International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 1
January, 2023
Pages: 383-390

Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia

Isnaini Imroatus Solichah; Faizin Sulistio; Milda Istiqomah

Program Studi Magister Ilmu Hukum, Fakultas Hukum Universitas Brawijaya, Indonesia

http://dx.doi.org/10.18415/ijmmu.v10i1.4409

Abstract

Deepfake containing pornographic elements is a phenomenon of sexual violence in which the majority of victims are women. This is because pornographic content is generally created by and for male viewers. In some cases, celebrities are the first and foremost targets for victims of these pornographic deepfakes. The reason why they are celebrities is because their photos and videos are so easy to come by. However, pornographic deepfake victims are no longer limited to celebrities and public figures, anyone can become a pornographic deepfake victim. Nowadays it's easier for perpetrators to steal photos of victims, especially through social media, the greater the opportunity for misuse in the form of making deepfakes. Victims of deepfake pornography are victims of sexual violence. Victims are the ones who suffer the most because manipulated photos and videos can change the way others see them. This can encourage bullying from the community. Victims of sexual violence are affected mentally and emotionally and are not easily cured. Depression, flashbacks to traumatic events, and post-traumatic stress disorder (PTSD) are hard to escape Victims of sexual violence really need psychological assistance to help them recover, because the deep wounds they feel can lead them to self-harm. Meanwhile, AI deviations, especially through pornographic deepfake technology, In Indonesia, there are no laws or regulations that specifically regulate the characteristics of offenses, criminal sanctions for perpetrators, and legal protection for victims of AI abuse crimes through pornographic deepfake technology. Regulatory conditions that have not regulated optimally and are even empty will of course affect the law enforcement process, both preventive and repressive in nature. Law as a tool for social reform (a tool of social engineering) should be able to pave the way for developments that occur in society.

K*eywords:* *Deep Fake; Pornography; Protection*

Introduction

In the current era of globalization, technology has played a very important role. Where technology has become an inseparable part of everyday life. Technological developments have changed the structure of society, which was initially local to a global structured society. One of the causes of this change is the presence of information technology. Furthermore, the development of information technology, then combined with the media and computers which then gave birth to a new tool called the internet.[1]

[1] Abdul Wahid dan Mohammad Labib**,** ***Kejahatan Mayantara (Cyber Crime)***, Jakarta, 2005: hlm 103.

The United State Supreme Court defines the internet as an International Network of Interconnected Computers, which means an international network of interconnected computer devices. As is usual for technological renewal, the internet besides providing benefits also creates negative sides by opening up opportunities for misuse of this technology, as well as having an impact on the loss of boundaries of space and time. One of the negative sides is related to the use of data and information that is done electronically. Therefore, in computer networks such as the internet, the problem of crime becomes increasingly complex because of its broad scope.[2]

According to the British Police, Cybercrime or cybercrime is any way of using computer networks for criminal purposes and/or high-tech crimes by utilizing the convenience of digital technology.[3] Furthermore, Indra Safitri argued that cybercrime is a type of crime related to the use of unlimited information technology and has strong characteristics with a technological engineering that relies on a high level of security and credibility of information conveyed and accessed by internet customers.[4]

The negative impact in the form of misuse of advances in information technology through computerized systems and internet networks is known as Cybercrime or cybercrime.[5] Cybercrime is a term that refers to criminal activity by using computer media or computer networks as a tool, target or place of crime. Some examples of cybercrimes include:[6]

1. phishing, which is the crime of stealing identity where the data that is often targeted is data on age, name, address, social media accounts and passcodes;
2. spoofing, is a digital crime besides the perpetrator trying to steal the victim's data, the perpetrator also sends dangerous malware to the victim's device/site;
3. cracking, namely attempts to enter into the victim's computer system for illegal purposes;
4. OTP fraud which is usually used for criminal acts of taking funds in digital wallets;
5. falsification of identity, for example when the perpetrator makes an account creation service through the website /www.jualanrekening.org, apart from being a media for online fraud, it can also be used as a medium for money laundering;
6. Ransomware, is a digital crime that aims to encrypt and lock the victim's files or data and to open it, the victim will be asked for a ransom;
7. Email and Site Hacking, also known as website and email defacement;
8. SQL injection, is a code injection attack on applications that have low security holes;
9. Carding, a crime with the main objective of stealing other people's credit card data or information;
10. Spreading illegal content, including buying and selling illegal goods, spreading pornographic videos and making immoral videos;
11. Cyber bullying is bullying that is carried out in cyberspace or social media which can cause victims to experience bad mental disorders, ranging from depression, self-isolation, becoming angry and even committing suicide;
12. Duplication of other people's sites, where this clearly violates a person's Intellectual Property Rights and is declared as an illegal activity;
13. Skimming crime, which is a banking crime that aims to steal debit or credit card data in order to withdraw funds in an account.

[2] Agus Raharjo, Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Citra Aditya Bakti, Bandung, 2002: hlm. 91.
[3] Abdul Wahid dan Mohammad Labib, op. cit, hlm. 40.
[4] Indra Safitri, Tindak Pidana di Dunia Cyber" dalam Insider, Legal Journal From Indonesian Capital & Investmen Market. Dapat dijumpai di Internet, http://business.fortunecity.com/buffett/842/art180199_tindak pidana.htm, diakses tanggal 13 Juli 2019.
[5] Barda Nawawi Arief, Kapita Selekta Hukum Pidana, Citra Aditya Bhakti, Bandung, 2003: hlm. 239.
[6] Didik M Arief Mansur dan Elisatris Gultom,**Urgensi Perlindungan Korban Kejahatan**,Jakarta: PT.RajaGrafindo,2007: hlm 3.

Deepfake is the name given to an algorithm that allows users to change the face of an actor in a photorealistic video into that of another actor. Photorealistic refers to a quality related to photorealism in the sense of an artistic style that depicts a subject in a precise and detailed orientation. Deepfake technology is a new method of videographic manipulation in recent years, which can manipulate one person's face to become another person's face in the form of a video. In plain language, deepfake is a term used to describe a situation in which a person's face is pasted on another person's body and used without permission in a video and/or audio.

Although on various occasions deepfakes are used as satire and parody, along with the increasing ease of access to technology and information, recently deepfakes have become propaganda and fraud, including elements of pornography, using personal facial shape data, which are part of personal data and are increasingly being exploited for political purposes, and including identity theft or other privacy concerns. Hence, deepfakes have gained a lot of attention due to their use in celebrity porn videos, photos, fake news, hoaxes and financial scams.

Research Method

According to Terry Hutchinson as quoted by Peter Mahmud Marzuki "doctrinal research, research which provides a systematic exposition of the rules governing a particular legal category, analyzes the relationship between rules, explains areas of difficulty and, perhaps, predicts future development." Legal education research is also called normative legal research. That is, research aimed at or conducted to investigate the application of rules or norms in positive law.[7]

As explained in the previous section, this research is classified as normative research, which is to analyze regulations related to criminal acts resulting from the misuse of deepfake technology and legal protection for victims of deepfake pornography.

Results and Discussion

a. Definition of Deepfakes

The development of Artificial Intelligence triggers a special algorithm called Deepfake Technology. Marissa Koopman, Andrea Macarulla Rodriguez, and Zeno Geradts explain deepfake technology as an algorithm in their journal, in the form: "The Deepfake algorithm allows a user to switch the face of one actor in a video with the face of a different actor in a photorealistic manner.[8]

Deepfake is a term used in an algorithm that has a working system that can change the face of an actor to the face of another actor in a photo and/or video, producing photorealism in the sense of an artistic style that depicts a subject in precise orientation and detail like photography. The Deepfake algorithm allows users to transform an actor's face into a photorealistic face of another actor.[9]

In recent years, we have seen that deepfake technology is a new way of manipulating videography that can manipulate one person's face to become another person's face in the form of a video.

So what's the difference between deepfakes and other action videos, here's an explanation;

[7] Johny Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif, Bayumedia, Surabaya, 2005: hlm. 295.
[8] Detection of Deepfake Video Manipulation, Marissa Koopman, Andrea Macarulla Rodriguez, Zeno Geradts. University of Amsterdam & Netherlands Forensic Institute 2018.
[9] Photorealistic merujuk pada sifat yang berkenaan dengan photorealism dalam artian gaya artistic yang merepresentasikan suatu subjek dalam arah yang akurat dan detil, seperti sebuah fotografi.

First, the potential for photo-realistic results. If you have a full face of each actor and enough time for the algorithm, the video results are very convincing.

Second, public access and use of public deepfake applications such as FaceApp and Reface. People can now create tools or systems that simplify their work, including using deepfakes.

So lately, deepfakes are widely used to manipulate photography and videography to manipulate one person's face into another person's face.[10] Deepfake technology is basically very helpful for human work, especially in the film industry to produce a scene that cannot be done by actors who play films, for example in a film called I, Tonya (2017) which uses a facial replacement technique for the main character Tonya. Harding, played by Margot Robbie. Tonya is the first female ice skater to be able to perform the triple axel jump at her appearance, and until now only six female athletes have been able to do it. It was difficult for Margot, who did not have knowledge and expertise in ice skating, to make the jump, so the film producers had to use special effects to replace the face of a female athlete doing the jump with Margot's.

The use of face replacement techniques for actors and actresses, of course, uses Artificial Intelligence through the use of deepfake technology which requires quite a large amount of money, but with technological sophistication and almost everyone currently has a computer or smartphone and can easily access the internet network, deepfake technology becomes easier. for everyone to access and use through a variety of applications that are available for free such as DeepFaceLab, FaceApp, FaceSwap, Reface, myFakeApp, and others.

Hao Li, a professor of computer science at the University of Southern California, said deepfakes created for malicious purposes, such as fake news, will become even more dangerous unless steps are taken to raise awareness of deepfake technology. Li predicts that rapid advances in artificial intelligence and computer graphics will reach a level where real videos and deepfakes are indistinguishable within six months from October 2019.[11]

Therefore, deepfake technology that uses data in the form of images/photos of someone's face which is part of personal data raises the potential to be misused to commit crimes such as pornography, revenge, bullying, political sabotage, extortion, fake video evidence, fraud, theft. identity, and other privacy issues. The act of the perpetrator falsifying the use of someone's personal data using deepfake technology to gain profit results in losses for the victim, namely the leakage of his personal data through terror threats by debt collectors will spread the victim's personal data if he does not pay off the debt and of course material losses in the amount of money obtained by the perpetrator using the victim's personal data on online loan services, even though the victim did not receive the loan at all.

b.Cyber Crime Regulation in Indonesia

There are several positive laws related to cybercrime, including:

1. Criminal Code;
2. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE);
3. Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE);
4. Law Number 44 of 2008 concerning Pornography (Pornography Law).
5. Law Number 36 of 1999 concerning Telecommunications (Telecommunication Law);
6. Law Number 5 of 1999 concerning Prohibition of Monopolistic Practices and Unfair Business Competition (Anti Monopoly Law);

[10] Marissa Koopman, Andrea Macarulla Rodriguez, Zeno Geradts, Detection of Deepfake Video Manipulation, University of Amsterdam & Netherlands Forensic Institute, 2018.
[11] "Perfect Deepfake Tech Could Arrive Sooner Than Expected", www.wbur.org.

7. Consumer Protection Law Number 8 of 1999 (Consumer Protection Law);
8. Law Number 19 of 2002 concerning Copyright (Copyright Law);
9. Law Number 8 of 1997 concerning Corporate Document Law;
10. Law Number 25 of 2003 Amendments to Law Number 15 of 2002 Concerning the Crime of Money Laundering (Money Laundering Law;
11. Law Number 15 of 2003 concerning Combating Terrorism (Terrorism Law).

According to the ITE Law, the characteristics of criminal acts in the field of information and electronic transactions include:

1. Performed by people who have the ability in the field of technology;
2. Using sophisticated and complicated techniques to be proven, if only by conventional criminal articles (KUHP);
3. Has a broader dimension than ordinary criminal acts.

Furthermore, Josua Sitompul explained about criminal offenses via the internet which are regulated in the ITE Law, including:

Criminal acts related to illegal activities, namely:

a) Distribution or dissemination, transmission, access to illegal content, consisting of:

   1. Insult or defamation (Article 27 paragraph (3) UU. ITE);
   2. Fake news that is misleading and detrimental (Article 28 paragraph (1) UU. ITE);
   3. Causing hatred based on SARA (Article 28 paragraph (2) UU. ITE);
   4. Sending information that contains threats of violence or intimidation that are directed personally (Article 29 UU. ITE);

b) In any way make illegal access (Article 30 of the ITE Law);

c) Illegal interception of electronic information or documents and Electronic Systems (Article 31 of the ITE Law).

   1. The crime of falsifying electronic information or documents (Article 35 of the ITE Law);
   2. Additional crimes (accessoir Article 36 of the ITE Law) and;
   3. Objections to criminal threats (Article 52 of the ITE Law).

Conclusion

Based on the discussion above, the researcher draws the following conclusions:

a. Victims of deepfake pornography are victims of sexual violence. Victims are the ones who suffer the most because manipulated photos and videos can change the way others see them. This can encourage bullying from the community. Victims of sexual violence are affected mentally and emotionally and are not easily cured. Depression, flashbacks to traumatic events, and post-traumatic stress disorder (PTSD) are hard to escape. Victims of sexual violence really need psychological assistance to help them recover, because the deep wounds they feel can lead them to self-harm.

b. Meanwhile, AI deviations, especially through pornographic deepfake technology, In Indonesia, there are no laws or regulations that specifically regulate the characteristics of offenses, criminal

sanctions for perpetrators, and legal protection for victims of AI abuse crimes through pornographic deepfake technology. Regulatory conditions that have not regulated optimally and are even empty will of course affect the law enforcement process, both preventive and repressive in nature. Law as a tool for social reform (a tool of social engineering) should be able to pave the way for developments that occur in society.

References

Book

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Jakarta, 2005.

Andi Hamzah, *Hukum Pidana Yang berkaitan Dengan Komputer*, Sinar Grafika, Jakarta, 1993.

Andrew Ashworth, *Victim Impact Statements and Sentencing, The Criminal Law Review*, Agustus 1993.

Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, Sinar Grafika, Jakarta, 1991.

Barda Nawawi Arief. *Kebijakan Hukum Pidana (Penal Policy), bahan Penataran Nasional Hukum Pidana dan Kriminologi*, Fakuitas Hukum Universitas Dipanegoro, Semarang. 1998.

Carl Öhman, 2019, '*Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography.' Ethics and Information Technology*. doi:10.1007/s10676-019-09522-1.

Didik M Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005.

H. Parman Soeparman, *Pengaturan Hak Mengajukan Upaya Hukum Peninjauan Kembali Dalam Perkara Pidana Bagi Korban Kejahatan*, Penerbit Refika Aditama, Bandung, 2007.

Johny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Surabaya, 2005.

Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT. Tatanusa, Jakarta, 2012.

Lilik Mulyadi, Kompilasi Hukum Pidana dalam Perpektif Teoritis dan Praktik Peradilan Pidana (Perlindungan Korban Kejahatan, Sistem Peradilan dan Kebijakan Hukum Pidana Filsafat Pemidanaan serta Upaya Hukum Peninjauan kembali oleh korban kejahatan), Penerbit CV. Mandar Maju, Bandung, 2010.

Melati, N. K., *Membicarakan Feminisme*, EA Books, Yogyakarta, 2019.

Muladi dan Barda Nawawi Arief, *Bunga Rampai Hukum Pidana*, PT. Alumni, Bandung, 1992.

Moeljatno, *Kitab Undang-undang Hukum Pidana*, Jakarta: Bumi Aksara, 2009.

Kaligis, O. C. (Otto Cornelis) & Indonesia. Undang-Undang tentang Informasi dan Transaksi Elektronik 2012, Penerapan Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dalam prakteknya, Cet. 1, Yarsif Watampone, Jakarta.

Peter Mahmud Marzuki, 2010, *Penelitian Hukum*, Cetakan ke-2, Kencana, Jakarta, 2010.

Peter Mahmud Marzuki, 2011, Penelitian Hukum, Kencana Prenada Media Group, Jakarta.

Philipus M. Hadjon, *Pengantar Hukum Administrasi Indonesia*, Gajah Mada University Press, Yogyakarta, 2011.

Sophie Maddocks, 2020, '*A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political' deep fakes, Porn Studie*s, DOI: 10.1080/23268743.2020.1757499.

Sutan Remi Syahdeni, 2009, *Kejahatan dan Tindak Pidana Komputer*, Pustaka Utama Graffiti, Jakarta.

Tata Sutabri, Sistem Informasi Manajemen, Penerbit Andi, Yogyakarta, 2005.

Widodo, Prabowo P, Dkk, P2011, *Pemodelan Sistem Berorientasi Obyek Dengan UML*, Graha Ilmu, Yogyakarta.

Journals

Dewi Bunga, *Penanggulangan Pornografi Dalam Mewujudkan Manusia Pancasila', Jurnal Konstitusi*, Vol.8, No. 4, Agustus 2011.

Dodo Zaenal Abidin, *Kejahatan dalam Teknologi Informasi dan Komunikasi*, Jurnal Ilmiah Media Processor, Vol. 10, No. 2, April 2015.

Suratman dan Andri Winjaya Laksana, *Analisis Yuridis Penyidikan Tindak Pidana Pornografi Berdasarkan Undang-Undang Nomor 44 Tahun 2008 Di Era Digitalisasi*, Jurnal Pembaharuan Hukum, Vol. 1, No. 2, Mei-Agustus 2014.

Ardi Sutedja, Ketua Indonesia Cyber Securty Forum (ICSF), ***Penyalahgunaan Deepfake Bisa Dijerat UU ITE, Tapi...*** https://cyberthreat.id/read/3323/Penyalahgunaan-Deepfake-Bisa-Dijerat-UU-ITE-Tapi.

Annisa Seva Kamil, *Penyalahgunaan Teknologi Deepfake: Mengapa Aktor Negara Perlu Bergerak Aktif dalam Komunitas Keamanan sebagai Penanganannya?*, https://www.researchgate.net/publication/342441503.

Articles

Ayu Yuliani, 2017, *Indonesia Diserang Hacker Miliaran Kali Tiap Hari*, https://kominfo.go.id/content/detail/11956/indonesia-diserang-hacker-miliaran-kali-tiap-hari/0/sorotan_media.

Catherine Stupp, 2019, *Fraudster Used AI to Mimic CEO's Voice in nusual Cybercrime Case*https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

Deeptrace, 2019, The State of Deepfakes: Landscape, Threats and Impact, http://deeptracelabs.com/reports/.

Emma Woollacott, 2019, *China Bans Deepfakes in New Content Crackdown*. dalam https://www.forbes.com/sites/emmawoollacott/2019/11/30/china-bans-deepfakes-in-new-content-crackdown/#1d14b1dc3537.

Grace Shao, 2019a. *What 'deepfakes' are and how they may be dangerous* [online]. dalam https://www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html [diakses 15 Juni 2020].

Indra Safitri, *Tindak Pidana di Dunia Cyber" dalam Insider, Legal Journal from Indonesian Capital & Investmen Market*, http://business.fortunecity. com/buffett/842/art180199_tindak pidana.htm,

Komnas Perempuan, 2020, *Catatan Kekerasan terhadap Perempuan Tahun 2019: Kekerasan Meningkat: Kebijakan Penghapusan Kekerasan Seksual untuk Membangun Ruang Aman Bagi Perempuan dan Anak Perempuan*, Jakarta, 6 Maret 2020.

Marty Puranik, 2019, *AI-Powered Malware, Smart Phising and Open Source Attack, Oh My! The New Wave of Hacking in 2019 and How to Prevent.* https://www.cpomagazine.com/cyber-security/ai-powered-malware-smart-phishing-and-open-source-attacks-oh-my-the-new-wave-of-hacking-in-2019-and-how-to-prevent/.

Theodora Shah Putri, Upaya Perlindungan Korban Kejahatan Melalui Lembaga Restitusi dan Kompensasi, lml. 3. (httpwww.pemantauperadilan.com).

----------, *AI Berisiko Disalahgunakan Hacker*, https://www.cnbcindonesia.com/tech/20180221142655-37-4997/ai-berisiko-disalahgunakan-hacker.

----------, *Deepfake: Rekayasa yang Menakutkan di Jagat Siber*, https://cyberthreat.id/read/3282/Deepfake-Rekayasa-yang-Menakutkan-di-Jagat-Siber.

----------, Deepfake Pornografi: Ketika Kekerasan Seksual Bertransformasi Tanpa Kendali,

https://www.infid.org/news/read/deepfake-pornografi, 15 Juli 2020.

Etc.

Data KPAI, 23 Juli 2019.

RAINN, 2020, Effects of Sexual Violence, https://www.rainn.org/effects-sexual-violence .

International Criminal Police Organization (INTERPOL) dan United Nations Interregional Crime and Justice Research (UNICRI), 2019. Second INTERPOL – UNICRI Report on Artificial Intelligence for Law Enforcement 2019.

Legislation

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 44 tahun 2008 tentang Pornografi.

Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.

Copyrights