



Research Paper

Legal Protection for Victims of Deepfake Pornography Under Indonesian Positive Law

Nia Kurnia¹✉, Laili Nur Anisah²

¹Criminal Law Department, Universitas Widya Mataram, Yogyakarta 55132, Indonesia

✉ laili.nur.anisah@gmail.com

doi <https://doi.org/10.30601/humaniora.v%vi%i.6983>

Published by Universitas Abulyatama

Artikel Info

Online first:
25/10/2025

Abstract

The advancement of technology has led to the emergence of deepfake, an artificial intelligence (AI)-driven algorithm capable of manipulating images and videos falsely, contributing to issues such as the proliferation of fake pornography. This research aims to analyze whether the misuse of deepfake applications can be considered a criminal offense and identify relevant legal regulations. Using a normative juridical research method, the findings indicate that the misuse of deepfake can be classified as a criminal act due to its societal harm, repetitive nature, and elicitation of social reactions. Potential criminal classifications may involve offenses related to pornography, fraud, and defamation, depending on the targets and losses incurred. Specific regulations governing AI are crucial to protect individual rights and support technological development. Although AI is regulated under the Information and Electronic Transactions Act, the absence of dedicated legislation results in ineffective sanctions against crimes like deepfake pornography. The establishment of dedicated laws is essential not only to safeguard victims but also to prevent the emergence of other offenses alongside the limitless progress of technology.

Keywords: Legal Protection; Deepfake; Pornography; Victims

1. Introduction

The rapid development of the digital era in technology is undeniable. This not only requires the global community to be proficient in using technology but also requires its users to be wise in responding to the various issues it raises. The impact of this rapid technological advancement is that almost all facilities (both public and private) use artificial intelligence to create something more efficient and effective. The emergence of artificial intelligence (AI) is a testament to the technological advancements of the digital era, with the potential to positively impact various



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

aspects of life. Artificial intelligence (AI) can potentially replace jobs currently performed by humans [1].

The development of AI has given rise to a specific algorithm called deepfake technology. Deepfake technology is highly beneficial to society, especially for workers in the entertainment industry. For example, during the COVID-19 pandemic, which required everyone to reduce face-to-face interactions, South Korean television stations used deepfakes to replace newscasters. This technology is used to create a perfect copy of a newscaster's voice, facial expressions, and even body language, thereby minimizing face-to-face interactions in the office. However, the existence of artificial intelligence (AI)-based technology in the form of deepfakes also has negative impacts, especially in this era of increasingly advanced technology, and has become a new threat to global society [2].

Deepfakes are sometimes misused, leading to various dangerous crimes, such as hate speech, propaganda, political tools, pornography, and so on. The use of deepfake technology to distribute pornographic content is a common and often disturbing crime. However, pornographic content is fundamentally linked to issues of gender-based violence. According to the National Commission on Violence Against Women (Komnas Perempuan), cases of online gender-based violence (KGBO) increased drastically during the COVID-19 pandemic [3]. Komnas Perempuan recorded 281 cybercrime cases out of 1,277 reported cases of gender-based violence, a significant 300% increase from 2018 [4]. However, throughout 2022, Komnas Perempuan reported 1.4% lower complaints of Gender-Based Cyber Violence (KSBG) compared to the previous year [3].

Crimes such as pornographic deepfakes created using AI and via the internet will only be subject to laws related to electronic information, morality, pornography, and defamation. The lack of specific legal protections results in ineffective sanctions [5]. The urgency of creating specific laws governing AI is crucial. In addition to protecting victims of pornographic deepfakes, specific laws are also needed because more complex crimes may emerge in the future [6]. Based on the exposure of the dangers of deepfake technology, this study aims to describe how deepfake technology works and how it can be categorized as a criminal act. It also examines the legal regulations and protections for victims of deepfake pornography, and the extent of government efforts to address pornography cases through deepfake technology. Therefore, this study is expected to assist the government in establishing effective policy solutions for both perpetrators and victims of pornography. Furthermore, this study is also expected to provide insight for readers and raise public awareness so they can respond more wisely to deepfake pornography and technological developments [7].

Based on the description above, the formulation of the problems that arise includes: (1) How does pornographic deepfake technology work in positive criminal law in Indonesia? (2) How is the protection for victims of pornographic deepfakes in positive criminal law in Indonesia? The objectives of this research are (1) to find out how the deepfake application works and the classification of deepfake misuse in criminal acts, (2) to find out how the legal regulations and protection for victims of pornography based on artificial intelligence (AI). The benefits of research in this writing are (1) Providing input and benefits for the development of science, especially in the field of criminal law, (2) The results of this research are expected to help and provide input to all parties who need knowledge related to the problems studied can be used as an effective and adequate means in efforts to resolve criminal cases that smell of Artificial Intelligence or Artificial Intelligence (AI).

2. Method

The research conducted is a normative juridical type, while the approach uses a qualitative descriptive approach, which focuses more on theoretical foundations aimed at producing descriptive research in the form of written or spoken words. This type of normative juridical research is library legal research conducted by examining or sourcing from library materials or secondary data [8]. The data collection technique, which is in the form of secondary legal materials used in this study, is by tracing all laws and regulations, journals, books, references, and internet media pages related to the problem of the influence of pornographic deepfakes. The research was conducted after all secondary data, including primary, secondary, and tertiary legal materials, had been collected. Interviews with the informants were then conducted. All data were then analyzed to determine the validity of the proposed problem formulation. This research uses an analytical description approach, meaning that the researcher's analysis aims to provide a description or explanation of the research subjects and objects, as reflected in the results of the research. In this case, the researcher does not justify the results. By following these steps, the research can provide in-depth insights into the laws and regulations related to the protection of victims of deep fake pornography in Indonesia.

3. Result and Discussion

3.1 Deepfake pornography in Indonesian positive criminal law

Pornographic deepfake perpetrators steal the victim's bodily authority by engineering the victim to do something they want without the victim's permission or even knowledge [9]. The perpetrator acts as if they have complete power over the victim in cyberspace (Ellen & Nenden, 2019). This is considered a criminal act, where the perpetrator commits several crimes simultaneously when creating pornographic deepfakes, for example, several crimes include theft of personal data, disseminating information with content that violates morality, and also manipulation or falsification of data [10]. Based on these types of crimes, referring to the provisions of the Electronic Information and Transactions Law (ITE Law) and its amendments, the Personal Data Protection Law (PDP Law), the Pornography Law, the TPKS Law, and Law No. 1 of 2023 concerning the New Criminal Code (New Criminal Code), Deepfake acts are relevant to the above laws.

Although Indonesia does not yet have specific regulations regarding artificial intelligence or AI technology, especially deepfake, artificial intelligence technology has similar characteristics to electronic agents regulated in the ITE Law and its amendments. Article 1, number 8 of the ITE Law states that an electronic agent is a device of an electronic system created to carry out an action on certain electronic information automatically, which is managed by a person. The word automatic in the article means working alone. In addition, artificial intelligence technology can be defined as a computer-based processing system that can think for itself and make its own decisions. Therefore, the characteristics of artificial intelligence technology can be equated with the characteristics of the electronic agent itself. Pornographic deepfakes as a misuse of AI is one of the acts prohibited under Article 27 paragraph (1) of the ITE Law.

Deepfake, according to the PDP Law, deepfake technology is used to manipulate images or videos using another person's face in its creation. For information, facial images are included in specific biometric data. Based on the PDP Law, the provisions on deepfakes are contained in Article 66 of the PDP Law. Article 4 paragraph (1) of the Pornography Law prohibits everyone from producing, making, reproducing, duplicating, distributing, broadcasting, importing, exporting, offering, selling, renting, or providing pornography that explicitly contains: sexual intercourse, including deviant sexual intercourse; sexual violence; masturbation or onanism; nudity or displays that give the impression of nudity; genitals; or child pornography.

In addition to being regulated in several laws above, pornographic deepfakes are also regulated in Article 407 of the New Criminal Code that anyone who produces, makes, reproduces, duplicates, distributes, broadcasts, imports, exports, offers, sells, rents, or provides pornography, shall be punished with imprisonment of at least 6 months and imprisonment of at most 10 years or a fine of at least category IV, namely IDR 200 million and a fine of at most category VI, namely IDR 2 billion. However, it is important to note that when the new Criminal Code came into effect, Article 27 paragraph (1) of the ITE Law, in conjunction with Article 45 paragraph (1) of Law 19/2016, was revoked and declared invalid.

The misuse of deepfake applications has a serious impact on the tendency towards criminal behavior, which can be analyzed through a criminological lens by considering three main aspects outlined [11]. First, from the perspective of "criminal biology," this approach attempts to identify internal factors within individuals that may be the cause of their criminal behavior. Second, "criminal sociology" seeks the relationship between criminal behavior and the social environment in which the individual operates. Finally, in the context of "criminal policy," appropriate measures must be taken to prevent and address the misuse of deepfake applications. Criminal policy, as a crucial element in criminology, is crucial for formulating appropriate measures for handling the misuse of deepfake applications [12].

From the description of criminological theories, it can be concluded that the application of these theories to cases of deepfake app abuse is urgent. This is because criminological theories can serve as a foundation for decision-makers in efforts to combat crimes related to deepfake apps, so that actions taken can be targeted and effective according to the perpetrator's characteristics and *modus operandi* [13]. In the context of deepfake app abuse, it is important to recognize that perpetrators' motivations can vary. Therefore, using criminological theories helps define and understand acts that may not previously have been categorized as crimes. The criminalization process involves the creation of laws that define prohibited acts and are subject to criminal sanctions. Therefore, a critical understanding of criminological theories is key to designing effective laws to address the complex challenges of deepfake app abuse [14].

The misuse of deepfake applications can be considered an act that qualifies for criminalization, especially when it causes harm to the public, involves victims, and has the potential to cause further harm. The indistinguishability of deepfake edits from the original can mislead the public, increasing the potential for harm to the affected individuals. The misuse of deepfakes, particularly in creating negative content aimed at public figures, can create an unhealthy environment in society. Such incidents can recur repeatedly and continuously, especially with easy access to deepfake applications that allow people to freely edit photos or videos without clear limitations [15]. Therefore, detailed legal regulations and strict sanctions are needed to prevent the misuse of deepfakes. The importance of establishing clear legal regulations and strict sanctions is to mitigate the impact and harm that can be caused by the misuse of deepfakes. This also aims to create a safer environment and suppress the potential spread of negative content generated through deepfakes [16].

3.2 Legal protection for victims of deepfake pornography

Implementing the above-mentioned legal regulations regarding pornography crimes using deepfake technology presents significant challenges that render enforcement largely ineffective. Law enforcement officers face substantial obstacles influenced by three interconnected factors including [2].

From a legal perspective, the distribution of pornographic content created through artificial intelligence (AI) technology, particularly deepfakes, lacks specific regulation within Indonesian law. This creates a critical gap in legal certainty, as authorities struggle to determine which legal

framework applies when prosecuting cases involving deepfake-generated pornographic content distributed on social media. The absence of targeted legislation means such cases could potentially fall under multiple laws, creating ambiguity in the prosecution process.

Technological challenges further complicate enforcement efforts. Deepfake technology represents a relatively new phenomenon involving sophisticated artificial intelligence that can seamlessly combine, replace, or overlay images and video clips to create convincing fabricated content. The resulting videos appear authentic, making it virtually impossible for viewers to distinguish manipulated material from genuine footage. This technology enables the production of videos showing individuals apparently saying or doing things they never actually said or did, creating significant evidentiary and identification challenges for investigators.

Additionally, law enforcement capacity remains inadequate to address this emerging threat. Cases involving deepfake-generated pornographic videos are still relatively rare and unfamiliar to most law enforcement agencies. These cases typically target public figures or celebrities and predominantly involve pornographic content. However, authorities have demonstrated limited responsiveness to these novel violations, often failing to deploy sufficient resources or develop specialized expertise to identify perpetrators effectively [17]. This lack of proactive engagement allows offenders to operate with relative impunity in this emerging technological landscape.

The following will explain examples of deep fake pornography cases and legal protection, accompanied by an analysis of the imposition of articles that can be applied in such cases: The Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency arrested a man with the initials MS (39). He was arrested for spreading content that insulted ethnic groups and edited photos of President Joko Widodo. MS also deliberately showed hatred towards others by committing racial discrimination. The suspect also deliberately showed hatred or insults towards one or several groups of Indonesian people. The Cyber Patrol Team found an account named Ahmad Fatihul Alif, which contained hate speech and racism. The suspect in this case utilized two Facebook accounts to disseminate hateful content, operating under the names Ahmad Fatihul Alif and Ilham Al Syahidi. The prosecution of this case was based on Article 16, in conjunction with Article 4, number 1 of Law Number 40 of 2008 concerning the Elimination of Racial and Ethnic Discrimination. The evidence clearly satisfied all required legal elements: the perpetrator was identified as Ahmad Fatihul Alif, who intentionally distributed manipulated content and edited photographs of President Jokowi with the clear purpose of demonstrating hatred and inciting racism toward others. These actions constituted racial discrimination and insults directed at one or more groups within Indonesian society, thereby fulfilling the criteria for hate speech based on racial and ethnic discrimination.

This case highlights a broader challenge facing Indonesia's legal framework. The absence of specific regulations governing the use of artificial intelligence (AI) technology in creating pornographic deepfakes has created a significant legal vacuum that demands urgent attention immediately [18]. When photos or videos are manipulated using deepfake technology and subsequently distributed, these actions constitute cybercrime—criminal activities occurring within the digital realm of cyberspace [19]. As cyberspace continues to evolve as an increasingly integral dimension of human interaction, it has simultaneously become a breeding ground for illegal activities. Deepfake technology, in particular, clearly falls within the category of illegal content that exploits this digital environment [20]. Given these emerging threats, the development of comprehensive and specific legislation addressing AI technology in the context of deepfakes has become critically important. Such regulations would not only establish clear legal foundations for prosecution but also serve as essential mechanisms to mitigate the risks associated with technology misuse that can cause substantial harm to individuals and society at large.

It is crucial to protect victims without compromising the individual's right to privacy and freedom of expression. Given that pornographic deepfakes constitute a violation of pornography laws, Indonesia requires specific legislation governing telecommunications through AI technology. It is crucial to ensure the responsible and ethical use of AI technology by employing highly sophisticated monitoring systems and deepfake detection tools. Furthermore, regulations and ethical norms must be considered in the development of AI to ensure its fair, safe, and privacy-respecting use. Beyond establishing regulations, educating users about AI is crucial so they understand the impacts and risks of this technology. This will help the public use AI technology more wisely and responsibly, while also preventing the legal issues. Victims of fake pornography should receive appropriate protection, including robust tools to report and address the consequences they experience, such as falsified photos or videos that damage their reputations. While technology to identify deepfakes continues to advance, challenges remain in identifying them quickly and accurately. Therefore, investment in research and development of more advanced technologies is needed to combat the threat of deepfakes [21].

Comprehensive deepfake education is also needed to raise public awareness. Educational campaigns should include information that is easily understood by the public, explain how deepfakes work, and provide examples of high-profile cases involving deepfakes. Schools and educational institutions should also play a crucial role in educating students on how to distinguish fake content and the risks of deepfakes. Media and online platforms can play a role in disseminating this information widely and providing users with practical guidance on how to protect themselves [20]. However, to identify, pursue, and prosecute perpetrators of deepfakes, a cross-border law enforcement mechanism is needed. This mechanism helps identify perpetrators who may be located outside the jurisdiction of the victim's country, gather evidence related to deepfakes, pursue prosecution of perpetrators in multiple jurisdictions, and create a uniform legal framework. Partnerships between countries are also crucial in preventing and enforcing laws against deepfake pornography, given that perpetrators often operate in multiple countries [16].

Effective extradition treaties and a robust legal framework are essential in this regard. Regular evaluation of public awareness programs, legal regulations, and technology is also crucial to ensure the effectiveness of the measures taken. A comprehensive and sustainable approach can protect the public from the dangers of deepfake pornography and prevent the spread of harmful content. Furthermore, to improve cross-border law enforcement mechanisms, countries must cooperate more actively and share information on deepfakes. This can be achieved through bi-state and tri-state agreements, as well as agreements between more than one country, that establish a framework for cooperation to combat deepfakes [22].

The development of dedicated teams working across borders to investigate deepfake cases involving perpetrators in multiple jurisdictions is part of this effort. The role of digital service providers, such as social media platforms and video-sharing websites, is also crucial in this effort. They must have strict policies regarding fake content and deepfakes, and effective systems for reporting them to users who encounter them. To mitigate the impact of deepfakes, service providers and authorities must work together to address them and identify perpetrators. Furthermore, platform transparency in tracking and addressing deepfakes must be improved. This includes the functions platforms perform to identify, remove, and report deepfake content to authorities. To mitigate the spread of deepfakes on these platforms, more effective monitoring systems must be implemented [23].

In combating the threat of deepfakes, strict and effective regulations are the main foundation for law enforcement against perpetrators. The continued development of deepfake identification techniques is key to identifying manipulated content. Broad public awareness and international

collaboration are crucial for protecting victims and reporting suspicious content. Public education about digital conditions and continuous evaluation of the effectiveness of preventative measures are integral to this effort. Developing international law, collaborating with online platforms, developing digital ethics, and supporting victims are also essential components in addressing the deepfake phenomenon.

4. Conclusion

Based on the analysis described above, a conclusion is drawn regarding the formulation of the problem, namely Deepfakes is a human image engineering technology or synthetic technique based on real visual Artificial Intelligence (AI). Deepfake Pornography is also included as Online Gender-Based Violence, the perpetrator of deepfake pornography in carrying out their actions will steal the victim's body authority by engineering the victim to do something the perpetrator wants without the victim's permission or even knowledge. Misuse of deepfake applications can be considered an action that meets the requirements to be criminalized as a crime, especially when it causes harm felt by the community, there are affected victims, and the potential to cause further harm. The urgency of addressing the problem of deepfake must be taken seriously to prevent greater harm. The urgency of addressing the problem of deepfake must be taken seriously to prevent greater harm. In cases of criminal acts of deepfake pornography, the provisions in Article 27 paragraph (1) of the Electronic Information and Transactions Law (ITE Law) and its amendments, Article 66 of the Personal Data Protection Law (PDP Law), Article 4 paragraph (1) of the Pornography Law, or Law No. 1 of 2023 concerning the new Criminal Code, Article 14 paragraph (1) of the TPKS Law, Article 407 of Law 1 of 2023 concerning the new Criminal Code.

Acknowledgement

The authors would like to express their sincere gratitude to Universitas Widya Mataram for providing internal research funding under contract number 23/LPPM-UWM/II/2025. Special appreciation is extended to LPPM (Lembaga Penelitian dan Pengabdian kepada Masyarakat) Universitas Widya Mataram for managing the research grant, and to the reviewers for their valuable feedback. The authors also thank the Criminal Law Department for institutional support, as well as the staff and students who participated in the research implementation.

Authors' contributions and responsibilities

Nia Kurnia: conceptualization, methodology, investigation, resources, data curation, writing-original draft. Laili Nur Anisah: methodology, formal analysis, resources, visualization, supervision, writing- review& editing.

Funding

This research was supported by internal research funding from Universitas Widya Mataram under contract number 23/LPPM-UWM/II/2025.

Availability of data and materials

All data are available from the authors.

Competing interests

The authors declare no competing interest.

Additional information

No additional information from the authors.

References

- [1] A. N. Utama, P. T. Kesuma, and R. M. Hidayat, "Analisis hukum terhadap upaya pencegahan kasus deepfake porn dan pendidikan kesadaran publik di lingkungan digital," *Jurnal Pendidikan Tambusai*, vol. 7, no. 3, pp. 26179–26188, Nov. 2023, doi: 10.31004/jptam.v7i3.10815.
- [2] E. I. Utawi and Neni Ruhaeni, "Penegakan hukum terhadap tindak pidana pornografi menurut peraturan perundang-undangan tentang pornografi melalui media sosial," *BCSLs*, vol. 3, no. 1, Jan. 2023, doi: 10.29313/bcsls.v3i1.4988.
- [3] "CATAHU 2022: Kekerasan terhadap perempuan di ranah publik dan negara: minimnya perlindungan dan pemulihan." Accessed: Oct. 12, 2025. [Online]. Available: <https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2022-kekerasan-terhadap-perempuan-di-ranah-publik-dan-negara-minimnya-perindungan-dan-pemulihan>
- [4] N. H. Mongkau, H. Y. A. Bawole, and A. A. Musa, "Penegakkan hukum terhadap penyalhgunaan kecerdasan buatan dengan cara memanipulasi wajah seseorang ke dalam gambar atau video porno," vol. 13, no. 2, 2025.
- [5] H. Z. Haefani and A. S. Mulyanti, "Urgensi reformasi hukum pidana indonesia dalam menjerat pelaku deepfake pornografi berbasis artificial intellegence | ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora," Jul. 2025, Accessed: Oct. 12, 2025. [Online]. Available: <https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH/article/view/1554>
- [6] M. Yudha *et al.*, "Perlindungan hukum bagi korban penggunaan deepfake dalam kejahatan pornografi," *Indonesian Journal of Sharia and Law*, vol. 2, no. 1, pp. 24–37, Jan. 2025, doi: 10.54622/ijsl.v2i1.371.
- [7] I. D. Kasita, "Deepfake Pornografi: Tren kekerasan gender berbasis online (KGBO) di era pandemi covid-19," *JWK*, vol. 3, no. 1, pp. 16–26, Jul. 2022, doi: 10.22146/jwk.5202.
- [8] S. Soekanto and S. Mamudji, *Penelitian hukum normatif: suatu tinjauan singkat*. Penerbit CV. Rajawali, 1986.
- [9] C. P. Samosir, "Kekerasan berbasis gender online (KBGO) dan cara mendukung korban: analisis konten film like dan share," *Jurnal PIKMA: Publikasi Ilmu Komunikasi Media Dan Cinema*, vol. 6, no. 1, pp. 230–245, Oct. 2023, doi: 10.24076/pikma.v6i1.1303.
- [10] S. A. U. Sijabat and D. Lukitasari, "Konten gambar dan video pornografi deepfake sebagai suatu bentuk tindak pidana pencemaran nama baik," *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, vol. 13, no. 2, pp. 179–194, Jul. 2024, doi: 10.20961/recidive.v13i2.86771.
- [11] H. Novyanti and P. Astuti, "Jerat hukum penyalhgunaan aplikasi deepfake ditinjau dari hukum pidana," *Novum: Jurnal Hukum*, vol. 9, no. 04, pp. 31–40, 2022, doi: 10.2674/novum.v0i0.43571.
- [12] C. T. Noerman and A. L. Ibrahim, "Kriminalisasi deepfake di Indonesia sebagai bentuk perlindungan negara," *Jurnal Usm Law Review*, vol. 7, no. 2, pp. 603–621, Jun. 2024, doi: 10.26623/julr.v7i2.8995.
- [13] M. A. Kholiq, "Urgensi pemikiran kritis dalam pengembangan kriminologi Indonesia di masa mendatang," *Iustum*, vol. 7, no. 15, pp. 161–174, 2000, doi: 10.20885/iustum.vol7.iss15.art12.
- [14] D. P. R. Pane and A. W. Tambe, "Tantangan penegakan hukum dan upaya mitigasi atas hadirnya deepfake porn sebagai jenis tindak pidana digital pada era artificial intelligence," *pk*, vol. 2, no. 3, pp. 185–203, Jul. 2025, doi: 10.62383/pk.v2i3.1055.

- [15] O. Novera and Yenny Fitri.Z, "Analisis pengaturan hukum pidana terhadap penyalahgunaan teknologi manipulasi gambar (Deepfake) dalam penyebaran konten pornografi melalui akun media sosial," *faqih*, vol. 10, no. 2, pp. 460–474, Oct. 2024, doi: 10.58401/faqih. v10i2.1539.
- [16] R. S. Arvitto, "Implikasi hukum deepfake: telaah terhadap UU ITE dan UU PDP," *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, vol. 4, no. 2, pp. 73–82, Jan. 2025, doi: 10.35912/jihham. v4i2.3937.
- [17] S. A. Kusnadi and D. W. S. Putri, "Perlindungan hak privasi dalam penyalahgunaan teknologi deepfake di Indonesia," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, vol. 14, no. 2, Aug. 2025, doi: 10.33331/rechtsvinding. v14i2.2135.
- [18] S. Gandrova and R. Banke, "Penerapan hukum positif indonesia terhadap kasus kejahatan dunia maya deepfake," *Madani: Jurnal Ilmiah Multidisiplin*, vol. 1, no. 10, Nov. 2023, doi: 10.5281/zenodo.10201140.
- [19] A. W. Laksana and S. Suratman, "Analisis yuridis penyidikan tindak pidana pornografi berdasarkan undang-undang nomor 44 tahun 2008 di era digitalisasi," *Jurnal Pembaharuan Hukum*, vol. 1, no. 2, pp. 169–177, Aug. 2014, doi: 10.26532/jph. v1i2.1473.
- [20] A. N. F. Rahman and F. Bari, "Perlindungan Hukum terhadap Korban Penyalahgunaan Teknik Deepfake".
- [21] P. F. Unpad, "Perlindungan hukum bagi korban deepfake pornografi: evaluasi efektivitas hukum positif dan...," Medium. Accessed: Oct. 12, 2025. [Online]. Available: <https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35>.
- [22] D. A. Y. Basah, A. Wijaya, and I. Januardy, "Kriminalisasi pelanggaran protokol digital: tinjauan hukum pidana terhadap penyebaran deepfake di media sosial," *Innovative: Journal of Social Science Research*, vol. 5, no. 4, pp. 386–398, Jul. 2025, doi: 10.31004/innovative. v5i4.20258.
- [23] M. A. Chairani, K. Yitawati, and A. P. Pradhana, "Urgensi pengaturan hukum bagi penyalahgunaan aplikasi deepfake," *Jurnal Rechtsens*, vol. 13, no. 1, pp. 81–96, Jun. 2024, doi: 10.56013/rechtsens. v13i1.2668.