

Legal Protection of Victims of AI-Driven Deepfake Pornography: An Analysis within Indonesian Law

Siti Nur Hidayah^{1*}, Gunawan Hadi Purwanto²

¹E-mail: siti.nurhidayah1415@gmail.com

²E-mail: gunawanhadipurwanto565@gmail.com

^{1,2}Universitas Bojonegoro, Indonesia

*corresponding author

Article history:

Received: 17 December 2025

Revised: 19 January 2026

Acceptance date: 11 March 2026

Available online: 30 April 2026

Keywords:

Deepfake Pornography; Artificial Intelligence; Victim Protection; Personal Data Protection; Indonesian Cyber Law.

How to Cite:

Hidayah, S. N., & Hadi Purwanto, G. (2026). Legal Protection of Victims of AI-Driven Deepfake Pornography: An Analysis within Indonesian Law. *Al-Risalah Jurnal Ilmu Syariah Dan Hukum*.

<https://doi.org/10.24252/al-risalah.vi.63687>

License:

Copyright (c) The authors (2026)



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

Abstract

The development of Artificial Intelligence technology has led to new forms of digital crime, one of which is deepfake pornography. This crime involves the manipulation of a person's facial identity into pornographic content without consent, resulting in serious violations of privacy, dignity, reputation, and psychological well being. This study aims to analyze the legal construction of deepfake pornography within the Indonesian legal system and to examine the forms of legal protection available for victims. This research employs a normative legal method using statutory and conceptual approaches, supported by prescriptive and interpretative analysis of primary, secondary, and tertiary legal materials. The findings indicate that although several laws, such as the Pornography Law, the Information and Electronic Transactions Law, the Personal Data Protection Law, and the Law on Sexual Violence Crimes, may be applied to prosecute perpetrators, Indonesia still lacks a specific, comprehensive regulation that addresses the unique technical complexities of AI-generated content. This regulatory gap leads to inconsistencies in law enforcement and fails to address the rapid, borderless dissemination of deepfakes, leaving victim protection severely limited, particularly regarding long-term psychological recovery and the complex restoration of digital reputation. This study highlights the urgency of establishing a comprehensive, victim-centered legal framework that integrates criminal, civil, and administrative approaches within a global context, acknowledging that technologically driven harms constitute a pervasive and transnational challenge faced by legal systems worldwide.

INTRODUCTION

The development of information and communication technology in the digital era has brought about highly significant changes in society. Digital technology not only functions as a medium for communication and information exchange, but also shapes patterns of social interaction, power relations, and the ways in which individuals represent their identities in the public sphere.¹ Behind the various conveniences and efficiencies it offers, the advancement of digital technology simultaneously gives rise to new forms of crime that are transnational, anonymous, and difficult to control.² This condition demonstrates that technological development always goes hand in hand with the potential for misuse, thereby requiring legal responses that are adaptive and oriented toward the protection of human rights.³

One concrete manifestation of digital technological development that has influenced patterns of cybercrime is the advancement of Artificial Intelligence (AI).⁴ AI is a technology designed to imitate human cognitive abilities, such as learning, analyzing, recognizing patterns, making predictions, and making decisions automatically through large-scale data processing. The presence of AI has provided numerous benefits in daily life, ranging from education, healthcare, and creative industries to public services. However, behind these benefits, AI also creates opportunities for increasingly complex digital crimes, particularly when this technology is misused for unlawful and unethical purposes.⁵ One rapidly developing form of AI misuse is deepfake technology. Deepfake is a form of digital content manipulation that utilizes Artificial Intelligence to fabricate a person's face or identity in images or videos, making them appear authentic even though they do not reflect reality.⁶ Initially, deepfake technology was used for entertainment, education, and technological research purposes.

¹ Jonathan Raymond Frederick Agestya Petra Amelia, Izzaty Nagita Putri, "Konstruksi Identitas Sosial Oleh Media Sosial : Studi Kritis Berdasarkan Pemikiran Marcuse Dan Habermas," *Jurnal Perspektif* 8, no. 3 (2025): 363–69, <https://doi.org/10.24036/perspektif.v8i3.1258>.

² Zahra Pitaloka Islami, "Tantangan Penegakan Hukum Di Era Globalisasi Digital : Strategi Menghadapi Kejahatan Siber Lintas Batas," *Jurnal Sains Ekonomi Dan Edukasi* 2, no. 12 (2025): 2579–91.

³ Timbul Dompok Elvan Maulana Rif'at, "Hak Asasi Manusia Di Era Digital : Tantangan Dan Peluang Dalam Mengatasi Kejahatan Siber," *Jurnal Ilmu Multidisiplin* 3, no. 1 (2025).

⁴ Renato Toasa and Maryory Urdaneta Carlos Varela Enríquez, "The Use of Artificial Intelligence in Cybercrime : Impact Analysis in Ecuador and Mitigation Strategies," *Journal of Cybersecurity and Privacy*, 2025, <https://doi.org/10.3390/jcp5040100>.

⁵ Mayur Shrestha Abhishek Gupta, "Menghadapi Dilema Teknologi Dan Hukum Dalam Eksploitasi Selebritas Yang Tidak Sah Informasi," *Jurnal Tren Baru Dan Penelitian Baru* 2, no. 12 (2024): 372–80.

⁶ Mahmutarom Mahrus Ali, Zico Junius Fernando, Chairul Huda, "Deepfake Dan Viktimologi : Menjelajahi Dampak Manipulasi Digital Terhadap Korban," *Jurnal Hukum Internasional Keadilan Substantif* 8, no. 1 (2025): 1–12, <https://doi.org/10.56087/substantivejustice.v8i1.306>.

Deepfake pornography is one of the most dangerous forms of digital crime because it involves manipulating a person's face into pornographic content without the victim's consent. This crime creates the impression that the victim is directly involved in sexual activities, even though, in reality, the victim has never engaged in such acts. According to a study by Deeptrace, approximately 96% of all analyzed deepfake videos contain pornographic content, and since 2019 the number of such materials has increased significantly.⁷ This data indicates that deepfake pornography has become a serious threat in the digital space, particularly for women, who are often the primary targets of such crimes.⁸

The widespread use of social media further accelerates the dissemination of deepfake pornographic content. Photos, videos, and personal data uploaded to digital public spaces can be easily exploited by perpetrators to create manipulative content. The spread of such content occurs rapidly and is difficult to control, causing victims to experience repeated harm as the content continues to circulate even after being reported or removed. The impacts experienced by victims are not limited to reputational damage, but also include psychological distress, social stigma, and a loss of security in both social and professional life.⁹

From a human rights perspective, deepfake pornography constitutes a serious violation of the rights to privacy, honor, and human dignity. These rights are guaranteed under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. In addition, Indonesia has ratified the International Covenant on Civil and Political Rights (ICCPR) through Law Number 12 of 2005, which, under Article 17, guarantees protection of individual privacy and reputation. Therefore, the practice of deepfake pornography without the victim's consent clearly contradicts human rights principles.¹⁰

Furthermore, deepfake pornography can be categorized as a form of Technology-Facilitated Sexual Violence and Online Gender-Based Violence (KBGO).¹¹ This crime

⁷ Christella Madalaine, "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi Madalaine Christella Seveney 1 , Demas Brian Wicaksono 2 , Irwan Kurniawan Soetijono 3," *Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31, no. 2 (2025): 97-106, <https://ojs.stihpada.ac.id/index.php/disiplin>.

⁸ Any Nugroho Memei Apriana, Fransisco, "Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (Ai) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual," *Jurnal Sosial Dan Ekonomi* 3(2), no. 1 (2021): 123-38, <https://idm.or.id/JSER/index.php/JSEROpen>.

⁹ Mahrus Ali, Zico Junius Fernando, Chairul Huda, "Deepfake Dan Viktimologi : Menjelajahi Dampak Manipulasi Digital Terhadap Korban."

¹⁰ Mahrus Ali, Zico Junius Fernando, Chairul Huda.

¹¹ Ivana Dewi Kasita, "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KBGO) Di Era Pandemi Covid-19," *Jurnal Wanita Dan Keluarga* 3, no. 1 (2022): 16-26, <https://doi.org/10.22146/jwk.5202>.

involves non-physical sexual elements, is committed without the victim's consent, and often places women as the most vulnerable group to digital exploitation. From a victimological perspective, victims of digital crimes such as deepfake pornography often experience layered suffering, including psychological trauma, social pressure, and the risk of revictimization.¹²

Previous studies have shown that the use of Artificial Intelligence in the context of non-consensual pornography has resulted in serious impacts on victims' privacy, dignity, and security.¹³ Research across various jurisdictions reveals that existing legal regulations are generally unable to keep pace with the development of deepfake technology, resulting in challenges in law enforcement against perpetrators, including issues of evidence, criminal qualification, and victim protection.¹⁴ These studies also highlight a tendency in criminal law to focus more on punishing perpetrators, while aspects of victim recovery and protection have not received adequate attention.

In the Indonesian context, although several studies have discussed deepfake pornography from the perspectives of criminal law and information technology, research that specifically frames deepfake pornography as a form of AI-based sexual violence and comprehensively examines legal protection for victims remains limited.¹⁵ Moreover, existing regulations, such as the Law on Electronic Information and Transactions, the Pornography Law, the Law on Sexual Violence Crimes, and the Personal Data Protection Law, have not explicitly and integratively regulated deepfake pornography as an AI-based crime. This condition creates a legal vacuum that leads to legal uncertainty and suboptimal protection for victims.¹⁶

Based on the above explanation, there is a gap between the development of Artificial Intelligence technology and the readiness of the national legal system to provide effective

¹² Memei Apriana, Fransisco, "Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (Ai) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual."

¹³ Zevanya Praja Syaharani, "Dari Fantasi Digital Ke Kekerasan Nyata Analisis Hukum Atas Kasus Deepfake Pornografi Dan Tanggung Jawab Negara," *Maleo Law Journal* 9, no. 2 (2025).

¹⁴ Ariy Khaerudin Indah Rohmawati, Amir Junaidi, "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBG0)," *Journal Of Social Science Research* 4 (2024): 1779-94, <https://j-innovative.org/index.php/Innovative%0AUrgensi>.

¹⁵ Juandry Aruan, "Legal Protection for Victims of Photo Abuse through Artificial Intelligence Technology in Pornography Crimes in Indonesia," *Law & Society Review* 5, no. 2 (2025): 1831-62, <https://doi.org/10.15294/lsr.v5i2.3834>.

¹⁶ Moody Risky Syailendra Putra Ivana Trixie, "Studi Perbandingan: Perlindungan Hukum Terhadap Deepfake Berbasis Kecerdasan Buatan (Ai)," *Jurnal Pendidikan Sejarah Dan Riset Sosial Humaniora (KAGANGA)* 8, no. 6 (2025), <https://doi.org/10.31539/gm8q1a03>.

protection for victims of deepfake pornography.¹⁷ Therefore, this study is important to analyze the legal construction of deepfake pornography within the Indonesian legal system and to examine forms of legal protection for victims, including preventive, repressive, and restorative approaches.

Normatively, Indonesia already has several laws and regulations that can be used to prosecute perpetrators of deepfake pornography, such as the Law on Electronic Information and Transactions, the Pornography Law, the Law on Sexual Violence Crimes, and the Personal Data Protection Law. However, to date, there is no explicit and comprehensive regulation governing deepfake pornography as an Artificial Intelligence-based crime. This situation results in a legal vacuum that contributes to legal uncertainty and inadequate protection for victims.¹⁸

Based on these considerations, it is evident that there is a disparity between the advancement of Artificial Intelligence technology and the preparedness of national law in providing effective protection for victims of deepfake pornography. Accordingly, this research aims to analyze the legal construction of deepfake pornography within the Indonesian legal system and to examine forms of legal protection for victims through preventive, repressive, and restorative approaches.

METHODS

This study employs a normative legal method, as it aims to analyze positive law related to AI-based deepfake pornography in Indonesia,¹⁹ assess the effectiveness of existing legal regulations, and identify legal gaps that affect victim protection. The normative method is chosen because it enables a systematic and scholarly examination of applicable legal norms, principles, and doctrines. The legal materials used in this study consist of primary sources, such as statutory regulations, court decisions, and official documents; secondary sources, including legal literature, journals, and scholarly articles; and tertiary sources, such as legal dictionaries, encyclopedias, and other supporting references.²⁰

¹⁷ Indah Rohmawati, Amir Junaidi, "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)."

¹⁸ Muhammad Afif, "Tindak Pidana Deepfake Pornography Di Indonesia : Analisis Yuridis Terhadap Kekosongan Norma Dalam KUHP Dan UU ITE," *Jurnal Ilmiah Multidisiplin* 3, no. 2 (2025): 27–35, <https://doi.org/10.62017/merdeka>.

¹⁹ Gunawan Hadi Purwanto, "Penetapan Putusan Pengadilan Negeri Surabaya Tentang Perkawinan Beda Agama Dalam Perspektif Hukum Positif," *Binamulia Hukum* 12, no. 1 (2023): 253–62, <https://doi.org/10.37893/jbh.v12i2.425>.

²⁰ M.A Dr. Drs. H. Rifa'i Abubakar, *Pengantar Metodologi Penelitian* (UIN Sunan Kalijaga, 2021).

The analysis is conducted through statutory and conceptual approaches, employing interpretative techniques to construe legal rules and human rights principles, as well as prescriptive techniques to evaluate the adequacy of the law in addressing cases of deepfake pornography.²¹ These approaches are applied to address the research questions, namely how deepfake pornography is legally constructed within Indonesian law and what forms of legal protection are available for victims. Accordingly, this study seeks to provide a critical assessment, identify legal loopholes, and formulate relevant recommendations for victim protection.

The collection of legal materials is carried out through a library-based research method by examining various legal sources, including primary, secondary, and tertiary materials.²² Furthermore, the analysis of legal materials adopts a normative juridical approach, focusing on statutory regulations and relevant legal doctrines to understand and examine the crime of deepfake pornography in the era of Artificial Intelligence.²³

RESULT AND DISCUSSION

1. Legal Construction of AI-Based Deepfake Pornography in Indonesian Law

The development of Artificial Intelligence technology has given rise to new and complex forms of crime, one of which is deepfake pornography.²⁴ As noted by Marissa Koopman, Andrea Macarulla Rodriguez, and Zeno Geradts in their study, deepfake technology is an algorithm that enables users to replace a person's face in a video with another person's face in a photorealistic manner.²⁵ Therefore, deepfake pornography can be defined as manipulated content created by inserting a person's face into pornographic material using Artificial Intelligence, thereby creating the impression that the individual is genuinely involved in the depicted activity.²⁶ This practice is often intended to conceal the actual perpetrator by substituting their face or body with that of another person.

²¹ Maria Karunia dkk., "Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana perundang-undangan dan pendekatan konseptual, proses analisa yang meliputi metode, menganalisis regulasi penyimpan," *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora* 4 (2025): 296-307.

²² MH Dr. H. Nur Solikin, S.Ag., *Pengantar Metodologi Penelitian Hukum*, 2021.

²³ Nur Solikin, S.Ag., *Pengantar Metodologi Penelitian Hukum*, h. 124.

²⁴ Muhammad Afif, "Tindak Pidana Deepfake Pornography Di Indonesia : Analisis Yuridis Terhadap Kekosongan Norma Dalam KUHP Dan UU ITE."

²⁵ Adnasohn Aqilla Respati et al., "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban," *Media Hukum Indonesia* 2, no. 2 (2024): 586-93, <https://doi.org/10.5281/zenodo.12508126>.

²⁶ Silvia Maharani, "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum," *Jurnal Hukum Legalita* 6 (2023): 83-90, <https://doi.org/10.47637/legalita.v6i2.1453> Kriminalisasi.

The misuse of deepfake technology poses a tangible threat to data protection and digital systems.²⁷ Mechanistically, deepfake technology relies on a widely known framework called Generative Adversarial Networks (GANs).²⁸ The sophistication of GANs makes deepfake pornography a serious legal concern, as the system continuously learns and improves the quality of manipulated outputs, rendering such content increasingly difficult to detect.²⁹ This challenge is further exacerbated by the widespread availability of publicly accessible AI-based software, enabling virtually anyone to create deepfake pornographic content with ease.³⁰ Moreover, the dissemination of such content is amplified by extensive distribution networks and weak controls over misinformation.³¹ Numerous video-sharing platforms, such as TikTok, Instagram, YouTube, and Facebook, provide avenues for rapid spread.³² Accordingly, any person who intentionally and unlawfully disseminates false information or content involving elements of falsification, obscenity, sexual exploitation, fraud, violations of privacy rights, or defamation may be subject to criminal liability.³³

Based on normative legal research, Indonesian positive law has not yet explicitly regulated deepfake pornography as a distinct criminal offense.³⁴ This absence of specific regulation results in law enforcement relying on interpretative applications of existing legislation.³⁵ In practice, law enforcement authorities tend to classify deepfake pornography under conventional criminal law frameworks, particularly through Law Number 44 of 2008 on Pornography. The act of inserting a person's face into sexually

²⁷ Cleophila Natania Putri Hernawan, "Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intelligence Dalam Tindak Pidana Kekerasan Seksual," *Lex Privatum Jurnal Fakultas Hukum Unsrat* 15, no. 4 (2025).

²⁸ Hendra Prayoga, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia," *Abdurrauf Law and Sharia* 1, no. 2 (2024): 22–38, <https://doi.org/10.70742/arlash.v2i1.194>.

²⁹ Hendra Prayoga.

³⁰ Brent Mittelstandt Will Hawkins, Chris Russell, *Deepfakes on Demand : The Rise of Accessible Non-Consensual Deepfake Image Generators, Proceedings of (FAccT '25)*, vol. 1 (Association for Computing Machinery, 2023).

³¹ Yenny Fitri Z Olivia Novera, "Analisis Pengaturan Hukum Pidana Terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) Dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial," *Jurnal Pemikiran Hukum Dan Hukum Islam* 10, no. 2 (2024): 460–74, <https://ejournal.iaifa.ac.id/index.php/faqih>.

³² Vressilia Witama Putri Ramadhani Rangkuti, Rahma Fitri Amelia Hasibuan and Siti salmiah Maria Arfah Nasution, Siti Kholizah, Nadilah Andini, "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE : Studi Kasus Di Media Sosial Indonesia Universitas Islam Negeri Sumatera Utara Medan, Indonesia," *Jurnal Publikasi Ilmu Hukum* 3 (2025).

³³ Respati et al., "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban."

³⁴ Rafi Satrya Arvitto, "Implikasi Hukum Deepfake : Telaah Terhadap UU ITE Dan UU PDP," *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 4, no. 2 (2025): 73–82, <https://doi.org/10.35912/jihham.v4i2.3937>.

³⁵ Hendra Prayoga, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia."

explicit content without consent may be interpreted as “producing” or “creating” pornographic material.³⁶ Furthermore, the dissemination of such content through digital media fulfills the element of “distribution” as stipulated in the law.³⁷ However, the Pornography Law primarily focuses on the existence and dissemination of pornographic content and does not adequately address violations of digital identity and the dignity of victims as legal subjects.³⁸

In addition to the Pornography Law, Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) is also applied to prosecute perpetrators of deepfake pornography, particularly through provisions related to the distribution of content that violates decency norms.³⁹ Nevertheless, the concept of decency under the ITE Law remains abstract and does not specifically anticipate AI-based digital identity manipulation. As a result, proving elements such as intent, perpetrator involvement, and the authenticity of digital content often becomes a significant challenge in law enforcement practice.

The analysis further indicates that Law Number 27 of 2022 on Personal Data Protection provides a more relevant legal basis in the context of deepfake pornography.⁴⁰ A person’s face constitutes biometric personal data that is legally protected; thus, the use or processing of such data without the individual’s consent may be classified as a legal violation. Accordingly, the Personal Data Protection Law introduces a victim-oriented protection framework, rather than focusing solely on controlling pornographic content. However, its effectiveness within the criminal law regime still requires strengthening, particularly in terms of coordination with substantive criminal law and the imposition of proportionate sanctions.⁴¹

³⁶ Diana Lukitasari Sarah Amanda Uly Sijabat, “Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik,” *Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 13, no. 2 (2024): 179–94.

³⁷ Halomoan Freddy Sitinjak Alexandra, “Pemberian Restitusi Dan Kompensasi Bagi Korban Tindak Pidana Berdasarkan Nilai Keadilan,” *Jurnal Pendidikan Dan Konseling* 4, no. 5 (2022): 5975–84.

³⁸ Muhammad Afif, “Tindak Pidana Deepfake Pornography Di Indonesia : Analisis Yuridis Terhadap Kekosongan Norma Dalam KUHP Dan UU ITE.”

³⁹ Cindy Natalia, “Perlindungan Hukum Bagi Korban Pornografi Deepfake Dalam Konteks Hukum Indonesia,” *Jurnal Kertha Desa* 12, no. 19 (2024).

⁴⁰ Anita Firdausi, “Tinjauan Etis Dan Hukum Terhadap Perlindungan Data Pribadi Di Tengah Maraknya Konten Deepfake Di Media Sosial,” *Jurnal Hukum Dan Kewarganegaraan* 12, no. 5 (2025), <https://doi.org/10.3783/causa.v2i9.2461>.

⁴¹ Muhammad Fadly Nasution Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, “Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana Di Indonesia,” *Jurnal Minfo Polgan Volume* 14, no. 1 (2025).

Normatively, AI-based deepfake pornography should be understood as a form of technology-facilitated sexual crime with distinct characteristics, including digital identity manipulation, the absence of victim consent, and serious impacts on personal dignity and security.⁴² Therefore, legal approaches that rely solely on decency norms and the distribution of pornographic content are no longer sufficient. A more comprehensive legal construction is required—one that explicitly recognizes digital identity manipulation as a constituent element of the offense and places victims at the center of legal protection. Harmonization among the Pornography Law, the ITE Law, the Law on Sexual Violence Crimes, and the Personal Data Protection Law is urgently needed to close regulatory gaps and strengthen legal certainty in addressing deepfake pornography crimes in Indonesia.

2. Legal Protection for Victims of AI-Based Deepfake Pornography Crimes

The development of Artificial Intelligence technology has given rise to new forms of crime that pose serious threats to human rights, one of which is deepfake pornography. This crime places victims in a highly vulnerable position because the manipulation of their faces into pornographic content is carried out without consent, thereby violating the rights to privacy, honor, and human dignity. Victims of deepfake pornography not only suffer reputational damage in the public sphere but also endure prolonged psychological harm, including emotional trauma, anxiety, depression, and revictimization due to the repeated dissemination of such content in digital media.⁴³ These characteristics demonstrate that deepfake pornography constitutes a form of technology-based victimization with multidimensional impacts, thereby requiring a victim-oriented approach to legal protection.⁴⁴

Within the context of Indonesian law, the protection of victims of deepfake pornography can normatively be classified into preventive and repressive legal protection. Preventive legal protection aims to prevent violations of victims' rights from the outset; however, it still faces fundamental weaknesses. The absence of specific regulations explicitly governing the misuse of Artificial Intelligence, particularly deepfake pornography, forces the state to rely on general legal instruments such as the

⁴² Dona Raisa Monica Naufal Zuhdi, Heni Siswanto, "Peran Kepolisian Terhadap Ancaman Kejahatan Pelecehan Seksual Melalui Modus Deepfake Porn Di Era Digital," *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial Dan Politik* 2, no. April (2025), <https://doi.org/10.62383/demokrasi.v2i2.856>.

⁴³ Memei Apriana, Fransisco, "Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (Ai) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual."

⁴⁴ Alif Alfani Rahman Doni Noviantama, "Deepfake : Sebuah Ulasan Dari Perspektif Viktimologi," *Isu-Isu Kontemporer Dalam Hukum Pidana* 1, no. November 2024 (2025): 107–28, <https://doi.org/10.20885/CICL.vol1.iss2.art1> Deepfake:

Law on Electronic Information and Transactions and the Personal Data Protection Law.⁴⁵ Consequently, preventive efforts have not been fully capable of addressing the evolving complexity of deepfake technology.⁴⁶

Preventive protection should not be limited to law enforcement after a crime has occurred, but should also include policies that encourage the supervision and regulation of technology. In this regard, the responsibility of electronic system operators and digital platforms becomes a key element in the framework of victim protection. Without clear legal obligations for digital platforms to detect, verify, and remove deepfake pornographic content, victims remain at risk of repeated victimization.⁴⁷ The lack of regulation concerning the accountability of digital platforms indicates a regulatory gap in preventive protection, which indirectly increases the risk of harm to victims.⁴⁸

On the other hand, repressive legal protection for victims of deepfake pornography in Indonesia is, in principle, available through criminal, civil, and administrative legal mechanisms. From a criminal law perspective, perpetrators may be held accountable under the Pornography Law, the ITE Law, and the Personal Data Protection Law, provided that their actions fulfill the elements of criminal offenses stipulated in those regulations.⁴⁹ However, the repressive approach through criminal law tends to focus on punishing perpetrators and has not yet positioned victim recovery as the primary objective of law enforcement.⁵⁰

The lengthy and complex criminal justice process often results in revictimization. Victims are compelled to recall and recount their traumatic experiences, while the circulation of harmful content in the digital space continues throughout the legal process. This condition reflects structural and procedural limitations within the criminal justice

⁴⁵ Christella Madalaine, "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi Madalaine Christella Seveney 1 , Demas Brian Wicaksono 2 , Irwan Kurniawan Soetijono 3."

⁴⁶ Ema Nurkhaerani Happy Sturaya Quratuainniza, "Regulasi Kecerdasan Buatan Untuk Mengatasi Penyalahgunaan Deepfake Di Indonesia Fakultas Hukum , Universitas Pembangunan Nasional ' Veteran ' Jakarta Melakukan Tindakan Kejahatan Maupun Sebagai Objek Dari Kejahatan Tersebut .," *ALADALAH : Jurnal Politik, Sosial, Hukum Dan Humaniora* 4, no. 1 (n.d.).

⁴⁷ Happy Sturaya Quratuainniza.

⁴⁸ Christella Madalaine, "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi Madalaine Christella Seveney 1 , Demas Brian Wicaksono 2 , Irwan Kurniawan Soetijono 3."

⁴⁹ Hayya Zafna Haefani, "Urgensi Reformasi Hukum Pidana Indonesia Dalam Menjerat Pelaku Deepfake Pornografi Berbasis Artificial Intelligence Pornografi Telah Menjadi Masalah Yang Cukup Mengkhawatirkan Di Kalangan Penegakan Hukum Terhadap Penyalahgunaan AI Dalam Kasus Kendala , Te," *Jurnal Politik, Sosial, Humaniora* 3 (2025): 12–26, <https://doi.org/10.59246/aladalah.v2i4>.

⁵⁰ Wahyu Handoko, "Digital Crime In The Era Of Society 5.0: Juridical Analysis Of Cyber And Victim Protection," *Ipsa Jure Journal* 2 (2025): 25–38, <https://doi.org/10.62872/arpt6m43>.

system, which has not yet fully accommodated the needs and vulnerabilities of victims of technology-based crimes.⁵¹ Therefore, legal protection that relies solely on the punishment of perpetrators is insufficient to ensure justice for victims of deepfake pornography.

In terms of victim recovery, civil law provides an alternative legal avenue that is more oriented toward the interests of victims. Through tort claims, victims may seek compensation for immaterial damages, such as reputational harm, psychological suffering, and the loss of a sense of security in the public sphere.⁵² Nevertheless, the effectiveness of civil remedies still faces challenges, particularly in proving damages and ensuring victims' access to justice.

In addition, administrative legal protection plays a crucial role in minimizing the ongoing harm experienced by victims. Measures such as blocking access to and removing deepfake pornographic content are strategic steps to prevent further dissemination and reduce victim suffering. Content takedown mechanisms can be regarded as one of the most responsive forms of protection, although their effectiveness largely depends on the commitment of the state and digital platforms in their implementation.⁵³ Therefore, administrative protection should be positioned as an integral component of the victim protection system.

The protection of victims of deepfake pornography must also be viewed from a human rights perspective. The state has a constitutional obligation to safeguard the rights to dignity, privacy, and security of every citizen. The Law on Sexual Violence Crimes provides a normative foundation for fulfilling victims' rights, including restitution and psychological rehabilitation as part of recovery efforts.⁵⁴ This approach emphasizes that victims must be treated as legal subjects with the right to recovery, rather than merely as instruments of evidence in criminal proceedings.

Accordingly, legal protection for victims of AI-based deepfake pornography must be implemented in a comprehensive, integrated, and victim-oriented manner. Such

⁵¹ Putri Ramadhani Rangkuti, Rahma Fitri Amelia Hasibuan and Maria Arfah Nasution, Siti Kholizah, Nadilah Andini, "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE : Studi Kasus Di Media Sosial Indonesia Universitas Islam Negeri Sumatera Utara Medan, Indonesia."

⁵² Tri Anugrah Rizki Syaiful Badri, Pristika Handayani, "Ganti Rugi Terhadap Perbuatan Melawan Hukum Dan Wanprestasi Dalam Sistem Hukum Perdata Compensation for Acts Against the Law and Default in the Civil Law System Penelitian Ini Berfokus Pada Bagaimana Ketentuan Ganti Rugi Atas Pelanggaran Hukum Diterapkan," *Jurnal USM Law Review* 7, no. 2 (2024): 6–7.

⁵³ Indah Rohmawati, Amir Junaedi, "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)."

⁵⁴ Nurini Aprilianda, "Reconstruction Of Restitution As An Additional Punishment For Victims Of Criminal Acts," *Arena Hukum* 17, no. 2 (2024): 226–41.

protection should not only involve criminal law enforcement but also the strengthening of civil and administrative mechanisms, as well as preventive policies that are adaptive to technological developments. Without a systematic and victim-oriented legal protection framework, victims of deepfake pornography will remain in a vulnerable position and continue to face the risk of repeated harm in the digital space.

3. Legal Implications of Deepfake Pornography on the Protection of Human Rights

The use of deepfake technology in the production of pornographic content carries serious legal implications for the protection of human rights, particularly in the context of digital society.⁵⁵ Deepfake pornography constitutes a form of visual identity manipulation that not only misleads the public but also directly undermines the personal integrity of victims through the creation of false representations without consent.⁵⁶ From a human rights perspective, this practice reflects a new form of violation arising from the misuse of Artificial Intelligence that has not yet been fully anticipated by conventional legal frameworks, particularly in relation to the protection of human dignity in digital spaces.⁵⁷

One of the primary legal implications of deepfake pornography is the violation of the right to privacy. A person's face and visual image form part of their personal identity, carrying significant legal and moral value. The use of such biometric data without consent, especially in a pornographic context, contradicts the principles of personal data protection, which place consent as the foundation for the lawful processing of data. The right to privacy, as a fundamental human right, is recognized in both international and national human rights instruments; therefore, deepfake pornography may be regarded as a serious violation of this right. Within the Indonesian legal framework, this practice reflects weak oversight in the use of personal data in digital spaces, despite its normative regulation under the Personal Data Protection Law.⁵⁸

Another implication relates to the violation of the right to honor and reputation. Technologically manipulated pornographic content creates a false public perception that the victim is genuinely involved in the depicted sexual activity.⁵⁹ The effects of this false

⁵⁵ Puja Aisyah Ayu Lestari Adzro Aqilah Wiguna, "Perlindungan Hukum Terhadap Perempuan Korban Deepfake Pornography Di Indonesia," *Jurnal Kajian Hukum Dan Kebijakan Publik* 3, no. 1 (2025): 198–205.

⁵⁶ Doni Noviantama, "Deepfake : Sebuah Ulasan Dari Perspektif Viktimologi."

⁵⁷ Christella Madalaine, "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi Madalaine Christella Seveney 1 , Demas Brian Wicaksono 2 , Irwan Kurniawan Soetijono 3."

⁵⁸ Rafi Satrya Arvitto, "Implikasi Hukum Deepfake : Telaah Terhadap UU ITE Dan UU PDP."

⁵⁹ Kayus Kayowuan Lewoleba Mira Aurelita, "PORNOGRAFI DALAM PERSPEKTIF VIKTIMOLOGI Mira Aurelita , Fakultas Hukum Universitas Pembangunan Nasional Veteran," *Jurnal Kertha Semaya* 12, no. 12 (2024): 3382–96, <https://doi.org/10.24843/KS.2024.v12.i12.p19>.

construction are not temporary, as digital footprints are inherently difficult to erase completely. Victims may suffer long-term reputational damage, social stigma, and ongoing psychological distress. From a human rights perspective, deepfake pornography can be classified as a form of technology-based defamation with a greater destructive impact than conventional defamation, as it involves fabricated visual representations that are difficult to refute.⁶⁰

From the perspective of protecting vulnerable groups, deepfake pornography has significant implications for non-physical sexual violence in digital spaces.⁶¹ This crime often targets women as primary victims and reinforces unequal power relations within digital society. The misuse of AI-based visual technology expands forms of sexual violence that may not be fully captured by conventional criminal categories, yet it produces tangible harm to victims' sense of security and dignity. Therefore, deepfake pornography can be positioned as a form of online gender-based violence, requiring a progressive and victim-oriented legal approach.⁶²

The legal implications of deepfake pornography are also closely linked to the responsibility of the state in protecting human rights in the digital era. Within the framework of the obligation to respect, protect, and fulfill human rights—including the rights to privacy, honor, and security in digital spaces—the state is not only required to prosecute perpetrators after crimes occur, but must also ensure preventive measures, oversight of technological use, and effective recovery mechanisms for victims. The absence of specific regulations on deepfake pornography indicates that the national legal response remains lagging behind the rapid development of Artificial Intelligence technology. As a result, victims are often placed in a legally disadvantaged position.⁶³

The delay of the state in establishing an adaptive legal framework risks producing systematic and recurring human rights violations.⁶⁴ Therefore, the legal implications of deepfake pornography for human rights protection underscore the urgent need for a

⁶⁰ Sarah Amanda Uly Sijabat, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik."

⁶¹ Rebecca dkk., "JURNAL ILMIAH DUNIA HUKUM Environmental Crime Enforcement in Indonesia : Ultimatum and Primum Remedium Perspectives" 10, no. 1 (2025): 242–60, <https://doi.org/10.35973/jidh.v10i1.6579.1>.

⁶² Cleophila Natania Putri Hernawan, "Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intelligence Dalam Tindak Pidana Kekerasan Seksual."

⁶³ Abhishek Gupta, "Menghadapi Dilema Teknologi Dan Hukum Dalam Eksploitasi Selebritas Yang Tidak Sah Informasi."

⁶⁴ Made Wira Yudha Raihani Latifatunnisa, "Urgensi Pembaruan Regulasi Dalam Menanggulangi Penyalahgunaan Teknologi," *Jurnal Hukum Dan Kewarganegaraan* 11, no. 1 (2025), <https://doi.org/10.8734/CAUSA.v1i2.3>.

reformulation of legal policies that are responsive to technological developments. Legal protection should not be solely focused on the punishment of perpetrators, but must also guarantee the restoration of dignity, the protection of privacy, and the sense of security of victims in digital spaces. Without strengthening a human rights-based legal framework and adopting a victim-oriented approach, deepfake pornography will continue to evolve as a serious threat to human rights protection in the digital era.

CONCLUSION

Deepfake pornography constitutes a form of digital crime that manifests through the manipulation of an individual's visual identity without consent into pornographic content. The rapid development of this technology has created a normative gap (legal vacuum) within Indonesian positive law, as no specific regulation currently governs the phenomenon of deepfake pornography. This study offers a theoretical contribution by asserting that deepfake pornography is not merely a violation of decency norms or the dissemination of harmful content, but rather a form of digital identity violation and technology-based violence. It encompasses broader dimensions of harm to personal rights and heightened victim vulnerability in digital spaces beyond what is traditionally recognized in conventional legal studies. The novelty of this research lies in its emphasis that deepfake pornography targets the legal relationship structure between individuals as legal subjects and predictive AI algorithms, thereby generating implications that extend beyond ordinary content violations, including challenges in digital evidence, cross-jurisdictional perpetrator tracing, and significant psychosocial impacts on victims.

From a practical perspective, this study demonstrates that reliance on general legal instruments—such as the Law on Electronic Information and Transactions, the Pornography Law, and the Personal Data Protection Law—remains insufficient to effectively prosecute perpetrators of deepfake pornography. This is primarily because these regulations do not explicitly capture the technological characteristics of Artificial Intelligence or the manipulation of others' data with clear legal consequences. These findings are consistent with prior research indicating that existing regulations generally contain broad prohibitions on immoral electronic content or unauthorized use of personal data, yet fail to specifically anticipate the modus operandi of deepfake technology, which involves machine learning and adversarial networks to produce hyper-realistic visual content.

The policy implications of this study highlight the necessity of establishing specific regulations on deepfake pornography to bridge the normative gap in law enforcement and victim protection. Such regulation should explicitly define the elements of deepfake

pornography offenses in accordance with the characteristics of AI-based technology, including the unauthorized use of biometric data. The proposed regulatory framework should be designed based on several key principles: a victim-oriented approach, which prioritizes the restoration of dignity, access to rapid content takedown mechanisms, and restitution as central components of the legal system; a technology-adaptive approach, requiring electronic system operators and digital platforms to proactively detect, verify, and remove deepfake pornographic content; and a human rights-based approach, strengthening the normative foundation of the rights to privacy, honor, and personal security.

This integrative policy approach not only expands the scope of criminal and civil law enforcement but also necessitates harmonization with administrative frameworks and robust digital forensic procedures to ensure legal certainty, efficient case handling, and the prevention of future misuse of deepfake technology. Through legal reform that is responsive to the development of Artificial Intelligence and the explicit recognition of deepfake pornography as a distinct criminal offense, the Indonesian legal system can more effectively prosecute perpetrators, provide equitable protection for victims, and anticipate the broader impacts of the continued evolution of AI-based technologies.

REFERENCES

- Abhishek Gupta, Mayur Shrestha. "Menghadapi Dilema Teknologi Dan Hukum Dalam Eksploitasi Selebritas Yang Tidak Sah Informasi." *Jurnal Tren Baru Dan Penelitian Baru* 2, no. 12 (2024): 372–80.
- Adzro Aqilah Wiguna, Puja Aisyah Ayu Lestari. "Perlindungan Hukum Terhadap Perempuan Korban Deepfake Pornography Di Indonesia." *Jurnal Kajian Hukum Dan Kebijakan Publik* 3, no. 1 (2025): 198–205.
- Agestya Petra Amelia, Izzaty Nagita Putri, Jonathan Raymond Frederick. "Konstruksi Identitas Sosial Oleh Media Sosial : Studi Kritis Berdasarkan Pemikiran Marcuse Dan Habermas." *Jurnal Perspektif* 8, no. 3 (2025): 363–69. <https://doi.org/10.24036/perspektif.v8i3.1258>.
- Carlos Varela Enríquez, Renato Toasa and Maryory Urdaneta. "The Use of Artificial Intelligence in Cybercrime: Impact Analysis in Ecuador and Mitigation Strategies." *Journal of Cybersecurity and Privacy*, 2025. <https://doi.org/10.3390/jcp5040100>.
- Christella Madalaine. "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi Madalaine Christella Seveney 1 , Demas Brian Wicaksono 2 , Irwan Kurniawan Soetijono 3." *Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31, no. 2 (2025): 97–106.

<https://ojs.stihpada.ac.id/index.php/disiplin>.

Cindy Natalia. "Perlindungan Hukum Bagi Korban Pornografi Deepfake Dalam Konteks Hukum Indonesia." *Jurnal Kertha Desa* 12, no. 19 (2024).

Cleophila Natania Putri Hernawan. "Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intelligence Dalam Tindak Pidana Kekerasan Seksual." *Lex Privatum Jurnal Fakultas Hukum Unsrat* 15, no. 4 (2025).

Doni Noviantama, Alif Alfani Rahman. "Deepfake : Sebuah Ulasan Dari Perspektif Viktimologi." *Isu-Isu Kontemporer Dalam Hukum Pidana* 1, no. November 2024 (2025): 107–28. <https://doi.org/10.20885/CICL.vol1.iss2.art1> Deepfake:

Dr. Drs. H. Rifa'i Abubakar, M.A. *Pengantar Metodologi Penelitian*. UIN Sunan Kalijaga, 2021.

Dr. H. Nur Solikin, S.Ag., MH. *Pengantar Metodologi Penelitian Hukum*, 2021.

Elvan Maulana Rif'at, Timbul Dompok. "Hak Asasi Manusia Di Era Digital : Tantangan Dan Peluang Dalam Mengatasi Kejahatan Siber." *Jurnal Ilmu Multidisiplin* 3, no. 1 (2025).

Firdausi, Anita. "Tinjauan Etis Dan Hukum Terhadap Perlindungan Data Pribadi Di Tengah Maraknya Konten Deepfake Di Media Sosial." *Jurnal Hukum Dan Kewarganegaraan* 12, no. 5 (2025). <https://doi.org/10.3783/causa.v2i9.2461>.

Gunawan Hadi Purwanto. "Penetapan Putusan Pengadilan Negeri Surabaya Tentang Perkawinan Beda Agama Dalam Perspektif Hukum Positif." *Binamulia Hukum* 12, no. 1 (2023): 253–62. <https://doi.org/10.37893/jbh.v12i2.425>.

Halomoan Freddy Sitinjak Alexandra. "Pemberian Restitusi Dan Kompensasi Bagi Korban Tindak Pidana Berdasarkan Nilai Keadilan." *Jurnal Pendidikan Dan Konseling* 4, no. 5 (2022): 5975–84.

Happy Sturaya Quratuainniza, Ema Nurkhaerani. "Regulasi Kecerdasan Buatan Untuk Mengatasi Penyalahgunaan Deepfake Di Indonesia Fakultas Hukum , Universitas Pembangunan Nasional ' Veteran ' Jakarta Melakukan Tindakan Kejahatan Maupun Sebagai Objek Dari Kejahatan Tersebut ." *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 4, no. 1 (n.d.).

Hayya Zafna Haefani. "Urgensi Reformasi Hukum Pidana Indonesia Dalam Menjerat Pelaku Deepfake Pornografi Berbasis Artificial Intelligence Pornografi Telah Menjadi Masalah Yang Cukup Mengkhawatirkan Di Kalangan Penegakan Hukum Terhadap Penyalahgunaan AI Dalam Kasus Kendala , Te." *Jurnal Politik, Sosial, Humaniora* 3 (2025): 12–26. <https://doi.org/10.59246/aladalah.v2i4>.

Hendra Prayoga. "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia." *Abdurrauf Law and Sharia* 1, no. 2 (2024): 22–38. <https://doi.org/10.70742/arlash.v2i1.194>.

Indah Rohmawati , Amir Junaidi, Ariy Khaerudin. "Urgensi Regulasi Penyalahgunaan

- Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO).” *Journal Of Social Science Research* 4 (2024): 1779–94. <https://j-innovative.org/index.php/Innovative%0AUrgensi>.
- Ivana Dewi Kasita. “Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGB0) Di Era Pandemi Covid-19.” *Jurnal Wanita Dan Keluarga* 3, no. 1 (2022): 16–26. <https://doi.org/10.22146/jwk.5202>.
- Ivana Trixie, Moody Risky Syailendra Putra. “Studi Perbandingan: Perlindungan Hukum Terhadap Deepfake Berbasis Kecerdasan Buatan (Ai).” *Jurnal Pendidikan Sejarah Dan Riset Sosial Humaniora (KAGANGA)* 8, no. 6 (2025). <https://doi.org/10.31539/gm8q1a03>.
- Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, Muhammad Fadly Nasution. “Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana Di Indonesia.” *Jurnal Minfo Polgan Volume* 14, no. 1 (2025).
- Juandry Aruan. “Legal Protection for Victims of Photo Abuse through Artificial Intelligence Technology in Pornography Crimes in Indonesia.” *Law & Society Review* 5, no. 2 (2025): 1831–62. <https://doi.org/10.15294/lsr.v5i2.3834>.
- Mahrus Ali, Zico Junius Fernando, Chairul Huda, Mahmutarom. “Deepfake Dan Viktimologi : Menjelajahi Dampak Manipulasi Digital Terhadap Korban.” *Jurnal Hukum Internasional Keadilan Substantif* 8, no. 1 (2025): 1–12. <https://doi.org/10.56087/substantivejustice.v8i1.306>.
- Memei Apriana, Fransisco, Any Nugroho. “Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (Ai) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual.” *Jurnal Sosial Dan Ekonomi* 3(2), no. 1 (2021): 123–38. [https://idm.or.id/JSER/index.php/JSER Open](https://idm.or.id/JSER/index.php/JSER%20Open).
- Mira Aurelita, Kayus Kayowuan Lewoleba. “PORNOGRAFI DALAM PERSPEKTIF VIKTIMOLOGI Mira Aurelita , Fakultas Hukum Universitas Pembangunan Nasional Veteran.” *Jurnal Kertha Semaya* 12, no. 12 (2024): 3382–96. <https://doi.org/10.24843/KS.2024.v12.i12.p19>.
- Muhammad Afif. “Tindak Pidana Deepfake Pornography Di Indonesia : Analisis Yuridis Terhadap Kekosongan Norma Dalam KUHP Dan UU ITE.” *Jurnal Ilmiah Multidisiplin* 3, no. 2 (2025): 27–35. <https://doi.org/10.62017/merdeka>.
- Naufal Zuhdi, Heni Siswanto, Dona Raisa Monica. “Peran Kepolisian Terhadap Ancaman Kejahatan Pelecehan Seksual Melalui Modus Deepfake Porn Di Era Digital.” *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial Dan Politik* 2, no. April (2025). <https://doi.org/10.62383/demokrasi.v2i2.856>.
- Nurini Aprilianda. “Reconstruction Of Restitution As An Additional Punishment For Victims Of Criminal Acts.” *Arena Hukum* 17, no. 2 (2024): 226–41.

- Olivia Novera, Yenny Fitri Z. "Analisis Pengaturan Hukum Pidana Terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) Dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial." *Jurnal Pemikiran Hukum Dan Hukum Islam* 10, no. 2 (2024): 460-74. <https://ejournal.iaifa.ac.id/index.php/faqih>.
- Putri Ramadhani Rangkuti, Rahma Fitri Amelia Hasibuan, Vressilia Witama, and Siti salmiah Maria Arfah Nasution, Siti Kholizah, Nadilah Andini. "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE : Studi Kasus Di Media Sosial Indonesia Universitas Islam Negeri Sumatera Utara Medan, Indonesia." *Jurnal Publikasi Ilmu Hukum* 3 (2025).
- Rafi Satrya Arvitto. "Implikasi Hukum Deepfake : Telaah Terhadap UU ITE Dan UU PDP." *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 4, no. 2 (2025): 73-82. <https://doi.org/10.35912/jihham.v4i2.3937>.
- Raihani Latifatunnisa, Made Wira Yudha. "Urgensi Pembaruan Regulasi Dalam Menanggulangi Penyalahgunaan Teknologi." *Jurnal Hukum Dan Kewarganegaraan* 11, no. 1 (2025). <https://doi.org/10.8734/CAUSA.v1i2.3>.
- Rebecca dkk. "Jurnal Ilmiah Dunia Hukum Environmental Crime Enforcement in Indonesia : Ultimatum and Primum Remedium Perspectives" 10, no. 1 (2025): 242-60. <https://doi.org/10.35973/jidh.v10i1.6579.1>.
- Respati, Adnasohn Aqilla, Astri Dewi Setyarini, Dodi Parlagutan, and Muhammad Rafli. "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban." *Media Hukum Indonesia* 2, no. 2 (2024): 586-93. <https://doi.org/10.5281/zenodo.12508126>.
- Sarah Amanda Uly Sijabat, Diana Lukitasari. "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik." *Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 13, no. 2 (2024): 179-94.
- Silvia Maharani. "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum." *Jurnal Hukum Legalita* 6 (2023): 83-90. <https://doi.org/10.47637/legalita.v6i2.1453> Kriminalisasi.
- Syaiful Badri, Pristika Handayani, Tri Anugrah Rizki. "Ganti Rugi Terhadap Perbuatan Melawan Hukum Dan Wanprestasi Dalam Sistem Hukum Perdata Compensation for Acts Against the Law and Default in the Civil Law System Penelitian Ini Berfokus Pada Bagaimana Ketentuan Ganti Rugi Atas Pelanggaran Hukum Diterapkan." *Jurnal USM Law Review* 7, no. 2 (2024): 6-7.
- Wahyu Handoko. "Digital Crime In The Era Of Society 5.0: Juridical Analysis Of Cyber And Victim Protection." *Ipsa Jure Journal* 2 (2025): 25-38. <https://doi.org/10.62872/arpt6m43>.
- Will Hawkins, Chris Russell, Brent Mittelstandt. *Deepfakes on Demand : The Rise of Accessible Non-Consensual Deepfake Image Generators. Proceedings of (FAccT '25)*. Vol.

1. Association for Computing Machinery, 2023.

Zahra Pitaloka Islami. "Tantangan Penegakan Hukum Di Era Globalisasi Digital : Strategi Menghadapi Kejahatan Siber Lintas Batas." *Jurnal Sains Ekonomi Dan Edukasi* 2, no. 12 (2025): 2579–91.

Zevanya Praja Syaharani. "Dari Fantasi Digital Ke Kekerasan Nyata Analisis Hukum Atas Kasus Deepfake Pornografi Dan Tanggung Jawab Negara." *Maleo Law Journal* 9, no. 2 (2025).