

Reconstructing Legal Protection for Victims of Deepfake Abuse through a Victim-Oriented Justice Approach

Mohammad Arief Widyanto¹, Risky Waldo², Tubagus Ahmad Ramadan³

^{1,2,3} Universitas Pamulang

 [10.32502/khk.v8i1.11483](https://doi.org/10.32502/khk.v8i1.11483)

Abstract

The rapid advancement of artificial intelligence has given rise to deepfake technology, which employs deep learning through Generative Adversarial Networks (GANs) to realistically manipulate audio-visual content without the subject's consent. Misuse of this technology inflicts multiple layers of harm on victims, including violations of honor and privacy, alongside prolonged psychological trauma. Indonesia's existing regulations, namely the ITE Law No. 1 of 2024 and the PDP Law No. 27 of 2022, have not explicitly defined deepfakes as an independent criminal offense, creating a legal vacuum (rechtsvacuum) that leaves victims vulnerable to further harm. This research employs a normative legal method, using legislative, conceptual, and comparative approaches. The findings reveal that both regulations remain reactive and inadequate to address the complexity of AI-based digital identity manipulation. In response, a victim-oriented justice approach is proposed as a paradigm for legal reconstruction, positioning victims as the central subject of recovery. The proposed ideal reconstruction consists of three layers of protection: preventive, through the establishment of lex specialis regulation; repressive, through mandatory restitution; and rehabilitative, through guarantees of the right to be forgotten and psychological recovery. This study concludes that comprehensive special legislation oriented toward fulfilling victims' rights in digital crimes is urgently needed.

Keywords: Deepfake; Legal Protection; Victim-Oriented Justice; Legal vacuum; Legal Reconstruction

Abstrak

Kemajuan pesat kecerdasan buatan melahirkan teknologi deepfake yang memanfaatkan algoritma deep learning melalui Generative Adversarial Network (GAN) untuk memanipulasi konten audio-visual secara realistis tanpa persetujuan subjeknya. Penyalahgunaan teknologi ini menimbulkan kerugian berlapis bagi korban, mencakup pelanggaran kehormatan, privasi, hingga trauma psikologis berkepanjangan. Regulasi Indonesia yang berlaku, yakni UU ITE No. 1 Tahun 2024 dan UU PDP No. 27 Tahun 2022, belum secara tegas mendefinisikan deepfake sebagai tindak pidana mandiri, sehingga menciptakan rechtsvacuum yang berujung pada reviktimisasi korban. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan. Hasil kajian menunjukkan bahwa kedua regulasi tersebut masih bersifat reaktif dan tidak memadai menjangkau kompleksitas manipulasi identitas digital berbasis kecerdasan buatan. Pendekatan victim-oriented justice ditawarkan sebagai paradigma rekonstruksi hukum yang menempatkan korban sebagai subjek utama pemulihan. Rekonstruksi ideal mencakup tiga lapisan perlindungan, yaitu preventif melalui regulasi lex specialis, represif melalui restitusi wajib, serta rehabilitatif melalui jaminan right to be forgotten dan pemulihan psikologis. Simpulan penelitian ini menegaskan perlunya legislasi khusus yang komprehensif dan berorientasi pada pemenuhan hak korban kejahatan digital.

Kata Kunci: Deepfake; Perlindungan Hukum; Victim-Oriented Justice; Rechtsvacuum; Rekonstruksi Hukum

Info Artikel

Masuk: 10 Januari 2026, Diterima: 12 April 2026, Terbit: 30 Juni 2026



Email Corresponding Author:

Nama Author : dosen02295@unpam.ac.id

INTRODUCTION

The rapid development of artificial intelligence has given birth to various digital innovations that have helped create the threat of technology-based crime that is increasingly complex and difficult to reach by conventional legal frameworks. One of its manifestations is *deepfake technology*, which is

digital media engineering that utilizes deep learning algorithms through artificial neural networks such as *Generative Adversarial Network* (GAN) to produce audio-visual content that is realistically difficult to distinguish from the original content. The increasingly open accessibility of this technology, including through free software, allows anyone to produce manipulative content without the need for special technical expertise, so the potential for its abuse of individuals as victims becomes a real and urgent threat.¹

The abuse of *deepfakes* causes multidimensional losses for victims, ranging from violations of the rights to self-image, honor, privacy, to long-term psychological impacts in the form of trauma, anxiety, and *post-traumatic stress disorder* (PTSD). Research shows that a *victim-centered* approach is a more effective instrument in dealing with the impact of *deepfake* pornography than legal mechanisms that focus solely on punishing the perpetrator, because victim recovery requires psychological, social, and juridical interventions at the same time.² In Indonesia, the legal framework that has been in force to date has not explicitly regulated the misuse of *deepfake* technology as a stand-alone criminal act. Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) only provides general articles related to honor, defamation, and manipulation of electronic information, so its application to *deepfake* cases is still interpretive and does not provide adequate legal certainty for victims.

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as a complementary regulation also contains substantial limitations in reaching the dimensions of artificial intelligence-based digital identity manipulation. Although the PDP Act prohibits the unlawful use of personal data and criminalizes the falsification of personal information, this regulation

¹ Michelle Azhari Iradat and Diah Ratna Sari Hariyanto, "The Urgency of Criminal Regulation of Deepfake Abuse: An Examination of Victim Protection Aspects in National Law," *ACADEMIC MEDIA JOURNAL* (JMA) 3, no. 12 (2025).

² Chiquita Thefirstly Noerman and Aji Lukman Ibrahim, "Criminalization of Deepfakes in Indonesia as a Form of State Protection can actually provide convenience in doing anything. Artificial Intelligence" 7, no. 2 (2024): 1–4.

has not accommodated the specific characteristics of *deepfakes* involving the biometric synthesis of faces and voices without the consent of the owner. This condition creates a *rechtsvacuum* or a vacuum of norms that is a systemic obstacle in the law enforcement process against this technology-based crime.³

The absence of regulations that are specifically oriented to victim protection has an impact on revitalization, which is a condition in which victims not only experience suffering due to *the deepfake* crime itself, but also face social stigma and obstacles in accessing justice due to legal uncertainty. The study from a victimological perspective confirms that the unique characteristics of *deepfake* crimes, which include easily deleted digital evidence, perpetrators operating anonymously, and content that can spread virally, demand the development of a justice system that is responsive to the needs and rights of victims across the board.⁴

The reconstruction of legal protection through a *victim-oriented justice* approach is inevitable in the context of Indonesia's national law reform. This approach prioritizes three complementary layers of protection, namely preventive protection through explicit prohibitions and content *takedown* mechanisms, repressive protection in the form of criminal sanctions and restitution for perpetrators, and rehabilitative protection that guarantees victims' access to psychological recovery and *the right to be forgotten*. Without a comprehensive normative reconstruction, Indonesia's legal system risks continuing to be reactive and unable to provide proportionate protection for victims of *deepfake abuse*.⁵

Based on the above background description, this study formulates three main questions that are the focus of the study. First, what are the conditions

³ Hendra Prayoga, "The Spread of Deepfake Content as a Criminal Offense: A Critical Analysis of Law Enforcement and Public Protection in Indonesia" 1, no. 2 (2024): 22–38.

⁴ Angelica Vanessa Audrey Nasution and Anggita Doramia Lumbanraja, "From Trauma to Recovery: How Victim-Centered Approaches Can Combat Deepfake Pornography.," *Pakistan Journal of Life & Social Sciences* 22, no. 2 (2024).

⁵ Komang Bagus Wicaksana Putra, "The Urgency of Regulating Deepfake Pornography Crimes in Indonesia" 13, no. 10 (2024), <https://doi.org/10.1016/j.cviu.2022.103525.1>.

and weaknesses of Indonesia's positive legal framework, especially the ITE Law (Law No. 1 of 2024) and the PDP Law (Law No. 27 of 2022), in providing legal protection for victims of *deepfake* abuse today? Second, why is the *victim-oriented justice* approach relevant and needed as a paradigm for reconstructing legal protection for *deepfake* victims in Indonesia? Third, how is the reconstruction of the ideal legal protection for victims of *deepfake* abuse that reflects a *victim-oriented justice approach* in the Indonesian national legal system?

This study aims to critically analyze the weaknesses and gaps in the Indonesian positive legal framework related to the protection of victims of *deepfake* abuse, focusing on the ITE Law and the PDP Law as the most relevant but inadequate regulations. In addition, this study aims to examine and argue the urgency and relevance of the *victim-oriented justice* approach as a paradigm that should be the basis for legal reform in dealing with artificial intelligence-based crimes. Furthermore, this study aims to formulate a comprehensive legal protection reconstruction model, oriented towards the restoration of victims' rights, and can be implemented in the Indonesian national legal system.

Theoretically, this research is expected to make an academic contribution to the development of criminal law, especially in the field of cyber law and technology, by offering a conceptual framework of *victim-oriented justice* as a new perspective in analyzing and responding to *multidimensional deepfake* crimes. Practically, the results of this study are expected to be a reference for policymakers, especially the House of Representatives and the government, in formulating *lex specialis* regulations that explicitly regulate the abuse of *deepfakes* while ensuring comprehensive protection and recovery of victims. For the wider community, this research is useful to increase legal awareness about the dangers of misusing *deepfake technology* and the rights of victims who should receive full protection from the state in the era of digitalization that continues to grow rapidly.

METHODS

This research uses a *normative legal research* method, which is a research model that places law as a rule or written norm that is the main object of study. In this framework, law is conceptualized not as a social phenomenon that is empirically observed, but as a set of rules that are analyzed systematically, logically, and scientifically in order to produce a prescription for the legal problems at hand. As emphasized, normative legal research is basically an intellectual activity to find relevant legal rules, legal principles, and legal doctrines in order to answer the legal issues under study, with an analysis process that relies entirely on *library research* as the main source. The choice of this method is considered the most appropriate considering that the focus of this study is to identify the norm void (*rechtvacuum*) in Indonesia's positive regulations related to the protection of victims of *deepfake* abuse, which is actually a normative issue that requires in-depth textual and doctrinal analysis.⁶

This study applies three approaches simultaneously, namely the statute *approach*, the conceptual *approach*, and the *comparative approach*. His study on the criminalization of *deepfakes* in Indonesia applies a combination of three similar approaches, and concludes that normative methods with a variety of approaches are able to comprehensively reveal the normative, conceptual, and comparative dimensions of a legal issue that does not yet have explicit regulations. The legislative approach in this study is focused on the review of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as the main applicable positive legal framework. A conceptual approach is used to examine the doctrine of *victim-oriented justice* as a victim protection paradigm. The comparative approach is applied to refer to the regulations of other jurisdictions that are more progressive in regulating the misuse of *deepfake technology*.

⁶ Irwansyah, "Legal Research: Choice of Methods and Practices for Article Writing (Revised Edition)," 2021.

The sources of legal materials used in this study are divided into three categories. Primary legal materials include applicable laws and regulations, especially the ITE Law and the PDP Law. Secondary legal materials include scientific journals, legal articles, and previous research results relevant to the topic of study. Tertiary legal materials consist of legal dictionaries and encyclopedias that serve as explanations of technical terms. In normative legal research that examines technology-based crimes, the combination of these three layers of legal material is inevitable so that the resulting analysis is not only doctrinally valid, but also responsive to the dynamics of technological developments that go beyond the speed of adaptation of positive legal norms. All legal materials collected are then analyzed qualitatively-prescriptively, namely by providing law-based arguments and recommendations on the issues studied, so that this research not only describes the condition of existing norms, but also offers a reconstruction of a legal protection framework that is more oriented to the interests of the victim.

RESULT AND DISCUSSION

1. Conditions and Weaknesses of Indonesia's Positive Legal Framework in Protecting Deepfake Victims

Artificial intelligence-based *deepfake technology* has developed into a serious threat to the fundamental rights of individuals, especially the right to honor, privacy, and the protection of biometric data. In principle, this technology utilizes *deep learning* algorithms through the *Generative Adversarial Network* (GAN) to generate synthetic audio-visual content that is realistically difficult to distinguish from the original content, so that a person's face and voice can be manipulated without his consent for various criminal purposes. Deepfake abuse includes non-consensual pornography, financial fraud, defamation, and the spread of false information that has the potential to permanently damage the reputation and psychological safety of the victim. Indonesia's current positive legal framework does not explicitly define or criminalize *deepfakes* as a stand-alone criminal act, so law enforcement still

relies on generic articles that are not designed to reach the complexities of AI-based digital manipulation.⁷

Law Number 1 of 2024 concerning the Second Amendment to the ITE Law provides a number of articles that can theoretically be used to ensnare *deepfake abusers*.⁸ Article 27A regulates the prohibition of attacking honor or good name through Electronic Information, Article 27 paragraph (1) prohibits the dissemination of content that violates morality, and Article 28 paragraph (1) prohibits the dissemination of misleading information that is detrimental to consumers. However, all of these articles are reactive to the consequences of the act, not to the algorithmic manipulation method that is the core of *deepfake* crimes, so that it does not meet the principle of *lex certa* which requires clarity and firmness in the formulation of delicacies. The applicable regulations are still reactive, do not contain a technical definition of *deepfake*, and do not meet the proportionate functions of preventive and repressive protection, so that law enforcement becomes ineffective and the vulnerability of victims is greater. This condition directly creates a *rechtsvacuum* or a void of norms that has an impact on legal uncertainty for victims who want to demand criminal responsibility for the perpetrator.

On the other hand, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) contributes as a complementary regulation that recognizes face and voice as biometric data that is included in the category of specific personal data based on Article 4 paragraph (2) letter b. Article 65 and Article 66 of the PDP Law prohibit everyone from illegally obtaining, disclosing or falsifying personal data belonging to another person. and Article

⁷ Rizgita Nurul Fauzyah, "Legal Protection for Victims of Crime of Making Fake Pornographic Videos (Deepfake Pom) Based on Artificial Intelligence (AI) in Indonesia," Student Journal of the Faculty of Law, Sheikh-Yusuf Islamic University 3, no. November (2024): 74–88.

⁸ "Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions," No. 190185 (2024).

68 threatens violators with imprisonment of up to six years.⁹ However, the PDP Law has fundamental limitations because it does not regulate accountability mechanisms for developers or users of AI systems that autonomously generate *deepfake* content, so there are significant legal loopholes in determining the responsible parties when perpetrators operate behind complex algorithmic systems. These two regulations, despite being the main legal framework available, have not been substantially able to provide adequate protection and are oriented towards the comprehensive restoration of victims' rights.

2. The Relevance of the Victim-Oriented Justice Approach as a Paradigm for Legal Protection Reconstruction

The inadequacy of the existing legal framework not only has implications for the difficulty of proving and prosecuting, but also results in *victims of deepfakes* experiencing revitalization, namely multi-layered suffering arising not only from the crime itself, but also from their helplessness in accessing justice. In this context, *the victim-oriented justice* approach is the most relevant paradigm as the foundation for the reconstruction of legal protection. This approach places the victim as the primary subject in the justice system, not just a witness or a passively protected party, by ensuring that all legal mechanisms are designed to actively and measurably restore the victim's rights, dignity and psychological well-being. The study of modern victimology confirms that forms of victimization continue to transform with technological developments, and that the scientific community and judicial institutions are required to adapt their theoretical and practical approaches to respond to the increasingly complex dynamics of contemporary crime.¹⁰

⁹ "Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection," no. 016999 (2022).

¹⁰ Muhammad Ilham Alfathoni, "Legal Protection for Victims of Deepfake Pornography in Terms of Criminal Law," *Andalas Law Journal* 9, no. 2 (2024).

The relevance of *victim-oriented justice* in the context of *deepfakes* is even stronger given the unique characteristics of this crime that have a multidimensional impact on victims. Manipulative content that has spread virally in the digital space cannot be completely removed even if the perpetrator has been convicted, so the victim's suffering in the form of psychological trauma, reputational damage, and social stigma continues far beyond the criminal justice process. Research shows that the most effective recovery efforts for *deepfake* victims are not just punishing the perpetrators, but integrated interventions that include psychological assistance, fast and structured content removal mechanisms, and guarantees of *the right to be forgotten* that can be legally enforced on digital platforms.¹¹ The victim protection aspect in the victimology dimension emphasizes that the criminal justice system must evolve from a retributive paradigm to a restorative paradigm centered on holistic victim recovery, as has been the direction of the development of victimology studies since the Second World War to the current digital era.

In addition, *the victim-oriented justice* approach also requires a reformulation of criminal offenses that is adaptive to technological developments and explicitly focuses on victim protection as the main goal of criminalization, not just a deterrent effect for perpetrators. Current regulations, including the ITE Law, the Pornography Law, and the PDP Law, are only preventive and do not provide a significant deterrent effect for AI-based criminals, so that victims do not get real legal certainty.¹² This condition strengthens the argument that the reconstruction of legal protection cannot be done partially through patching existing articles, but must be designed systemically with *victim-oriented justice* as the main paradigm.

¹¹ Andriansyah Kartadinata, "Reconstruction of Criminal Deliques in Deepfake Crimes: Challenges of Proving and Protecting Victims," 2026, 36-48.

¹² Rendi Syaputra, "The Urgency of Legal Protection Arrangements for Deepfake Victims through Artificial Intelligence (AI) from the Perspective of Indonesian Criminal Law," 2024, 5-12.

3. Reconstruction of Ideal Legal Protection for Victims of Deepfakes Based on Victim-Oriented Justice

The ideal reconstruction of legal protections for victims of *deepfake* abuse must be built on three layers of complementary norms and fully oriented towards victim recovery. First, a layer of preventive protection through the establishment of *lex specialis* regulations that explicitly define *deepfakes* as a separate criminal offense with elements of delicacy that are clear, measurable, and meet the principles of *lex certa*. This regulation should require digital platforms to implement a *proactive deepfake* content detection system and a fast takedown *mechanism*, as well as regulate the obligation to *watermark* all content generated by artificial intelligence systems. The absence of concrete rules related to AI-based crime results in more victims falling without legal certainty, while perpetrators continue to operate in gaps in existing norms.¹³ This *lex specialis* regulation must integrate the provisions of the existing ITE Law and the PDP Law while filling the gaps in norms that have not been reached by the two regulations.

Second, a layer of repressive protection that is strengthened with restitution and compensation mechanisms for victims that are compulsorily integrated into criminal sentences. In this framework, *deepfakes* are not only sentenced to prison and fines, but are also required to pay compensation to the victim which includes material, immaterial, and psychological recovery costs. Comprehensive victim protection efforts must include preventive, repressive, restitution, compensation, and counseling protection as an inseparable system.¹⁴ Strengthening this repressive layer must be accompanied by increasing the capacity of law enforcement officials in the field of digital

¹³ Kartika Ardina Raesyah Putri, "Legal Liability For Using Artificial Intelligence To Produce Deepfakes Under Personal Data Protection Law," 2025.

¹⁴ Doni Noviantama, "Deepfake: A Review from The Victimology Perspective" 1, no. May (2025): 107-28.

forensics so that proving elements of error in AI-based crimes can be carried out more effectively and accurately.¹⁵

Third, a layer of rehabilitative protection that ensures victims' access to psychological, social, and juridical recovery on an ongoing basis. This dimension includes *right-to-be forgotten* guarantees that can be imposed on digital platforms, trauma counseling services organized by the state, and legal assistance that ensures victims can access all available recovery mechanisms without bureaucratic barriers.¹⁶ Victim-centered *approaches* in the context of *deepfakes* have proven to be more effective in recovering long-term impacts than approaches that focus solely on punishing perpetrators, as victim recovery requires simultaneous and integrated psychological, social, and juridical interventions.¹⁷ Thus, this reconstruction of *victim-oriented justice-based* legal protection represents a paradigmatic shift that not only answers the demands of technological developments, but also fulfills the country's constitutional obligation to provide full protection for every citizen from the ever-evolving threat of digital crime.¹⁸

CONCLUSION

This study reveals that Indonesia's positive legal framework, especially the ITE Law No. 1 of 2024 and the PDP Law No. 27 of 2022, has not been able to adequately reach the complexity of *deepfake-based* crimes. The absence of an explicit juridical definition of *deepfakes* creates a *rechtsvacuum* that has a direct impact on the victim's victimization. The *victim-oriented*

¹⁵ G M Borges, A Guerreiro, dan M Pina, "Modern Insights and Strategies in Victimology," in *IGI Global, Advances in Criminology, Criminal Justice, and Penology*, 2024, <https://igiprodst.blob.core.windows.net/ancillary-files/8946de73-cc42-47e9-9c0b-2bb6af1039c7.pdf>.

¹⁶ S Walklate, *Advanced Introduction to Victimology*, Elgar Advanced Introductions series (Edward Elgar Publishing Limited, 2023).

¹⁷ Rendi Syaputra, "The Urgency of Legal Protection Arrangements for Deepfake Victims through Artificial Intelligence (AI) from the Perspective of Indonesian Criminal Law," Faculty of Law, Lancang Kuning University, Jalan Yos Sudarso KM 8 Rumbai Pekanbaru, Riau, 2024, 5–12.

¹⁸ Musfala Yudha and Sunardi Purwanda, "Legal Protection for Victims of the Use of Deepfakes in Pomographic Crimes," *INDONESIAN JOURNAL OF LAW AND SHARIAH* 2, no. 1 (2025).

justice paradigm exists as a normative solution that places the victim as the main subject of recovery, not just a passive party in the justice process. Ideal legal reconstruction requires three complementary layers of protection, namely preventive, repressive, and rehabilitative protection, in order to realize proportionate and fair legal certainty for all victims of digital crime.

Policymakers, especially the House of Representatives and the government, need to immediately formulate *lex specialis* regulations that expressly define *deepfake abuse* as an independent criminal offense with elements of decriminality that are measurable according to the principle of *lex certa*. Digital platforms must be involved through the obligation to implement a *deepfake* content detection system along with a *structured takedown* mechanism. In addition, the state needs to guarantee victims' access to psychological recovery services and the legal enforcement of the *right to be forgotten*. Strengthening the capacity of law enforcement officials in the field of digital forensics is also an urgent priority so that law enforcement against crimes based on artificial intelligence can run effectively and accountably.

ACKNOWLEDGMENTS

Intended for those who assist in research, especially those who fund the author's research. Include either individuals or institutions who are advisors, financial supporters or maybe other supporters, namely readers, typists or those who have contributed material and so on.

REFERENCES

- Alfathoni, Muhammad Ilham. "Legal Protection for Victims of Deepfake Pornography in Terms of Criminal Law." *Andalas Law Journal* 9, no. 2 (2024). <https://alj.fhuk.unand.ac.id/index.php/alj/article/view/90>.
- Borges, G M, A Guerreiro, dan M Pina. "Modern Insights and Strategies in Victimology." In *IGI Global. Advances in Criminology, Criminal Justice, and Penology*, 2024. <https://igiprodst.blob.core.windows.net/ancillary-files/8946de73-cc42-47e9-9c0b-2bb6af1039c7.pdf>.
- Fauzyah, Rizgita Nurul. "Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence (Ai) Di Indonesia." *Jurnal Mahasiswa Fakultas*

Hukum Universitas Islam Syekh-Yusuf 3, no. November (2024): 74–88.

- Haida, Rendi Syaputra Nur, dan Eko Nuriyatman. “Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (Ai) Dari Perspektif Hukum Pidana Indonesia.” *Jurnal Hukum Respublica* 24, no. 1 (2024): 5–12. <https://doi.org/10.31849/respublica.v24i01.23327>.
- Iradat, Michelle Azhari, dan Diah Ratna Sari Hariyanto. “Urgensi Pengaturan Pidana Penyalahgunaan Deepfake: Telaah Aspek Perlindungan Korban Dalam Hukum Nasional.” *Jurnal Media Akademik (JMA)* 3, no. 12 (2025). <https://doi.org/10.62281/611cwh46>.
- Irwansyah. “Penelitian Hukum: Pilihan Metode dan Praktik Penulisan Artikel (Edisi Revisi),” 2021.
- Kartadinata, Andriansyah. “Rekonstruksi Delik Pidana dalam Kejahatan Deepfake : Tantangan Pembuktian dan Perlindungan Korban.” *MUARA HUKUM: Jurnal Ilmiah Ilmu Hukum dan Administrasi Publik* 1, no. 1 (2026): 36–48. <https://jurnal.muaraedukasi.id/index.php/muarakum/article/view/203>.
- Komang Bagus Wicaksana Putra. “Urgensi Pengaturan Tindak Pidana Deepfake Pornografi Di Indonesia” 13, no. 10 (2024). <https://doi.org/10.1016/j.cviu.2022.103525.1>.
- Nasution, Angelica Vanessa Audrey, dan Anggita Doramia Lumbanraja. “From Trauma to Recovery: How Victim-Centered Approaches Can Combat Deepfake Pornography.” *Pakistan Journal of Life & Social Sciences* 22, no. 2 (2024). <https://doi.org/10.57239/PJLSS-2024->.
- Noerman, Chiquita Thefirstly, dan Aji Lukman Ibrahim. “Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara Criminalization of Deepfake in Indonesia as a Form of State Protection hakikatnya dapat memberikan kemudahan dalam melakukan apapun . Artificial intelligence” 7, no. 2 (2024): 1–4. <https://doi.org/10.26623/julr.v7i2.8995>.
- Noviantama, Doni, dan Alif Alfani Rahman. “Deepfake: A Review from The Victimology Perspective.” *Contemporary Issues in Criminal Law* 1, no. May (2025): 107–28. <https://doi.org/10.20885/CICL.vol1.iss2.art1>.
- Prayoga, Hendra, dan Hadi Tuasikal. “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>.
- Putri, Kartika Ardina Raesyah. “Legal Liability For Using Artificial Intelligence To Produce Deepfakes Under Personal Data Protection Law Pertanggungjawaban Hukum Atas Penggunaan Artificial Intelligence Untuk Deepfake Menurut Uu Perlindungan Data Pribadi.”

Rechtswetenschap: Jurnal Mahasiswa Hukum 3, no. 1 (2025).
<https://doi.org/10.36859/rechtswetenschap.v3i1.3962>.

Walklate, S. *Advanced Introduction to Victimology*. Elgar Advanced Introductions series. Edward Elgar Publishing Limited, 2023.

Yudha, Musfala, dan Sunardi Purwanda. “Perlindungan Hukum Bagi Korban Penggunaan Deepfake Dalam Kejahatan Pornografi.” *Indonesian Journal of Sharia and Law* 2, no. 1 (2025).
<https://doi.org/10.54622/ijsl.v2i1.371>.