Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volumes 6 No. 4 (2026)

ENFORCEMENT AGAINST MISUSE OF *DEEPFAKE TECHNOLOGY FOR* PORNOGRAPHY ON SOCIAL MEDIA

Ery Susanti[1], Tahasak Sahay[2], Rizki Setyobowo Sangalang[3], Indang Sulastri[4]
[1,2,3,4] Faculty of Law, Universitas Palangka Raya
Email: erysusanti468@gmail.com[1], tahasak.sahay68@gmail.com[2], rizkisetyobowo@law.upr.ac.id[3] indangfh@gmail.com[4]

Received	: 01 March 2026	Accepted	: 30 March 2026
Revised	: 15 March 2026	Published	: 09 April 2026

Abstract

deepfake technology , which is being misused for pornographic content on social media. This study aims to analyze law enforcement and its obstacles in the Cyber Crimes Directorate of the Central Kalimantan Regional Police. The method used is empirical legal research with a qualitative descriptive approach through interviews and literature review. The results show that law enforcement is carried out through stages of inquiry, investigation, and prosecution, referring to the ITE Law, the Pornography Law, and the Criminal Code, and supported by preventive efforts such as digital literacy and cyber patrols. However, its implementation has not been effective due to obstacles in digital evidence, limited forensic facilities, and difficulties in identifying anonymous perpetrators across regions. Therefore, strengthening specific regulations, improving digital forensic facilities, and increasing the capacity of law enforcement officers is necessary.

Keywords: Deepfake , Pornography, Law Enforcement, Cybercrime, Social Media

INTRODUCTION

The development of digital technology has had a significant impact on various aspects of life, including the realm of criminal law. One issue that has increasingly attracted attention is *deepfake technology* , which uses artificial intelligence *to* alter images or videos to make them appear more authentic. [1]While this technology can be used for beneficial purposes, in reality, it is often exploited to create pornographic content without the consent of the parties involved. The term *deepfake* comes from a combination of the words *deep learning* , referring to deep machine learning technology, and *fake* , which means fake.[2] *Deepfake* is a technology that uses artificial intelligence (AI *)* . Deepfakes *are* created by combining original images or videos with the desired images or videos. Initially, this technology was used for entertainment purposes on social media. However, over time, *deepfakes* began to be used as a way to deceive people and spread fake news .

[3]This crime is a bad act committed by sending data or information to the internet about things that are false, impolite, or could be considered illegal, even disturbing public order, such as spreading pornographic material.[4] *Deepfakes* first became known in 2017 through Reddit forums. *Deepfake technology* uses *a Generative Adversarial Network* (GAN). GAN was first developed with the help of *TensorFlow* , a tool owned by *Google* , and was used to superimpose the faces of famous figures onto women's bodies in pornographic videos. In January 2018, a *deepfake application* called *FakeApp* was launched, allowing anyone to create *deepfake content* . This has made it easier to distribute various types of pornographic content, both in the form of videos and photos.[5] From a legal perspective, the use of pornographic *deepfake technology* is considered a cybercrime that is contrary to law and morality. In

[1] Mahfudz Ikhsan Mahardika, 2025, *Legal Review of Deepfake Porn Perpetrators as Online Gender-Based Violence According to the Pornography Law* , Jurnal Lex Privatum, Vol.14 No.5, P. 22.

[2]Shannon Gandrova and Ricky Banke, 2023, *The Application of Indonesian Positive Law to Deepfake Cybercrime Cases* , Jurnal Ilmiah Multidiscipline, Vol. 1 No. 10, P. 651, https://doi.org/https://doi.org/10.5281/zenodo.10201140.e

[3] Meirza Aulia Chairani, et al., 2024, *The Urgency of Legal Regulations for the Abuse of Deepfake Applications* , Jurnal Rechtens, Vol. 13 No. 1, P. 84, https://doi.org/10.56013/rechtens.v13i1.2668.

[4] Muchammad Zaidun and Pratama Persdha, 2018, *Law Enforcement of Cyber Crime in Indonesia* , Media Nusa Creative, Malang, p. 30.

[5]Ivana Dewi Kasita, 2022, *Deepfake Pornography: Trends in Online Gender-Based Violence (KGBO) in the Covid-19 Pandemic Era* , Journal of Women and Families, Vol.3 No.1, P. 20, https://doi.org/10.22146/jwk.5202.

Indonesia, the application of the law to such acts is through the provisions of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions in Article 27 paragraph (1). This law prevents the use of electronic media to disseminate content that is contrary to moral norms. In addition, the provisions of Law Number 44 of 2008 concerning Pornography in Article 29 can be used to ensnare perpetrators of distributing pornographic content through social media, and can use the 2023 Criminal Code contained in Article 407.[6] Enforcing the law against pornographic *deepfake crimes* is the responsibility of law enforcement officials. The rapid development of *deepfake technology requires authorities to continuously strive to improve their capacity and capabilities. Furthermore, the process of proving evidence in deepfake cases* is quite complex, as it requires demonstrating the perpetrator's motive or intent and the authenticity of the content.[7] Despite their role and authority, the Central Kalimantan Regional Police face various challenges in enforcing the law on *deepfake crimes* . Technical challenges arise because specialized expertise is required to detect and analyze increasingly sophisticated *deepfake* content . Jurisdictional issues also pose a challenge when the perpetrators are located outside Central Kalimantan or even abroad.

In Central Kalimantan, cybercrime is handled by the Central Kalimantan Regional Police's Cyber Division of the Special Criminal Investigation Directorate (Ditreskrimsus). Interviews with law enforcement officers within the Central Kalimantan Regional Police revealed that over the past three years (2023-2025), there have been at least 10 public reports of pornography distributed through social media platforms such as Instagram, Facebook, Telegram, and Twitter. In practice, investigators face various challenges in handling pornographic *deepfake cases* , such as difficulty identifying perpetrators using anonymous accounts and the continued advancement of digital manipulation technology.[8] Another obstacle encountered is the lack of supporting facilities and infrastructure for handling cybercrime, particularly the lack of forensic laboratories at the regional level, including within the Central Kalimantan Regional Police. The Central Kalimantan Regional Police's Directorate of Special Criminal Investigations must first send evidence for examination to regional police departments with forensic laboratories, such as those in Jakarta and Surabaya. This slows down the process of solving cases. Based on this background, this research is important to understand how law enforcement is applied to the misuse of pornographic *deepfake technology* on social media and how it is faced, especially within the Cyber Crimes Directorate of the Central Kalimantan Regional Police.

FORMULATION OF THE PROBLEM

Based on the description of the reasons for choosing the title above, the problem is formulated as follows:

1. How is law enforcement against the misuse of pornographic *deepfake technology* on social media at the Cyber Crimes Directorate of the Central Kalimantan Regional Police?
2. What are the obstacles in law enforcement against the misuse of pornographic *deepfake technology* on social media at the Cyber Crimes Directorate of the Central Kalimantan Regional Police?

RESEARCH METHODS

This study uses an empirical legal research method, namely legal research that analyzes and examines the functioning of law in society. [9]This research is descriptive qualitative with a sociological approach that aims to understand law enforcement against the misuse of pornographic *deepfake technology* on social media. This research was conducted at the Special Criminal Investigation Directorate (Ditreskrimsus) of the Cyber Division of the Central Kalimantan Regional Police, as the institution authorized to handle cybercrime. Data sources consist of primary data obtained through interviews with law enforcement officers, and secondary data obtained through library research in the form of laws and regulations, books, journals, and relevant legal literature.

[6]Bintang Muhammad Akbar, et al., 2026, *The Urgency of Reformulating the Electronic Information and Transactions Law against the Abuse of Deepfake Artificial Intelligence in the Perspective of Criminal Law Reform* , Journal of Politics, Social, Law and Humanities, Vol.4 No.2, P. 52, https://doi.org/10.59246/aladalah.v2i4.

[7]Ani Heskia Putri and Pudji Astuti, 2026, *Deepfake Law Enforcement at the East Java Regional Police as a Form of Cybercrime* **,** Indonesian Journal of Contemporary Law **,** Vol.1 No.1, P. 5.

[8] Interview with officers from the Cyber Crime Division of the Central Kalimantan Regional Police, conducted in March 2026

[9]Wiwik Sri Widiarty, 2024, *Legal Research Methods* , Publika Global Media, Yogyakarta, p. 37.

DISCUSSION

Law Enforcement Against the Abuse of Pornographic *Deepfake Technology* on Social Media

Law enforcement against the use of pornographic *deepfake technology* on social media is carried out by the Cyber Crimes Directorate of the Central Kalimantan Regional Police, with stages ranging from investigations and inquiries to criminal prosecutions based on applicable laws and regulations. Law enforcement officers utilize regulations such as the Electronic Information and Transactions Law , the Pornography Law, and the 2023 Criminal Code to prosecute perpetrators. In practice, within the Cyber Crimes Directorate of the Central Kalimantan Regional Police, law enforcement for pornography crimes begins with receiving reports from the public or conducting cyber patrols to detect pornographic content. Authorities identify the reports and confirm their authenticity. Validation and identification also include several technical steps used to gather digital evidence that can assist in further investigations. Authorities also coordinate and collaborate with the Central Kalimantan Communications and Information Office to block pornographic content and conduct investigations to gather digital evidence for the investigation phase. The next stage is further investigation.

After the initial stage of digital evidence collection, the investigative team has successfully gathered enough evidence to confirm the alleged pornography crime. The investigation will then move to the next stage. This stage aims to gain a deeper understanding of the perpetrator, the motives behind the crime, and any possible groups or relationships involved.[10] Law enforcement efforts undertaken by the Cyber Crimes Directorate of the Central Kalimantan Regional Police include measures to prevent crime and punish perpetrators. Preventive efforts include providing digital literacy education and raising public awareness of the dangers of *deepfakes* . Meanwhile, repressive efforts include conducting investigations, inquiries, and taking action against individuals found to be distributing pornographic content in the form of *deepfakes*. However, the law's effectiveness has not been optimal. This is due to several factors, including the lack of specific regulations, limited digital evidence, and the public's limited ability to report such cases. Furthermore, many victims are reluctant to report cases due to fear of social stigma.

Obstacles to Law Enforcement Against the Abuse of Pornographic *Deepfake Technology* on Social Media

Law enforcement in the development of AI-based *deepfake* technology has created new challenges, particularly in cases of digital pornography on social media, with various normative, structural, and technical barriers. Authorities often struggle because conventional procedural law differs from cybercrime, particularly regarding evidence. Technical obstacles also arise due to the increasingly sophisticated and difficult-to-detect nature of *deepfake technology* . This technology can create content that closely resembles the real thing, making it difficult for authorities to distinguish between real and fake. This complicates the process of proof in the criminal justice system.

Furthermore, the cross-border nature of cybercrime also poses a serious obstacle to law enforcement. Perpetrators often use false identities or anonymous accounts, even operating from outside their local jurisdiction. This makes it difficult to determine *the locus delicti* and coordinate between law enforcement agencies.[11] Structural barriers can also be seen in the lack of digital forensic laboratory facilities and infrastructure at the regional level. Not all police agencies have digital forensic equipment or experts capable of handling cybercrime cases. This limitation impacts the lengthy investigation process and the failure of many cybercrime cases to be fully prosecuted due to weak evidence. Furthermore, low public legal awareness is a significant obstacle. Many social media users are unaware that creating and distributing pornographic *deepfake content* is illegal. This lack of digital literacy makes such content easier to spread.[12]

CLOSING

Conclusion

1. Law enforcement against the misuse of pornographic *deepfake technology* on social media by the Cyber Crimes Directorate of the Central Kalimantan Regional Police has been carried out through preventive and repressive mechanisms based on applicable laws and regulations. However, its effectiveness remains suboptimal due to limited specific regulations, the complexity of digital evidence, and low public awareness in reporting cases.
2. Obstacles to law enforcement include technical, structural, and legal aspects, such as the difficulty of detecting increasingly sophisticated *deepfake content* , limited digital forensic facilities in the regions, and the cross-

[10] Husamuddin MZ., et.all., 2024, *Criminal Procedure Law and Cyber Crime* , PT Media Penerbit Indonesia, Medan, p. 85.

[11] Edmon Makarim, 2019, *Introduction to Telematics Law* , Rajawali Pers, Jakarta, p. 120.

[12] Asty Raisha Agma, 2025, *Criminal Law Policy in Combating Cybercrime in Indonesia* , Journal of Criminal Law and Criminology, Vol.1 No.1, P. 27.

regional nature of cybercrime and the use of anonymous identities, thus complicating the process of identifying perpetrators and providing legal evidence.

Suggestion

1. Due to the suboptimal law enforcement, it is necessary to strengthen more specific regulations related to pornographic *deepfakes* and increase the capacity of law enforcement officers through digital technology training and the provision of digital forensic facilities at the regional level to support a more effective evidence-gathering process.
2. In line with these various obstacles, it is necessary to increase digital literacy and public legal awareness through massive education and strengthening cooperation between institutions, both national and international, to overcome cybercrime that is cross-regional and involves fake or anonymous accounts.

REFERENCES

A. Book

Makarim, Edmon, 2019, *Pengantar Hukum Telematika*, Rajawali Pers, Jakarta.

MZ., Husamuddin, et.all., 2024, *Hukum Acara Pidana dan Pidana Cyber*, PT Media Penerbit Indonesia, Medan.

Widiarty, Sri, W., 2024, *Metode Penelitian Hukum*, Publika Global Media, Yogyakarta.

Zaidun, Muchammad, dan Persdha, Pratama, 2018, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, Media Nusa Creative, Malang.

B. Legislation

Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 Tentang Pornografi (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 181, Tambahan Lembaran Negara Republik Indonesia Nomor 4928).

Undang.Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905)

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republikindonesiatahun 2023 Nomor I, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).

C. Journals And Empirical Sources

Agma, Raisha, A., 2025, Kebijakan Hukum Pidana dalam Penanggulangan Cybercrime di Indonesia, *Jurnal Hukum Pidana dan Kriminologi*, Vol.1 No.1.

Akbar, Muhammad, A., dkk, 2026, Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana, *Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol.4 No.2, https://doi.org/10.59246/aladalah.v2i4.

Chairani, Aulia, M., dkk, 2024, Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake, *Jurnal Rechtens*, Vol. 13 No.1, https://doi.org/10.56013/rechtens.v13i1.2668.

Gandrova, Shannon dan Banke, Ricky, 2023, Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya Deepfake, *Jurnal Ilmiah Multidiscipline*, Vol. 1 No.10, https://doi.org/https://doi.org/10.5281/zenodo.10201140.e

Kasita, Dewi, I., 2022, Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19, *Jurnal Wanita dan Keluarga*, Vol.3 No.1, https://doi.org/10.22146/jwk.5202.

Mahardika, Ikhsan , M., 2025, Tinjauan Yuridis Terhadap Pelaku Deepfake Porn Sebagai Kekerasan Gender Berbasis Online Menurut UU Pornografi, *Jurnal Lex Privatum*, Vol.14 No.5.

Putri, Heskia, A., dan Astuti, Pudji 2026, Penegakan Hukum Deepfake Di Polda Jawa Timur Sebagai Bentuk Kejahatan Siber**,** *Indonesian Journal of Contemporary Law***,** Vol.1 No.1.

Wawancara dengan aparat Kepolisian Ditreskrimsus Bidang Siber Polda Kalimantan Tengah, Maret 2026.