manipulation of deepfake technology. The existence of the deepfake porn video causes the victim's

[28] Chazawi, Adami. *Hukum Pidana Positif Penghinaan*. Media Nusa Creative (MNC Publishing), 2022.

[29] Setiawan, Iwan. "Kajian Terhadap Pencemaran Nama Baik Melalui Facebook." *Jurnal Ilmiah Galuh Justisi* 7, no. 1 (2019): 39–48.

[30] Mahrus Ali, "Pencemaran Nama Baik Melalui Sarana Informasi Dan Transaksi Elektronik (Kajian Putusan MK No. 2/PUU-VII/2009)," *Jurnal Konstitusi* 7, no. 6 (December 2010): 126–27.

[31] Ibid

good name to be defamed and tarnished.[32] One prime example of the case is an offense conducted by M, a woman from Kediri who is suspected of spreading a pornographic video wherein the face of the actor is similar to that of a singer named Rini Fatimah Jaelani or commonly known as Syahrini. For her actions, M was arrested by investigators from Polda Metro Jaya on the grounds of defaming Syahrini.[33]

3. Crime of Misinformation and Hoax

The spread of fake news or what is more commonly known as a hoax is information that contains lies, slander and fabrication that is not true and misleading in nature. The spread of fake news or hoaxes is not merely spreading misleading fake news, but often there are hidden motives from the perpetrators of the spread of hoax news which result in losses for the people who are made the subjects of the fake news, such losses cover both material and immaterial ones.[34]

The rapid development of internet technology and the advancement of social media have made it very easy for people to create fake news or hoaxes. The main goal of those spreading fake news is to influence public opinion towards certain information so that people feel sure and believe in the information, even though in fact the information is fake information or fake news. This fake news content can be created using deepfake technology by manipulating videos, images or voices of a person as if the person is conveying information in a real and realistic way.

An example of a fake news case created using the deepfake technology is a video recording of a voice between Anies Baswedan and Surya Paloh after the 2024 Indonesian Presidential Debate. In the video recording, the voice contains a narrative that Anies Baswedan is being scolded by the General Chairperson of the Nasdem Party, Surya Paloh, because the results of the 2024 Presidential Election survey are always at the bottom. The video recording then went viral on various social media

[32] Amanda, Sijabat, and Lukitasari.

[33] Yusuf, M Manurung, "Polisi Sebut Identitas Wanita Penyebar Video Porno Mirip Syahrini," https://metro.tempo.co/read/1346858/polisi-sebut-identitas-wanita-penyebar-video-porno-mirip-syahrini, May 3, 2020.

[34] Basrief Aryanda, "Tindak Pidana Penyiaran Berita Bohong Dalam Putusan Pengadilan Negeri Jakarta Selatan Nomor 203/Pid.Sus/2019/Pn.Jkt.Sel," *Locus Journal of Academic Literature Review* 3, no. 4 (April 2024): 337, https://doi.org/https://doi.org/10.56128/ljoalr.v3i4.313.

platforms and many people believed the video recording. Seeing the virality of his video recording, Anies Baswedan then provided clarification that the video recording of the conversation was not true or a lie. Anies Baswedan explained that technological advances are often misused by certain individuals. One way is by utilizing AI applications such as deepfake to manipulate images, audio and videos of other people as if they were real.[35]

4. Crime of Fraud

The crime of fraud is a series of acts of persuading others by trickery, a series of lies, a false name or a false statement so that others give something. The crime of fraud has been regulated in Article 378 of the Criminal Code. Along with the development of the times, criminal acts of fraud develop as well. Nowadays, not only can it be carried out directly, but also by utilizing the development of internet technology. One of the *modus operandi* of fraudsters through electronic media is by manipulating a person's voice identity so that the victim would believe that a close relative of them is asking for help to borrow some money. Where through this mode, the perpetrator will use a voice that is the result of deepfake manipulation so that his voice sounds exactly like a family member who is asking for help. As a result, the victim who fell for the trick eventually complies with the perpetrator's wishes by transferring money.[36] An example of a criminal case of fraud using deepfake technology occurred in Hong Kong, where the perpetrator managed to trick a worker into being conned out of US$ 25 million or approximately Rp. 392 billion.[37]

5. Crime of Misuse of Personal Data

Personal data refers to data of an individual who is identified or can be identified individually or in combination with other information either directly or indirectly

[35] CNN Indonesia, "Anies Buka Suara Soal Hoaks Rekaman Dimarahi Surya Paloh," https://www.cnnindonesia.com/nasional/20240124064555-617-1053546/anies-buka-suara-soal-hoaks-rekaman-dimarahi-surya-paloh, January 3, 2024.

[36] M, Ahmad Ramli, "'Deepfake, AI-Crime', UU PDP, Dan KUHP Baru," https://www.kompas.com/tren/read/2023/10/14/154802465/deepfake-al-crime-uu-pdp-dan-kuhp-baru?page=all#page2, October 2023.

[37] CNBC Indonesia, "Penipuan Deepfake Kuras Duit Rp 392 M, Kominfo Kasih Peringatan Ini," https://www.cnbcindonesia.com/tech/20240424161935-37-533098/penipuan-deepfake-kuras-duit-rp-392-m-kominfo-kasih-peringatan-ini, April 2024.

through electronic or non-electronic systems. As regulated in Article 4 paragraph (1) of Law No. 27 of 2022 on PDP Law, personal data consists of both specific and general data. Specific personal data consists of health data and information, biometric data, genetic data, crime records, child-related data and personal financial data. While general personal data consists of full name, gender, citizenship, religion, marital status and personal data combined to identify a person.[38]

If we look into the explanation of personal data as regulated in the PDP Law, a person's face is part of the biometric data that is protected by law. Biometrics is the recognition of a person's identity based on physical form such as face, fingerprints, palm lines, eye retina or the human voice.[39] Therefore, if a person uses deepfake technology to make a video using the face of another person as if they were conducting something, even though in fact the latter never did as such.[40] In this regard, the action is categorized as an unlawful act and the perpetrator can be subject to criminal sanctions. This is as regulated in Article 67 paragraph (1) of the PDP Law.

One example of a criminal act of using biometric data in the form of a person's face by manipulating them using deepfake technology as if the person is performing the accused act is a video of former President Joko Widodo giving a speech in Mandarin fluently. This caused a commotion on social media that which was immediately responded to by the Ministry of Communication and Information which stated that the video of former President Joko Widodo giving a speech in Mandarin was a video edited using AI in the form of deepfake.[41]

Regulations on the Protection of Victims in Relation to the Use of Deepfakes

The study of victimology is defined within the terminological context which bears the meaning as a branch of science that studies the victims of criminal acts, the circumstantial causes that lead to the emergence of the victims and the consequences

[38] "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," Pub. L. No. 27 (2022).

[39] Sugeng Widodo and Supatman, "Prototype Desain Keamanan Login Menggunakan Biometrik Wajah Dengan Metode Eigenface," *Jurnal Multimedia & Artificial Intellegence* 4, no. 1 (February 2020): 35.

[40] Noerman and Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara."

[41] Gibran Maulana, "Beredar Vidio Jokowi Fasih Mandarin, Kominfo: Editan AI Menyesatkan!," https://news.detik.com/berita/d-7003320/beredar-video-jokowi-fasih-mandarin-kominfo-editan-ai-menyesatkan, October 2023.

derived from the existence of victims of criminal acts. Whereas the notion of a victim according to J. E. Sahetapy is an individual or legal entity who suffers injuries, damage or other forms of loss that are felt either physically or mentally. These losses are not only seen from the legal side, but also from an economic, political, social or cultural perspective. Those who become victims of criminal acts can occur because of the victim's own fault, because of the victim's role directly or indirectly in a criminal act or without the role of the victim of the criminal act.[42]

The definition of a victim of a crime can also be found within the results of the United Nations conference held in Milan, Italy in September 1985, which asserted that a victim is a person who individually or in a group has suffered losses, including physical or mental, emotional suffering, economic loss, or deprivation of their basic rights, either due to actions or negligence. Meanwhile, according to Article 1 number 3 of Law Number 31 of 2014 on the Amendments to Law Number 13 of 2006 on the Protection of Witnesses and Victims, a victim is a person who experiences physical, mental and/or economic loss caused by a crime.[43]

The importance of protecting the victims of crime has received serious attention from various countries in the world. This can be seen in the Declaration of Fundamental of Justice for Victims of Crime and Abuse of Power by the UN which is the result of the Seventh United Nations Congress on the Crime and the Treatment of Offenders held in Milan in 1985. One of the recommendations resulting from the congress states that the offender or third party is responsible for their behavior. If necessary, they must provide fair compensation to the victims or their families. The restitution includes payment for losses suffered by the victim as well as reimbursement of costs incurred as a result of victimization, namely the provision of services and restoration of rights. Legal protection for victims is a form of service that must be provided by the government in order to provide a sense of security to all citizens, including citizens who are victims of crime.

---

[42] John Kenedi, *Perlindungan Saksi Dan Korban (Studi Perlindungan Hukum Korban Kejahatan Dalam Sistem Peradilan Di Indonesia)*, ed. Hariyanto, Pertama (Yogyakarta: Pustaka Pelajar, 2020).

[43] "Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban," Pub. L. No. 31 (2014).

According to Philipus M. Hadjon, the form of legal protection provided by the state is divided into two, namely preventive legal protection and repressive legal protection. Preventive legal protection aims to prevent the occurrence of disputes that lead to government action to be careful when wanting to make decisions based on discretion. Whilst the repressive legal protection aims to resolve a case that has already occurred, including handling it through the judicial institution.[44]

As a joint commitment to ensure protection for victims of criminal acts and to carry out the mandate of the 1945 Constitution of the Republic of Indonesia, the government together with the DPR ratified Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Protection of Witnesses and Victims (PSK Law) while simultaneously establishing the Witness and Victim Protection Agency or commonly referred to as LPSK. If seen in the provisions of Article 5 paragraph (1) of the PSK Law, victims of criminal acts have the right to protection from the state, including the victim has the right to obtain protection for the security of their person, family, and property and to be free from threats relating to testimony that will be given, is being given, or has been given and receive legal advice.[45]

Regulations regarding protection for victims of crime are also implied in Article 3 paragraph (2) of Law Number 39 of 1999 on Human Rights (Human Rights Law) which states that "Every person has the right to recognition, guarantees, protection and fair legal treatment and to receive legal certainty and equal treatment before the law". In addition, Article 5 paragraph (1) of the Human Rights Law likewise explains that everyone is recognized as a human being who has the right to demand and receive equal treatment and protection in accordance with their human dignity before the law. Not only that, Human Rights Law additionally regulates that everyone has the right to protection for themselves, their families, their honor, their dignity and their property rights. Therefore, it can be concluded that the Human Rights Law is one of the laws that regulates victims of crime, considering the element of "every

[44] Jesaldi, Frits Leunupun, Sherly Adam, and Iqbal Taufik, "Perlindungan Hukum Terhadap Pelaku Tindak Pidana Yang Menjadi Korban Penganiayaan Massa," *TATOHI Jurnal Ilmu Hukum* 2, no. 11 (2023): 1142.

[45] Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

person" in the Human Rights Law can also be interpreted as a victim of crime as the words "every person" referred to in the Human Rights Law generally refers to all people without exception.[46]

Derived from the discussion above, victims of criminal acts shall be satisfied with a fair coverage of rights that have been guaranteed by the state, which extends to deepfake victims as well whereby the use of deepfake technology allows the perpetrator to manipulate a person's facial features using the help of AI technology. This certainly causes losses for the victims of deepfake whose biometric data in the form of their faces is misused by others to commit crimes, such as for pornographic content, defamation, fake news or used to commit fraud. Thus, undoubtedly, the said victim does possess the right to legal protection from the state, which shall include:

1. Deepfake victims have the right to submit reports or complaints to the police officer regarding the criminal acts that have occurred. Based on the provisions of Law Number 8 of 1981 on Criminal Procedure Law, it is provided that a report is a notification submitted by a person due to their rights or obligations under the law to an authorized official on a criminal event that has occurred, is occurring or is suspected of occurring. A complaint is a notification accompanied by a request by an interested party to an authorized official to take legal action against a person who has committed a criminal complaint that is detrimental to them.[47] If the action taken by the deepfake perpetrator is a crime categorized as a common crime such as fraud, then the victim can submit a report to the police. However, if the action taken by the deepfake perpetrator is a crime categorized as a complainant crime such as defamation, then the victim can submit a complaint to the police;
2. Deepfake victims have the right to apply for restitution to request compensation from the perpetrators of the crime. This is as regulated in Government Regulation Number 7 of 2018 on the Provision of Compensation, Restitution, and Assistance to Witnesses and Victims as amended by

[46] Law Number 39 of 1999 on Human Rights
[47] "Law Number 8 of 1981 on Criminal Procedure," Pub. L. No. 8 (1981).

Government Regulation Number 35 of 2020, specifically in Article 19 paragraph (1) which states that victims of a crime have the right to receive restitution in the form of compensation for loss of wealth or income, compensation for losses caused by suffering directly related to the crime and/or reimbursement of medical and/or psychological care costs. Where the application to obtain restitution can be submitted in writing by the victim, the family or relatives of the victim or their attorney through the Witness and Victim Protection Agency (**Lembaga Perlindungan Saksi dan Korban**, LPSK).[48] The application for restitution can be submitted before or after the court decision has obtained its permanent legal force status. If the application for restitution is submitted before the court decision has obtained its permanent legal force status, then the LPSK can submit restitution to the Public Prosecutor to be included in the letter of demand;

3. Deepfake victims have the right to request that access be terminated (takedown) to the authorized Ministry or Institution for deepfake content that has been circulating on social media. The measure to terminate access (takedown) has been regulated in the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 5 of 2020 on Private Electronic System Organizers (hereinafter referred to as *Permenkominfo-PSELP*). Article 1 paragraph 15 of *Permenkominfp-PSELP* states that terminating access refers to the action of blocking access, closing accounts and/or deleting content. Wherein the content that is terminated (takedown) refers to any electronic information or electronic document that does not comply with the provisions in Article 9 paragraph (4), namely content that violates the provisions of laws and regulations and content that disturbs the public and disrupts public order, including content resulting from deepfake. This request for termination of access (takedown) can be submitted by the public, Ministries or Institutions, Law Enforcement Officers and Judicial

[48] "Government Regulation Number 7 of 2018 on Provision of Compensation, Restitution and Assistance to Witnesses and Victims as amended by Government Regulation Number 35 of 2020," Pub. L. No. 35 (2020).

Institutions with several requirements as stipulated in Articles 15 to 17 of the *Permenkominfo-PSELP*. In addition, termination of access (takedown) by deleting content is regulated in Article 26 paragraph (3) of Law No. 19 of 2016 on Amendments to Law 11 of 2008 on Information and Electronic Transactions which states that every electronic system organizer is required to delete irrelevant electronic information and/or electronic documents under its control at the request of the person concerned based on a court ruling. The deletion of irrelevant content is also further regulated in Article 15 paragraph (2) of Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions which reads "The obligation to delete irrelevant Electronic Information and/or Electronic Documents as referred to in paragraph 1 consists of: a. deletion (right to erasure); and b. removal from the search engine list (right to delisting)".[49]

CONCLUSION

Derived from the discussion above, the authors have concluded that deepfake is a work of AI that is used to engineer or manipulate images, videos or voices of a person with deep learning techniques that produce a highly realistic work, as if the face or voice of the person in the image or video is real even though it is merely the result of high engineering. The results of the analysis above indicate that deepfake, which was previously used solely for entertainment purposes but in its development, has instead been misused by irresponsible individuals to commit crimes, such as pornography, defamation, spreading fake news, fraud, and the crime of using other people's personal data without their consent. This then results in victims whose faces or voices are used for deepfake content experiencing losses, both materially and immaterially. So that victims of deepfakes have the right to obtain legal protection from the state. Although currently, the provisions regarding criminal acts related to deepfake, along

with legal protection for deepfake victims, are regulated in various types of laws and regulations and various Ministerial Regulations.

Therefore, the authors would like to offer recommendations on the creation of novel provisions regarding prohibited acts related to deepfakes as well as criminal sanctions in the form of fines and imprisonment. These recommendations can be implemented by creating new administrative criminal laws regarding AI and deepfake or simply inserting new provisions regarding deepfake in the PDP Law and the IT Law. In that regard, it is our hope that it would become clearer to categorize which actions are included as part of a deepfake crime in order to establish legal certainty for the community. In addition, it is necessary to regulate in a more specific manner regarding the rights of victims and the form of legal protection for deepfake victims, which provisions can be inserted in the new administrative criminal law regarding AI and deepfake or inserted in the PDP Law, the IT Law or the Regulation of the Minister of Communication and Information which specifically discusses AI and deepfake. This needs to be regulated clearly and firmly, since this far, the provisions of norms governing the rights of victims of criminal acts remain scarce when compared to the provisions of norms governing the rights of perpetrators of criminal acts, in this case, the suspects as well as the defendants.

ACKNOWLEDGMENTS

The authors would like to express their deepest gratitude to all parties who have aided the authors in conducting this research, both in the inputs as well as suggestions.

COMPETING INTEREST

The authors declare that there is no conflict of interest in the publication of this study.

REFERENCES

Ainuddin. *Hukum Acara Pidana Dari Teori Ke Praktek*. Edited by Syahida, Siti Nuraini. 1st Ed. Yogyakarta: Genta Publishing, 2020.

Ali, Mahrus. "Pencemaran Nama Baik Melalui Sarana Informasi Dan Transaksi Elektronik (Kajian Putusan MK No. 2/PUU-VII/2009)." *Jurnal Konstitusi* 7,

no. 6 (December 2010): 126–27.

Amanda, Sarah, Uly Sijabat, and Diana Lukitasari. "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik" 13, no. 2 (2024): 180. https://doi.org/10.20956recidive.v7i2.xxxx.

Aryanda, Basrief. "Tindak Pidana Penyiaran Berita Bohong Dalam Putusan Pengadilan Negeri Jakarta Selatan Nomor 203/Pid.Sus/2019/Pn.Jkt.Sel." *Locus Journal of Academic Literature Review* 3, no. 4 (April 2024): 337. https://doi.org/https://doi.org/10.56128/ljoalr.v3i4.313.

Chairani, Aulia, Meirza, Yitawati Krista, and Pradhana Pramodya Angga. "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake." *Jurnal Rechtens* 13, no. 1 (June 2024): 88.

CNBC Indonesia. "Penipuan Deepfake Kuras Duit Rp 392 M, Kominfo Kasih Peringatan Ini." https://www.cnbcindonesia.com/tech/20240424161935-37-533098/penipuan-deepfake-kuras-duit-rp-392-m-kominfo-kasih-peringatan-ini, April 2024.

CNN Indonesia. "Anies Buka Suara Soal Hoaks Rekaman Dimarahi Surya Paloh." https://www.cnnindonesia.com/nasional/20240124064555-617-1053546/anies-buka-suara-soal-hoaks-rekaman-dimarahi-surya-paloh, January 3, 2024.

Gieseke, Pechenik, Anne. "The New Weapon of Choice: Law's Current Inability to Properly Address Deepfake Pornography." *Vanderbilt Law Review* 73, no. 1479 (October 2020): 2.

Grathwohl, Bridget. "Preserving Truth on the Prairie: Navigating Deepfake Challenges to Self-Authenticating Evidence in North Dakota Courts." *North Dakota Law Review* 99, no. 657 (2024): 2.

Husna, Triari, Hanifah. "Sampai Mei 2023, Kominfo Identifikasi 11.642 Konten Hoaks." www.kominfo.go.id, June 2023.

Kasita, Dewi, Ivana. "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19." *Jurnal Wanita Dan Keluarga* 3, no. 1 (July 2022): 18.

Kenedi, John. *Perlindungan Saksi Dan Korban (Studi Perlindungan Hukum Korban Kejahatan Dalam Sistem Peradilan Di Indonesia)*. Edited by Hariyanto. Pertama. Yogyakarta: Pustaka Pelajar, 2020.

Khusna, Hidayatul, Itsna, and Sri Pangestuti. "Deepfake, Tantangan Baru Untuk Netizen Deepfake, a New Challenge for Netizen." *Jurnal Promedia* 5, no. 2 (2019): 1–24. https://doi.org/https://doi.org/10.52447/promedia.v5i2.2300.

Koscis, Eric. "Deepfakes, Shallowfakes, and the Need for a Private Right of Action." *Dickinson Law Review* 126, no. 621 (2022): 3.

Krisnalita, Yesami, Louisa, and Siti Rahayu. "Analisis Yuridis Mengenai Tindak Pidana Pornografi Secara Berlanjut." *Justice Voice* 1, no. 2 (December 2024): 72–73.

Leunupun, Jesaldi, Frits, Sherly Adam, and Iqbal Taufik. "Perlindungan Hukum Terhadap Pelaku Tindak Pidana Yang Menjadi Korban Penganiayaan Massa." *TATOHI Jurnal Ilmu Hukum* 2, no. 11 (2023): 1142.

Manurung, Yusuf, M. "Polisi Sebut Identitas Wanita Penyebar Video Porno Mirip Syahrini." https://metro.tempo.co/read/1346858/polisi-sebut-identitas-wanita-penyebar-video-porno-mirip-syahrini, May 3, 2020.

Maulana, Gibran. "Beredar Vidio Jokowi Fasih Mandarin, Kominfo: Editan AI Menyesatkan!" https://news.detik.com/berita/d-7003320/beredar-video-jokowi-fasih-mandarin-kominfo-editan-ai-menyesatkan, October 2023.

Noerman, The firstly, Chiquita, and Lukman, Aji Ibrahim. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara." *USM Law Review* 7, no. 2 (2024): 604–7. https://doi.org/http://dx.doi.org/10.26623/julr.v7i2.8995.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, Pub. L. No. 5 (2020).

Peraturan Pemerintah Nomor 7 Tahun 2018 tentang Pemberian Kompensasi, Restitusi dan Bantuan kepada Saksi dan Korban sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 35 Tahun 2020, Pub. L. No. 35 (2020).

Ramli, M, Ahmad. "'Deepfake, AI-Crime', UU PDP, Dan KUHP Baru." https://www.kompas.com/tren/read/2023/10/14/154802465/deepfake-al-crime-uu-pdp-dan-kuhp-baru?page=all#page2, October 2023.

Sasse, WIlliam. "Deepfakes and the Courtroom." *Maryland Bar Journal* 2, no. 2 (2020): 1.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pub. L. No. 1 (2024).

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, Pub. L. No. 8 (1981).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pub. L. No. 27 (2022).

Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, Pub. L. No. 31 (2014).

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Pub. L. No. 39 (1999).

Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Pub. L. No. 44 (2008).

Waldstreicher, Bradley. "Deeply Fake, Deeply Disturbing, Deeply Constitutional: Why the First Amendment Likely Protects the Creation of Pornographic Deepfakes." *Cardozo Law Review* 42, no. 729 (2021): 2.

Widodo, Sugeng, and Supatman. "Prototype Desain Keamanan Login Menggunakan

Biometrik Wajah Dengan Metode Eigenface." *Jurnal Multimedia & Artificial Intelligence* 4, no. 1 (February 2020): 35.