Legal Protection for Deepfake Victims: Tackling Pornography Crimes in the Age of Advanced Technology

Musfala Yudha; Sunardi Purwanda; Amir; Kairuddin Karim; Muh. Akbar Fhad Syahril; Samiruddin; Asriyadi Latif

Faculty of Law, Institut Ilmu Sosial dan Bisnis Andi Sapada, Parepare, Indonesia

Abstract

The purpose of this research is to find out the impact and also legal protection on victims of deepfake technology abuse against pornography. This research uses a normative legal research type with a statutory and analytical approach. Types and sources of legal materials use primary and secondary legal materials. Data analysis will be reviewed prescriptively and qualitatively. The results of this study show that several laws indirectly relate to deepfake porn, namely Law No. 1 of 2024 concerning ITE, Law No. 44 of 2008 concerning Pornography, Law No. 27 of 2022 concerning Personal Data Protection and Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence, so that the relationship between deepfake and the crime of pornography can be seen through laws and regulations regarding pornography. And there are several ways or things that victims of deepfake porn can do to get protection, which is indirectly regulated in Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence.

Keywords: Protection Law; Pornography; Deepfake

Introduction

Nowadays, in the digital era, there is a rapid development of advances in science and technology, one of which is artificial intelligence (AI).[1] The development of internet technology and law are two elements that influence each other and affect society.[2] One of them is a humanoid robot which is a representation of artificial intelligence, but also

computer systems, software, and programs capable of making decisions and acting like humans. One innovation that stands out from the advancement of AI is deepfake, which is a combination of "Deep learning" and "Fake". Deepfake refers to fake audio-visual data such as video, audio or photos, created through deep learning methods. Deep learning is a group of AI that refers to algorithms and is capable of

---

[1] Karim, K., Herman, B., Akbar, M., & Syahril, F. (2021). Criminological Analysis Of Online Buying Fraud. 10–16. Https://Doi.Org/10.53361/Dmejl.V2i01.0002

[2] Suardi, S., Asba, P., & Iksan, M. N. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Investasi Melalui Media Internet. *Jurnal Litigasi Amsir*, *10*(1), 72–83. Http://Journalstih.Amsir.Ac.Id/Index.Php/Julia/Article/View/156

learning and making independent decisions. Simply put, deepfake is a synthetic human image creation technique based on artificial intelligence, where videos or images can be combined with certain methods to create results that look real.[3]

Deepfake is a new technology that allows users to create customized video or image edits and is free to download. It is a result of the development of Artificial Intelligence (AI). Initially, Deepfake was only used in TV entertainment and social media, but gradually, this technology was misused by some people to mislead and spread false information. The negative impact is mainly felt in terms of eroding public trust, especially when it involves famous people. Not only can deepfakes create fake videos, they can also quickly damage a person's reputation. Many utilize this app to spread negative content, including fake news, data manipulation, and even sexual or pornographic content.[4]

The availability of various apps such as DeepFaceLab, FaceSwap, MyFakeApp, Reface, and others has made Deepfake easily accessible to anyone, not just professionals. This is supported by the development of social media which makes it easy to access one's data, such as videos, images, and sounds. Public figures such as politicians and artists are often the main targets. This ease allows someone to make deepfakes and then use them for various purposes. However, it is unfortunate that this convenience is often misused, especially in making deepfakes without the consent of the data owner. This can hurt the victim, especially when deepfakes are used to create harmful pornographic content.[5]

Recently, news circulated of a provocative hoax video resembling the celebrity Syahrini. This video has been widely spread on social media since May 12, 2020. The perpetrator is a woman who initiated MS who was charged by the Kediri police, East Java. The perpetrator shared a provocative hoax video linking Syahrini's name through her personal Instagram account. The police revealed that MS, a housewife during the day, often plays social media. In addition, the motive for the popularity of the video that was spread was also because MS was a fan of other celebrities. Her actions made MS face sanctions for distributing pornographic videos.[6]

The presence of deepfakes involving prominent figures can have a real impact on the social conditions of society, ranging from an increase in hate speech, discord, and division, to an increase in intolerance. This technology also opens up loopholes for criminal acts. As technology advances, the spread of hoaxes, fake news, and deepfake-based pornographic content is increasing. The ease of spreading such content through social media also threatens the freedom of individuals who should not be involved in the use of such technology.[7]

Law is a social phenomenon. This means that where there is society, there is law.[8] (Dwiyanti et al., 2024). Legal protection has been stated in Article 28 Letter G of the 1945 Constitution of the Republic of Indonesia, which means that every citizen is entitled to protection from the State both for himself, his family, honour and dignity and the property he has under his power.

Although there are personal information protection regulations in Indonesia, such as Law No. 27 of 2022 on Personal Data Protection, there are no specific provisions regulating the use of personal data in deepfake creation. Personal information/data includes information about individuals that can be identified

---

[3] Al-Khowarizmi, S., & Lubis, A. R. (2023). Artificial Intelligence. Umsu Press.

[4] Yuadi, I., Sos, S., & MT, M. (2023). Forensik Digital Dan Analisis Citra. CV. AE Media Grafika.

[5] Renata, B. (N.D.). Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake Dalam.

[6] Renata, B. (N.D.). Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake Dalam.

[7] Syamsidar, S., Muhammad Reza, Z., Eka Ari, E., & Retno Sari, D. (N.D.). Tantangan Dalam Menjaga Kebebasan Berpendapat Di Era Digital.

[8] Dwiyanti, A., Megawati, L., Pujiningsih, D., Widaningsih, W., Girsang, H., Zamroni, M., Fajrina, R. M., Asmarani, N., & Phireri, P. (2024). Buku Ajar Pengantar Ilmu Hukum. Pt. Sonpedia Publishing Indonesia. Https://Scholar.Google.Com/Citations?View_Op=View_Citation&Hl=Id&User=Phvepriaaaaj&Citation_For_View=Phvepriaaaaj :Bnk-Pcrlprsc

directly or indirectly through electronic and non-electronic systems. There are two categories of personal information: general personal information/data and specialized personal information. One category of specialized personal data/information is biometric data, which includes information about an individual's body/physical, physiological, or behaviour such as voice, facial image, or body movements.

Regulations governing pornographic content in Indonesia include the Criminal Code (KUHP), Law No. 11/2008 on Electronic Information and Transactions (ITE Law) as amended by Law No. 19/2016, Law No. 44/2008 on Pornography (Pornography Law), and Law No. 27/2022 on Personal Data Protection.

Based on the description above, the author wants to conduct research on the impact given by the use of deepfake on criminal acts of pornography and seek legal protection for victims of criminal acts of pornography using deepfake.

Method

This research uses normative legal research. This research applies a statutory approach and an analytical approach.[9] Then the legal materials used are primary legal materials, namely Law Number 1 of 2024 on the second amendment to the ITE Law, Law Number 44 of 2008 on Pornography, and Law Number 12 of 2022 on Sexual Violence Crimes. As well as primary legal materials.

The data in this study comes from primary and secondary data which are first processed and then qualitatively analyzed. This is done by presenting the results in the form of descriptions that explain, describe, and illustrate information relevant to the issues discussed by the researcher. Thus, this research combines descriptive aspects that include a description of social phenomena with descriptive aspects focused on ongoing legal provisions.[10]

A. The Impact of Deepfake Use on the Crime of Pornography

Artificial intelligence technology, also known as artificial intelligence (AI), has been applied to various aspects of living things, including virtual household devices, transportation, chatbots on smartphones and deepfake technology.[11] Deepfake is an artificial method that produces duplicates of living things by utilizing AI. The technology utilizes machine learning techniques and is known as the Generative Adversarial Network, abbreviated as GAN, to combine and insert images and videos into other image or video sources.[12]

Pornographic offences involving artificial intelligence deepfake techniques have significant effects. Due to their easy accessibility to many people, deepfakes are often used in pornography offences, such as creating pornographic videos with celebrities or public figures, spreading fake news, or being

---

[9] Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., Tl, A. D., Asriyani, A., Hazmi, R. M., Syahril, M. A. F., Saputra, T. E., Arman, Z., & Rauf, M. A. (2023). Metode Penelitian Hukum. Cv. Gita Lentera. Https://Books.Google.Co.Id/Books?Hl=En&Lr=&Id=Vyxbeaaaqbaj&Oi=Fnd&Pg=Pa107&Dq=Info:Fm43wrnf4qaj:Scholar.Google.Com&Ots=Urtmkj13w0&Sig=-Vkpj78pfecsva_Frw2jvggzrva&Redir_Esc=Y#V=Onepage&Q&F=False

[10] Baro, R. (2021). Metode Dan Teknik Penelitian Sosial Di Bidang Hukum. Makassar: Penerbit Rana.

[11] Syahril, M. A. F., Tl, A. D., Murdiono, M., & Asriyani, A. (2024). Artificial Intelligence Dan Hak Asasi Manusia: Kajian Hukum Tentang Potensi Bahaya Di Indonesia. Jurnal Litigasi Amsir, 11(3), 359–364. Http://Journalstih.Amsir.Ac.Id/Index.Php/Julia/Article/View/443

[12] Khusna, I. H., & Pangestuti, S. (2019). Deepfake, Tantangan Baru Untuk Netizen (Deepfake, A New Challenge For Netizen). Promedia (Public Relation Dan Media Komunikasi), 5(2).

---

used to commit malicious hoaxes. This shows that the use of deepfakes in criminal pornography can have serious negative impacts, especially on individual privacy and security.[13] (Validnews.id, 2024).

Legally, deepfake is closely related to the crime of pornography. Logically, cases of deepfake pornography in Indonesia are also related to the Criminal Code which regulates acts of pornography, which can be seen in Article 4 paragraph 1 of Law Number 44 of 2008 concerning Pornography.

Deepfake technology became popular in 2017 through Reddit forum users. The use of the GAN network was developed using TensorFlow, software from Google, to insert the likeness of public figures into the bodies of women in porn movies. In January 2018, an app called FakeApp appeared and allowed anyone to create deepfakes. This app became one of the potential sources for the spread of deepfake content, especially pornographic content. Based on a review conducted by Deeptrace in 2019, approximately 96 percent of deepfake content was pornographic (Deeptracelab.com, 2024).

One example of what has happened in this country is the case in the introduction above, namely the deepfake porn case against celebrities named Syahrini and also Nagita Salvina. Not only Indonesian celebrities have been victimized, but also some celebrities from abroad such as Kristen Bell, Emma Watson, Taylor Swift, Natalie Portman, and many more have been caught in deepfake attacks. However, it is important to note that it is not only celebrities who are targeted by deepfakes. For example, Indian journalist Rana Ayyub was subjected to deepfake pornography right after discussing the Kathua gang rape issue in 2018. In addition, American Twitch streamer QTC Cinderella has been targeted by deepfake pornography after being harassed by a fake featuring her form. These incidents show that deepfakes are a widespread and indiscriminate threat, affecting individuals from various backgrounds and professions.[14]

Deepfake technology is significantly different from the face-swapping filters often used on social media. Face-swapping filters allow the user to superimpose their face on another user's face, but the user retains control over their face and expression. In contrast to deepfake, where the executor can obtain the victim's facial features and then operate the face with another individual's expression. This makes deepfakes particularly invasive, as the perpetrator holds power over the victim's likeness and uses it for purposes that the victim did not intend. The act contributes to a long history of sexual harassment against women, given that perpetrators utilize this technology to spread pornographic content involving victims' faces without their permission. Legal experts consider this phenomenon as a motive for sexual privacy aggression and classify deepfake pornography as a form of pornography minus consent and sex crimes through pictures. Perpetrators of deepfake pornography take control of their victims' bodies by manipulating them to carry out the perpetrator's desired actions without the victim's consent or knowledge. The perpetrators act as if they have complete control over women's bodies in cyberspace. This act can be categorized as a crime, as the perpetrator commits a series of criminal acts, including sexual abuse, theft of personal information, dissemination of false data, and exploitation.[15]

GBV is a form of technology-mediated, gender/sex-related exploitation, where the act of violence aims or intends to degrade the victim based on their gender or sexual orientation. According to the definitions of the Internet Governance Forum and the Association for Progressive Communications, GBV includes a wide range of acts that are often a continuation of conventional gender-based crimes, such as domestic violence, stalking, sex crimes, or targeting people based on their gender and sexual orientation, that are carried out partially to fully using information and communication technologies (ICTs), for

---

[13] https://Validnews.Id/Kultura/Mengenal-Deepfake-Dan-Tetap-Aman-Dari-Kepalsuan. Accessed 16 August 2024
[14]   https://Www.Whiteboardjournal.Com/Ideas/Human-Interest/Mengatasi-Ancaman-Pornografi-Deepfake-Stopncii-Lindungi-Korban-Dengan-Cepat. Accessed 21 August 2024
[15] Ivana Dewi Kasita, 2022, Deepfakepornografi: Tren Kekerasan Gender Berbasis Online(KGBO) Di Era Pandemi Covid-19.

example, internet mobile phones, social media platforms and email[16] (Bullyid.org, 2024). The following behaviours are included in KBGO:

1) *Stalking (online surveillance/cyberstalking/stalking and monitoring)*;

2) Threats   of rape or death *(cyber harassment/harassment/networked harassment)*;

3) *Image-based sexual abuse/nonconsensual distribution of intimate images/nonconsensual pornography/revenge porn/sexting/sextortion*;

4) *Voyeurism* is secretly taking photos for sexual purposes *(creepshots)*;

5) Media manipulation *(deep fake/synthetic media/morphing)*;

6) *Doxing* or the public dissemination of a person's data to harass, demean, and damage their prestige;

7) *Defamation* and *misinformation*;

8) *Hate speech*; and

9) *Hacking*.

In Article 14 paragraph (1) of Law No. 12 of 2022 on the Crime of Sexual Violence, recording, taking pictures, or screenshots with sexual content of a person without their consent, transmitting electronic information with sexual content without the consent of the recipient, or stalking using electronic systems for sexual purposes are subject to legal sanctions. In cases where such acts are committed for blackmailing, threatening, coercing, misleading, or tricking a person into doing something, the perpetrator may be sentenced to imprisonment of not more than six years and/or a fine of not more than 300,000,000.00.

It can be seen from Article 14 paragraphs (1) and (2) of Law Number 12 of 2022 that indirectly has a relationship between the KBGO behaviours above, one of which is deepfake itself.

Victims of counterfeit pornography require special attention as they face serious repercussions. In addition to experiencing trauma, loss of self-esteem and humiliation, victims are often stigmatized by their social environment. This points to the need to provide psychological attention, emotional support, as well as legal protection to victims. Public awareness of the issue is also important so that victims feel supported and not isolated. By providing proper attention and support, victims of deepfake pornography can have a better recovery and get the justice they deserve.

From the explanation above, the author can analyze that deepfake has a broader impact than just pornography because it can be classified as a type of KBGO (online gender-based violence). Deepfake perpetrators not only engage in the creation of pornographic content involving victims without their consent but also commit a range of other crimes. These include sexual assault, theft of personal information, dissemination of false data, and exploitation, where this can be seen in Article 14 paragraphs (1) and (2) of Law Number 12 of 2022 indirectly has a connection between the KBGO behaviors above, one of which is deepfake itself.

---

[16]   Deeptrace,   The   State   Of   Deepfakes: Landscape,   Threats   And   Impact, http://Deeptracelabs.Com/Reports/https://Bullyid.Org/Educational-Resources/Kekerasan-Berbasis-Gender-Definisi-Dan-Jenis-Jenisnya/

B. Legal Protection for Victims of Deepfake Pornography

Indonesia is a country based on law, that is undeniable.[17] However, in Indonesia, there is currently no comprehensive and specialized regulation to control the use of AI technology in the creation of fake pornographic content. This is due to the view that the circulation of videos and photos via the internet in the realm of cyberspace or cybercrime is considered a criminal act, with cyberspace as its parent.[18]

Cyberspace is likened to the world of computer-based communication that has become a new reality in human activities and is known as the internet in everyday language. The act of forgery is a type of cybercrime. Since real forgery or deepfake is illegal content that violates the law or disturbs public order, until now there has been no decree that regulates it specifically.[19]

In the case of cybercrime, the entities involved in unlawful acts must certainly feel the consequences of the losses for their actions, as well as the responsibility for the losses arising from their lack of caution. The exercise of legal rights and obligations always requires individuals to bear legal responsibility for their actions.[20]

Hans Kelsen's theory also emphasizes that the concept of legal obligation and the concept of legal responsibility are closely related. Thus, individuals must be legally responsible for certain actions they take, meaning they must be responsible for the consequences of their actions.[21]

The statutory provisions that apply to perpetrators of the dissemination of pornographic content are contained in Article 4 paragraph 1 of Law Number 44 of 2008 concerning Pornography, which reads:

> "Every person is prohibited from producing, making, reproducing, duplicating, disseminating, broadcasting, importing, exporting, offering, selling, renting, or providing pornography that explicitly contains: a) intercourse, including deviant intercourse; b) sexual violence; c) masturbation or masturbation; d) nudity or the appearance of nudity; e) genitals; or f) child pornography."[22]

The crime of pornography is included in Article 27 Paragraph (1) of Law Number 1 Year 2024 on Electronic Information and Transactions (ITE Law). Perpetrators involved in this act can be charged with Article 27 Paragraph (1) and Article 45 Paragraph (1) of the ITE Law, which carries a maximum sentence of 6 years in prison. Therefore, regulations related to pornography are not only regulated in the Pornography Law but also in the ITE Law, which prohibits acts that violate decency as stated in Article 27 Paragraph (1):

> "Every person intentionally and without the right to broadcast, show, distribute, transmit, and/or make accessible Electronic Information and/or Electronic Documents that have content that violates decency for public knowledge."[23]

---

[17] Balla, H. (2023). Hukum Acara Pidana Di Indonesia (Suatu Pengantar). Cv. Mitra Ilmu.

[18] Syahril, M. A. F. (2023). Hukum Informasi Dan Transaksi Elektronik (Aulia Ambarwati (Ed.); 2023rd Ed.). Eureka Media Aksara. Https://Repository.Penerbiteureka.Com/Publications/560970/Hukum-Informasi-Dan-Transaksi-Elektronik

[19] Andhika Nugraha Utama, Prama Tusta Kesuma, Rio Maulana Hidayat, 2023, Analisis Hukum Terhadap Upaya Pencegahan Kasus Deepfake Porn Dan Pendidikan Kesadaran Publik Di Lingkungan Digital, Jurnal Diterbitkan Oleh: Jurnal Pendidikan Tambusai, 7(3), 26179–26188. https://Doi.Org/10.31004/Jptam.V7i3.10815.

[20] Renata Christha Auli, 2024, Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya Https://Www.Hukumonline.Com/Klinik/A/Apa-Itu-Deepfake-Porn-Dan-Jerat-Pidana-Bagi-Pelakunya-Lt6530d3546d9c4/#_Ftn10

[21] Bachtiar, E., Duwila, A. A., Chaerul, M., Affandy, N. A., Makbul, R., Tanjung, R., Purba, B., Saidah, H., Sutrisno, E., & Sari, M. 2021, Pengetahuan Kebencanaan Dan Lingkungan. Yayasan Kita Menulis.

[22] *Vide* 4 ayat 1 Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi

[23] *Vide* Pasal 27 Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Meanwhile, Article 45 paragraph (1) of the ITE Law for criminal threats:

> "Every person who intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have content that violates decency as referred to in Article 27 paragraph (1) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00."[24]

According to Law No 11 of 2008 on ITE, Law No 19 of 2016 on the Amendment of ITE Law, and Law No 1 of 2024 on the Second Amendment of ITE Law, deepfake pornography AI is regulated in Article 1 paragraph 8 of Law No 19 of 2016, which defines an electronic agent as a device in an electronic system that can automatically perform actions on electronic information, operated by humans. This definition reflects characteristics similar to Artificial Intelligence (AI). Article 27 Paragraph (1) of Law No. 1 of 2024 also covers the use of AI in this context.

> "Every person intentionally and without the right to broadcast, show, distribute, transmit, and/or make accessible Electronic Information and/or Electronic Documents that have content that violates decency for public knowledge."[25]

Article 27 Paragraph (1) of Law No. 1 Year 2024 regulates "broadcasting", which includes transmitting, distributing, and making electronic information or documents accessible in an electronic system. Violation of this article can result in a maximum imprisonment of 6 years and/or a maximum fine of Rp1 billion, by Article 45 Paragraph (1) of Law No. 1 of 2024. In addition, there is also Article 27A of Law No. 1 of 2024 concerning the second amendment to the ITE Law which regulates the act of Deepfake Porn AI:

> "Every person intentionally attacks the honour or good name of another person by alleging a matter with the intention that it becomes public knowledge in the form of Electronic Information and/or Electronic Documents carried out through an Electronic System"[26]

From this article, it can be concluded that deepfake is a technology crime because the process of making it to spreading it all utilizes technology and the internet network.

Perpetrators of deepfake pornography can be prosecuted under Law No. 27 of 2022 on Personal Data Protection, which prohibits unlawfully obtaining, collecting, disclosing, or using personal data that does not belong to them, for personal or other people's benefit, which may harm the personal data subject.

Article 66 prohibits creating or falsifying personal data for personal or other people's benefit to the detriment of other parties. Disclosure of personal data that does not belong to them may result in imprisonment for a maximum of 5 years and/or a maximum fine of IDR 5 billion, by Article 67.[27]

Article 68 reads: "Any Person who intentionally creates false Personal Data or falsifies Personal Data with the intent to benefit themselves or others which may result in harm to others as referred to in Article 66 shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp6,000,000,000.00 (six billion rupiahs)".[28]

Law No. 12 of 2022 on the Crime of Sexual Violence stipulates that anyone who without permission records or takes sexually charged images, transmits sexual information without the recipient's

---

[24] *Vide* Pasal 45 Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
[25] *Vide* Pasal 27 Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
[26] *Vide Vide* Pasal 27 a Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
[27] *Vide* Pasal 66-Pasal 67 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan data Pribadi
[28] *Vide* Pasal 68 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan data Pribadi

permission, or conducts stalking with an electronic system for sexual purposes is subject to sanctions. The maximum penalty is 4 years imprisonment and/or a fine of IDR 200,000,000.

Article 14 paragraph (2) of Law Number 12 Year 2022 stipulates that if the actions mentioned in paragraph (1) are carried out with the purpose of extortion, threatening, coercion, or to mislead and/or deceive someone, the perpetrator may be subject to imprisonment of up to 6 years and/or a maximum fine of IDR 300 million.[29]

Although many laws indirectly relate to artificial intelligence or deepfakes, there is no law specifically dedicated to regulating artificial intelligence in isolation. As a result, crimes such as the creation of deepfake pornography using artificial intelligence and through the internet will only be followed up based on laws and regulations related to electronic information, sexual violence, pornography, and the protection of personal information.

Victims of deepfake pornography can get protection through various measures and agencies available. Here are some ways to get protection as a victim of deep fake pornography:[30]

1) Victims of *deepfake* pornography can report to law enforcement about what they have experienced. This is the most important step to prevent the feeling of being victimized again and or creating other victims by punishing the perpetrator.
2) Access to Protection and Recovery Mandated by the State: Victims and witnesses of *deep fake* pornography crimes who qualify as victims of Sexual Violence Crimes regulated in Law No. 12 of 2022 in Article 43 so that victims have the right to get protection and recovery guaranteed by the state through the Witness and Victim Protection Agency (LPSK).
3) Better Legal Protection: An evaluation of existing legal protection for victims of *deep fake* pornography can help strengthen legal protection for victims of deep fake pornography by ensuring that victims have adequate access to justice (Purwanda, et. Al, 2024) (Jumadi, 2024) and deterring perpetrators.
4) Contacting the Website to Request Content Removal: If someone is a victim of deepfake pornography, they can contact the website to request for the content to be removed which is regulated in Law No. 12 of 2022 in Article 46 and Article 47.

Conclusion

Based on the results of the research conducted and the discussion described above, it can be concluded that the use of deepfake has a very significant impact on the crime of pornography, even not only on pornography but also extends such as theft of personal data, exploitation, fraud, and also on the crime of sexual violence.

In addition, there are several ways or steps that victims of deepfake pornography can take to obtain legal protection, which is indirectly regulated in Law No. 12 of 2022 on the Crime of Sexual Violence. The Indonesian government needs more specific and effective legal reforms related to the use of artificial intelligence technology including deepfake itself, to protect the public and their data. The government should also socialize the public about artificial intelligence technology so that they pay more attention to every personal data they have so that cases like Deepfake porn do not occur.

---

[29] *Vide* Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual
[30] Yusuf, K., Frasetyo, M., Gumilar, R. R., & Hosnah, A. U. (2024). Perlindungan Hukum Terhadap Korban Kejahatan Identitas Online di Indonesia. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 2(1)

References

Al-Khowarizmi, S., & Lubis, A. R. (2023). Artificial Intelligence. Umsu Press.

Andhika Nugraha Utama, Prama Tusta Kesuma, Rio Maulana Hidayat, (2023), Analisis Hukum Terhadap Upaya Pencegahan Kasus Deepfake Porn Dan Pendidikan Kesadaran Publik Di Lingkungan Digital, Jurnal Diterbitkan Oleh: Jurnal Pendidikan Tambusai, 7(3), 26179–26188. https://Doi.Org/10.31004/Jptam.V7i3.10815.

Bachtiar, E., Duwila, A. A., Chaerul, M., Affandy, N. A., Makbul, R., Tanjung, R., Purba, B., Saidah, H., Sutrisno, E., & Sari, M. (2021), Pengetahuan Kebencanaan Dan Lingkungan. Yayasan Kita Menulis.

Balla, H. (2023). Hukum Acara Pidana Di Indonesia (Suatu Pengantar). Cv. Mitra Ilmu.

Baro, R. (2021). Metode Dan Teknik Penelitian Sosial Di Bidang Hukum. Makassar: Penerbit Rana.

Deeptrace, The State of Deepfakes: Landscape, Threats And Impact, http://Deeptracelabs.Com/Reports/https://Bullyid.Org/Educational-Resources/Kekerasan-Berbasis-Gender-Definisi-Dan-Jenis-Jenisnya/

Dwiyanti, A., Megawati, L., Pujiningsih, D., Widaningsih, W., Girsang, H., Zamroni, M., Fajrina, R. M., Asmarani, N., & Phireri, P. (2024). Buku Ajar Pengantar Ilmu Hukum. Pt. Sonpedia Publishing Indonesia. Https://Scholar.Google.Com/Citations?View_Op=View_Citation&Hl=Id&User=Phvepriaaaaj&Citation_For_View=Phvepriaaaaj:Bnk-Pcrlprsc

Ivana Dewi Kasita, (2022), Deepfakepornografi: Tren Kekerasan Gender Berbasis Online(KGBO) Di Era Pandemi Covid-19.

Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., Tl, A. D., Asriyani, A., Hazmi, R. M., Syahril, M. A. F., Saputra, T. E., Arman, Z., & Rauf, M. A. (2023). Metode Penelitian Hukum. Cv. Gita Lentera. Https://Books.Google.Co.Id/Books?Hl=En&Lr=&Id=Vyxbeaaaqbaj&Oi=Fnd&Pg=Pa107&Dq=Info: Fm43wrnf4qaj:Scholar.Google.Com&Ots=Urtmkj13w0&Sig=-Vkpj78pfecsva_Frw2jvggzrva&Redir_Esc=Y#V=Onepage&Q&F=False

Karim, K., Herman, B., Akbar, M., & Syahril, F. (2021). Criminological Analysis Of Online Buying Fraud. 10–16. Https://Doi.Org/10.53361/Dmejl.V2i01.0002

Khusna, I. H., & Pangestuti, S. (2019). Deepfake, Tantangan Baru Untuk Netizen (Deepfake, A New Challenge For Netizen). Promedia (Public Relation Dan Media Komunikasi), 5(2).

Renata Christha Auli, 2024, Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya Https://Www.Hukumonline.Com/Klinik/A/Apa-Itu-Deepfake-Porn-Dan-Jerat-Pidana-Bagi-Pelakunya-Lt6530d3546d9c4/#_Ftn10

Renata, B. (N.D.). Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake Dalam.

Renata, B. (N.D.). Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake Dalam.

Suardi, S., Asba, P., & Iksan, M. N. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Investasi Melalui Media Internet. Jurnal Litigasi Amsir, 10(1), 72–83. Http://Journalstih.Amsir.Ac.Id/Index.Php/Julia/Article/View/156

Syahril, M. A. F. (2023). Hukum Informasi Dan Transaksi Elektronik (Aulia Ambarwati (Ed.); 2023rd Ed.). Eureka Media Aksara. Https://Repository.Penerbiteureka.Com/Publications/560970/Hukum-Informasi-Dan-Transaksi-Elektronik

Syahril, M. A. F., Tl, A. D., Murdiono, M., & Asriyani, A. (2024). Artificial Intelligence Dan Hak Asasi Manusia: Kajian Hukum Tentang Potensi Bahaya Di Indonesia. Jurnal Litigasi Amsir, 11(3), 359–364. Http://Journalstih.Amsir.Ac.Id/Index.Php/Julia/Article/View/443

Syamsidar, S., Muhammad Reza, Z., Eka Ari, E., & Retno Sari, D. (N.D.). Tantangan Dalam Menjaga Kebebasan Berpendapat Di Era Digital.

Yuadi, I., Sos, S., & MT, M. (2023). Forensik Digital Dan Analisis Citra. CV. AE Media Grafika.

Yusuf, K., Frasetyo, M., Gumilar, R. R., & Hosnah, A. U. (2024). Perlindungan Hukum Terhadap Korban Kejahatan Identitas Online Di Indonesia. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 2(1)

https://Validnews.Id/Kultura/Mengenal-Deepfake-Dan-Tetap-Aman-Dari-Kepalsuan.

https://Www.Whiteboardjournal.Com/Ideas/Human-Interest/Mengatasi-Ancaman-Pornografi-Deepfake-Stopncii-Lindungi-Korban-Dengan-Cepat.

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 44 Tahun (2008) tentang Pornografi

Undang-Undang Nomor 12 Tahun (2022) tentang Tindak Pidana Kekerasan Seksual

Undang-Undang Nomor 27 Tahun (2022) Tentang Perlindungan data Pribadi

Undang-Undang Nomor 1 Tahun (2024) tentang Informasi dan Transaksi Elektronik