Juris Doctrina Journal
Vol. 1, No. 1, April 2026, pp. 10~18

Legal Protection of Women Against AI-Based Cybercrime (Deepfake, Harassment, and Exploitation)

Farahavisa Rifastya Mahfud
Kementerian Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia

Article Info

Article history:

Received February 20, 2026
Revised March 21, 2026
Accepted April 04, 2026

Keywords:

AI-based cybercrime,
deepfake pornography,
online harassment,
digital identity exploitation,
legal protection of women

ABSTRACT

This study examines the legal protection of women against AI-based cybercrime, focusing on deepfake pornography, AI-driven online harassment, and digital identity exploitation within the Indonesian legal system. The rapid development of Artificial Intelligence has facilitated new forms of technology-enabled violence that disproportionately target women, raising serious concerns regarding legal certainty, victim protection, and effective law enforcement. The central legal issue lies in the existence of a legal vacuum in regulating AI-based cybercrime, particularly the absence of explicit legal recognition of deepfake as digital sexual violence, the lack of adequate regulation of AI-based harassment as gender-based violence, and the insufficient legal framework addressing the exploitation of personal data and digital identity. This research employs a normative juridical method using statute, conceptual, and case approaches, analyzing relevant regulations such as the Electronic Information and Transactions Law, the Sexual Violence Crimes Law, the Pornography Law, the Personal Data Protection Law, and the Criminal Code. The findings indicate that Indonesian positive law has not fully accommodated the complexity of AI-driven cybercrime, resulting in weak protection for victims and difficulties in law enforcement. This study proposes a prescriptive legal framework through the explicit criminalization of deepfake-related offenses, the recognition of AI-based harassment as gender-based cyber violence, and the integration of data protection and victim protection mechanisms to ensure comprehensive legal protection for women in digital spaces.

Corresponding Author:

Farahavisa Rifastya Mahfud
Kementerian Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia
Email: faarahrifastya@gmail.com

1. INTRODUCTION

The rapid development of Artificial Intelligence (AI) has generated new forms of cybercrime that disproportionately affect women, including deepfake pornography, AI-based online harassment, and digital exploitation of personal identity. These forms of technology-facilitated violence represent an evolution of cybercrime, characterized not only by technological

sophistication but also by their capacity to inflict severe psychological, social, and reputational harm on victims. The use of AI in generating realistic manipulated content has intensified the scale and impact of such crimes, particularly due to the accessibility of generative tools and the anonymity provided by digital platforms.[1]

Deepfake technology, in particular, enables the creation of highly realistic images and videos by manipulating facial and bodily features without the consent of the individual concerned. In many cases, this technology is used to produce non-consensual pornographic content targeting women, thereby violating their dignity, privacy, and personal security. Unlike traditional forms of cybercrime, AI-based manipulation introduces new legal challenges, as it blurs the boundaries between real and fabricated content, complicating both legal classification and evidentiary processes.[2]

The Indonesian legal framework provides several instruments that are relevant to addressing cybercrime, including Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions, Law Number 12 of 2022 on Sexual Violence Crimes, Law Number 44 of 2008 on Pornography, Law Number 27 of 2022 on Personal Data Protection, and the new Criminal Code under Law Number 1 of 2023. However, these regulations were not designed to specifically address AI-based cybercrime, resulting in a legal vacuum in the regulation of such offenses.[3]

The central legal issue in this study is the existence of a legal vacuum in regulating AI-based cybercrime against women. This vacuum is evident in several aspects. First, there is no explicit legal definition of deepfake as a form of digital sexual violence. Second, AI-based harassment is not adequately recognized as gender-based violence within existing legal frameworks. Third, there is no specific regulation addressing the exploitation of women's digital identity through AI technologies. These gaps create significant challenges in law enforcement and weaken the protection afforded to victims.[4]

The implications of this legal vacuum are substantial. Victims face difficulties in seeking legal remedies due to the lack of clear legal provisions, while perpetrators may exploit regulatory gaps to evade accountability. Furthermore, the absence of gender-sensitive legal frameworks exacerbates the vulnerability of women in digital spaces, reinforcing structural inequalities and limiting access to justice.[5]

Previous studies have examined digital violence and AI-related crimes; however, notable research gaps remain. Akhtar and Bhowmik (2025), in "Digital Violence: The Rise of Online Gender-Based Violence Against Women," analyze the increase in digital violence but do not specifically address AI-driven mechanisms such as deepfake technology. Ali et al. (2025), in "Deepfakes and Victimology," explore the impact of digital manipulation on victims but lack a normative analysis of legal vacuum within national legal systems. Anggraeni et al. (2025), in "Penegakan Hukum terhadap Modus Kekerasan Berbasis Gender Online (KBGO): Deepfake Porn AI," focus on enforcement issues but do not provide a comprehensive prescriptive framework for legal reform. These gaps highlight the need for a normative legal analysis that specifically addresses the legal vacuum in AI-based cybercrime against women.[6]

[1] S. Akhtar and M. Bhowmik, "Digital Violence: The Rise of Online Gender-Based Violence Against Women," *International Journal For Multidisciplinary Research* (2025).
[2] Muskan Sharma, "Deepfake Pornography: Examining the Impact on Women's Digital Privacy and Consent," *International Journal For Multidisciplinary Research* (2024).
[3] Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP," *Jurnal Ilmiah Hukum dan Hak Asasi Manusia* (2025).
[4] Maria Karunia Putri Maan et al., "Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi," *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora* (2025).
[5] Vagia Polyzoidou, "Digital Violence Against Women: Is There a Real Need for Special Criminalization?," *International Journal for the Semiotics of Law* (2024).
[6] S. Akhtar and M. Bhowmik, "Digital Violence"; Mahrus Ali et al., "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims," *Substantive Justice International Journal of Law* (2025); Monica Dyah Ayu Anggraeni et al., "Penegakan Hukum terhadap Modus Kekerasan Berbasis Gender Online (KBGO): Deepfake Porn AI," *Lex Journal* (2025).

Based on these considerations, this study aims to analyze the legal protection of women against AI-based cybercrime and to formulate a prescriptive legal framework that integrates cyber law, criminal law, and gender-based perspectives to ensure effective protection and enforcement.

2. METHOD

This research employs a normative juridical method, focusing on the analysis of legal norms, principles, and doctrines governing the protection of women against AI-based cybercrime within the Indonesian legal system. The research is prescriptive-analytical in nature, aiming to identify the existence of a legal vacuum and to formulate legal solutions that enhance victim protection and ensure effective law enforcement. This approach is particularly relevant in addressing emerging forms of crime driven by technological advancements.[7]

The statute approach is used to examine relevant legal instruments, including Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions, Law Number 12 of 2022 on Sexual Violence Crimes, Law Number 44 of 2008 on Pornography, Law Number 27 of 2022 on Personal Data Protection, and Law Number 1 of 2023 concerning the Criminal Code. These laws are analyzed to assess their applicability and limitations in addressing AI-based cybercrime.[8]

The conceptual approach is applied to analyze key theoretical frameworks, including feminist legal theory, cyber law, victim protection theory, and the concept of gender-based violence in digital spaces. This approach enables a critical evaluation of whether existing legal doctrines adequately address the gendered impact of AI-based cybercrime or require reformulation.[9]

The case approach is utilized to examine global cases of deepfake pornography and AI-based online harassment, providing insights into the characteristics, impacts, and legal challenges associated with such crimes. Comparative analysis is used to evaluate the relevance of these cases to the Indonesian legal context and to identify potential regulatory approaches.[10]

The legal materials used in this research consist of primary and secondary sources. Primary materials include statutory regulations governing cybercrime, criminal law, and data protection, while secondary materials consist of scholarly articles and legal studies related to AI, gender-based violence, and digital harm. These materials are systematically analyzed to support the prescriptive recommendations proposed in this study.

3. RESULTS AND DISCUSSION

Legal Vacuum in Regulating Deepfake as a Form of Digital Sexual Violence

The emergence of deepfake technology has introduced a new dimension of digital sexual violence, particularly targeting women through the creation of non-consensual pornographic content. Deepfake, which utilizes Artificial Intelligence to manipulate facial and bodily features in images or videos, enables the production of highly realistic yet fabricated content that can severely harm the dignity, privacy, and reputation of victims. Despite the growing prevalence of such practices, Indonesian positive law has not yet explicitly recognized deepfake as a distinct criminal offense, thereby creating a significant legal vacuum in addressing this form of harm.[11]

Existing legal instruments, such as the Pornography Law and the Electronic Information and Transactions Law, primarily regulate the distribution and dissemination of pornographic content. However, these laws do not specifically address the manipulation of an individual's identity through AI technologies. As a result, the act of creating deepfake content without consent

[7] Peter Mahmud Marzuki, *Pengantar Ilmu Hukum* (Jakarta: Kencana, 2014).
[8] Rafi Satrya Arvitto, "Implikasi Hukum Deepfake."
[9] Matthew Hall, Andreas Pester, and Alex Atanasov, "AI Threats to Women's Rights," *Journal of Law and Emerging Technologies* (2022).
[10] Debarati Halder and Subhajit Basu, "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment," *Information & Communications Technology Law* (2024).
[11] Muskan Sharma, "Deepfake Pornography: Examining the Impact on Women's Digital Privacy and Consent," *International Journal For Multidisciplinary Research* (2024).

is not clearly categorized within the existing legal framework, leading to difficulties in qualifying such conduct as a criminal offense. This normative gap is particularly problematic in cases where the content is fabricated but produces real harm to the victim.[12]

The Sexual Violence Crimes Law provides a broader framework for addressing sexual violence, including forms of violence conducted through electronic means. Nevertheless, the law does not explicitly mention deepfake technology, nor does it provide specific provisions regarding the unauthorized use of a person's image or identity for sexual purposes. This absence of explicit regulation further reinforces the legal vacuum, as law enforcement authorities may face challenges in applying existing provisions to cases involving AI-generated content.[13]

The implications of this legal vacuum are substantial. First, it creates uncertainty in the classification of deepfake-related acts, which may hinder effective prosecution. Second, it weakens the protection of victims, as the absence of clear legal norms limits their ability to seek justice. Third, it increases the risk of impunity, as perpetrators may exploit legal ambiguities to avoid accountability. These conditions undermine the fundamental objectives of criminal law, particularly the protection of individual rights and the deterrence of harmful conduct.[14]

From a juridical perspective, deepfake pornography should be conceptualized as a form of digital sexual exploitation and a violation of personal dignity and privacy rights. The unauthorized use of a person's image for sexual purposes constitutes a form of violence that extends beyond traditional notions of physical harm. Therefore, it is necessary to adopt a broader interpretation of existing legal provisions or to establish new norms that explicitly recognize deepfake as a criminal offense.

A prescriptive approach requires the development of legal provisions that define deepfake-related acts, establish clear elements of the offense, and provide appropriate sanctions. Such regulation should also incorporate a victim-centered perspective, ensuring that victims receive adequate protection, including the right to content removal and psychological support. By addressing this legal vacuum, the legal system can better respond to the challenges posed by AI-based digital sexual violence.

Legal Vacuum in Addressing AI-Based Online Harassment Against Women

Artificial Intelligence has also facilitated the emergence of new forms of online harassment, including automated abusive messaging, coordinated attacks using bots, and the creation of manipulated content aimed at damaging the reputation of women. These forms of harassment are often systematic, scalable, and difficult to trace due to the use of automated systems and digital anonymity. Despite their severity, existing legal frameworks in Indonesia have not adequately addressed AI-based harassment as a distinct form of gender-based violence.[15]

The Electronic Information and Transactions Law provides provisions on defamation and insults in digital spaces. However, these provisions are primarily focused on individual acts and do not account for the collective and automated nature of AI-based harassment. The use of bots and algorithms to conduct large-scale harassment campaigns introduces new challenges that are not contemplated within traditional legal frameworks. As a result, the law fails to capture the systemic nature of such conduct.[16]

The legal vacuum is further reflected in the absence of recognition of online harassment as a form of gender-based violence. While the Sexual Violence Crimes Law provides important protections for victims of sexual violence, it does not explicitly regulate harassment conducted through AI technologies. This lack of recognition limits the ability of the legal system to address

[12] Rafi Satrya Arvitto, "Implikasi Hukum Deepfake," *Jurnal Ilmiah Hukum dan Hak Asasi Manusia* (2025).
[13] Monica Dyah Ayu Anggraeni et al., "Penegakan Hukum terhadap Modus Kekerasan Berbasis Gender Online," *Lex Journal* (2025).
[14] Mahrus Ali et al., "Deepfakes and Victimology," *Substantive Justice International Journal of Law* (2025).
[15] Septhiany Meryam Saleh, "Cyber Harassment and Exploitation of Women on Social Media," *International Journal of Multidisciplinary Research and Analysis* (2025).
[16] A. Fikri, "Kebijakan Hukum dalam Pemberantasan Pelaku Online Romance Fraud," *JCIC* (2024).

the gendered impact of such conduct, particularly in cases where harassment is intended to silence or intimidate women in public and digital spaces.[17]

Another critical issue concerns the difficulty of proof in cases of AI-based harassment. The anonymity of perpetrators, combined with the automated and distributed nature of attacks, makes it challenging to identify and prosecute those responsible. Existing evidentiary rules may not be sufficient to address these complexities, thereby further weakening the effectiveness of law enforcement.[18]

The implications of this legal vacuum are significant. Women become increasingly vulnerable to harassment in digital spaces, which may discourage their participation in public discourse and limit their access to digital opportunities. Furthermore, the lack of effective legal remedies undermines trust in the legal system and perpetuates a culture of impunity.[19]

From a conceptual perspective, AI-based harassment should be recognized as a form of gender-based cyber violence, requiring a specialized legal approach that integrates criminal law, cyber law, and gender perspectives. Such recognition is essential to ensure that the legal system adequately reflects the nature and impact of the conduct.

To address this issue, it is necessary to harmonize existing legal frameworks and to introduce specific provisions regulating AI-based harassment. These provisions should define the elements of the offense, establish standards for identifying automated attacks, and provide mechanisms for victim protection. Additionally, legal reforms should strengthen investigative and evidentiary procedures to address the challenges posed by digital anonymity and algorithmic systems.

By addressing the legal vacuum in this area, the legal system can provide more effective protection for women against AI-based harassment and ensure that digital spaces remain safe and inclusive.

The analysis of deepfake-based sexual violence and AI-driven online harassment demonstrates that existing legal frameworks are not adequately equipped to address the evolving nature of cybercrime against women. These deficiencies highlight the existence of a legal vacuum in both substantive criminal law and victim protection mechanisms. As illustrated in Table 1, the differences between conventional cybercrime and AI-based cybercrime reveal structural gaps that necessitate comprehensive legal reform.

Table 1. Comparative Framework of Conventional Cybercrime and AI-Based Cybercrime Against Women

Aspect	Conventional Cybercrime	AI-Based Cybercrime	Legal Vacuum	Proposed Legal Solution
Nature of act	Direct human action	Automated & algorithmic	No legal recognition of AI conduct	Explicit legal classification
Type of harm	Defamation, fraud	Deepfake, mass harassment	Not specifically regulated	Specific criminal provisions
Evidence	Traceable actions	Complex digital traces	Difficulty in proof	Digital forensic standards
Victim impact	Individual harm	Mass & systemic harm	Lack of victim-centered approach	Victim protection mechanisms
Legal framework	Partially regulated	Fragmented & incomplete	Normative gaps	Harmonization of laws

[17] Frans Reumi et al., "Online Gender-Based Violence Crime in the Perspective of Indonesian Criminal Law," *Journal of Strafvordering Indonesian* (2025).
[18] Debarati Halder and Subhajit Basu, "Digital Dichotomies," *Information & Communications Technology Law* (2024).
[19] Vagia Polyzoidou, "Digital Violence Against Women," *International Journal for the Semiotics of Law* (2024).

Aspect	Conventional Cybercrime	AI-Based Cybercrime	Legal Vacuum	Proposed Legal Solution
Accountability	Individual liability	Diffused actors (AI, user)	Unclear responsibility	Role-based liability

Legal Vacuum in the Protection Against Exploitation of Women's Data and Digital Identity

The advancement of Artificial Intelligence has significantly increased the capacity to collect, process, and exploit personal data, thereby creating new forms of digital harm, particularly against women. AI systems are capable of aggregating vast amounts of personal information to construct detailed digital profiles, which can then be used to generate manipulated content, including deepfake materials, impersonation, and targeted harassment. Despite the existence of legal provisions governing personal data protection in Indonesia, there remains a substantial legal vacuum concerning the exploitation of women's digital identity through AI-based technologies.

Law Number 27 of 2022 on Personal Data Protection establishes general principles for the collection, processing, and safeguarding of personal data. However, the law does not explicitly regulate the use of personal data in the context of AI-driven content generation or algorithmic manipulation. This omission creates a normative gap, as the misuse of personal data for creating deepfake content or other forms of exploitation is not clearly categorized as a distinct legal violation. Consequently, existing legal frameworks may be insufficient to address the specific risks posed by AI technologies.

The legal vacuum is further reflected in the absence of explicit prohibitions against the use of personal data for generating harmful or deceptive digital content. While data protection laws emphasize consent and lawful processing, they do not adequately address situations where data is used to create entirely new forms of digital harm that extend beyond traditional data misuse. This is particularly problematic in cases involving non-consensual deepfake pornography, where victims may suffer significant psychological and social harm despite the absence of direct physical interaction.

From a constitutional perspective, the exploitation of personal data through AI technologies constitutes a violation of fundamental rights, including the right to privacy and the right to personal security. The 1945 Constitution guarantees the protection of human rights, yet the absence of specific legal safeguards against AI-based exploitation undermines the effectiveness of these guarantees. This creates a contradiction between constitutional principles and the realities of digital governance.

The implications of this legal vacuum are extensive. First, it enables widespread violations of privacy through unauthorized data use. Second, it exacerbates the vulnerability of women in digital spaces, particularly in contexts where personal data is used to create harmful or degrading content. Third, it weakens the deterrent effect of the law, as perpetrators may exploit regulatory gaps to avoid accountability.

To address these challenges, a prescriptive legal framework is required that integrates data protection and victim protection principles. This includes the establishment of explicit prohibitions against the use of personal data for harmful AI-generated content, as well as the development of effective mechanisms for content removal and victim recovery. Additionally, legal provisions should ensure that victims have access to remedies, including compensation and psychological support.

Furthermore, it is necessary to adopt a holistic approach that combines legal regulation with technological safeguards, such as monitoring systems and content verification mechanisms. By addressing the legal vacuum in this area, the legal system can provide more comprehensive protection for women against the exploitation of their digital identity in the age of AI.

4. CONCLUSION

AI-based cybercrime against women, including deepfake pornography, online harassment, and digital identity exploitation, reveals a significant legal vacuum within the Indonesian legal system. This study demonstrates that existing legal frameworks are not sufficiently equipped to address the complexity and evolving nature of such crimes, particularly in terms of legal classification, accountability, and victim protection.

The absence of explicit legal provisions recognizing deepfake as a form of digital sexual violence creates uncertainty in the qualification of criminal acts and weakens the protection afforded to victims. Similarly, the lack of specific regulation on AI-based harassment limits the ability of the legal system to address gender-based cyber violence effectively. Furthermore, the inadequate regulation of personal data exploitation in AI systems highlights the need for stronger integration between data protection and victim protection frameworks.

Therefore, this study emphasizes the urgency of developing a comprehensive legal framework that specifically addresses AI-based cybercrime against women. Such a framework should include the explicit criminalization of deepfake-related offenses, the recognition of AI-based harassment as gender-based violence, and the strengthening of legal protections against data and identity exploitation. Additionally, legal reform should prioritize victim protection, including mechanisms for rapid content removal, access to justice, and psychological recovery.

In conclusion, the protection of women in the digital era requires a responsive legal system that integrates technological awareness, gender sensitivity, and human rights principles. Only through such an approach can the legal system effectively address the challenges posed by AI-based cybercrime and ensure justice and protection for victims.

REFERENCES

Journal/Periodicals

Akhtar, S., & Bhowmik, M. (2025). Digital Violence: The Rise of Online Gender-Based Violence Against Women in the Age of Social Media. International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2025.v07i02.41785.

Ali, M., Fernando, Z., Huda, C., & Mahmutarom, M. (2025). Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims. Substantive Justice International Journal of Law. https://doi.org/10.56087/substantivejustice.v8i1.306.

Anggraeni, M., Soekorini, N., Borman, M., & Sidarta, D. (2025). Penegakan Hukum terhadap Modus Kekerasan Berbasis Gender Online (KBGO): Deepfake Porn AI. Lex Journal : Kajian Hukum dan Keadilan. https://doi.org/10.25139/lex.v9i2.11023

Arvitto, R. (2025). Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP. Jurnal Ilmiah Hukum dan Hak Asasi Manusia. https://doi.org/10.35912/jihham.v4i2.3937.

Blauth, T., Gstrein, O., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. IEEE Access, 10, 77110-77122. https://doi.org/10.1109/access.2022.3191790

Cheng, X. (2024). The Gendered Impact of Deepfake Technology: Analyzing Digital Violence Against Women in South Korea. Lecture Notes in Education Psychology and Public Media. https://doi.org/10.54254/2753-7048/75/20241102 (2024). https://doi.org/10.54254/2753-7048/75/20241102.

Di, Y. (2024). Legal Reflections: Optimizing Global Strategies Against Cyber Sexual Violence Through Comparative Perspectives. Transactions on Social Science, Education and Humanities Research. https://doi.org/10.62051/zw6md078

Fikri, A. (2024). Kebijakan Hukum dalam Pemberantasan Pelaku Online Romance Fraud di Ruang Maya. JCIC : Jurnal CIC Lembaga Riset dan Konsultan Sosial. https://doi.org/10.51486/jbo.v6i2.219

Halder, D., & Basu, S. (2024). Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India. Information & Communications Technology Law,

34, 163 - 186. https://doi.org/10.1080/13600834.2024.2408914.

Hall, M., Pester, A., & Atanasov, A. (2022). AI Threats to Women's Rights. Journal of Law and Emerging Technologies. https://doi.org/10.54873/jolets.v2i2.86

Kira, B. (2024). When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act. Comput. Law Secur. Rev., 54, 106024. https://doi.org/10.1016/j.clsr.2024.106024.

Maan, M., Amalo, H., & Dede, N. (2025). Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana. Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora. https://doi.org/10.55606/jurrish.v4i1.5071.

Marzuki, Peter Mahmud. (2014). Pengantar Ilmu Hukum. Jakarta: Kencana

Nazakat, T., & Malik, F. (2025). Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence with Advanced Solutions. Journal of Law & Social Studies. https://doi.org/10.52279/jlss.07.01.2642.

Ong, H., Afdal, W., & , T. (2025). PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA. Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat. https://doi.org/10.55809/tora.v11i2.579.

Polyzoidou, V. (2024). Digital Violence Against Women: Is There a Real Need for Special Criminalization?. International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique, 37, 1777 - 1797. https://doi.org/10.1007/s11196-024-10179-3

Putri, N., & Apriyani, M. (2025). Pertanggungjawaban Pidana Pelaku Kekerasan Seksual Berbasis Elektronik Artificial Intelegence (Deep Fake Porn). Wajah Hukum. https://doi.org/10.33087/wjh.v9i1.1725.

Reumi, F., Medan, K., Pelupessy, A., & Usman, R. (2025). Online Gender-Based Violence(GBV) Crime In The Perspective Of Indonesian Criminal Law. Journal of Strafvordering Indonesian. https://doi.org/10.62872/xez31j88.

Saleh, S. (2025). Cyber Harassment and Exploitation of Women on Social Media: Perspective of Positive Law and Islamic Law. INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS. https://doi.org/10.47191/ijmra/v8-i06-21.

Sharma, M. (2024). Deepfake Pornography: Examining the Impact on Women's Digital Privacy and Consent. International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2024.v06i04.24146.

Statute

Republic of Indonesia. Constitution of the Republic of Indonesia. 1945. Jakarta: State Secretariat, 1945.

Republic of Indonesia. Amendment to the Law on Information and Electronic Transactions. Law No. 19 of 2016. Jakarta: State Secretariat, 2016.

Republic of Indonesia. Law on Sexual Violence Crimes. Law No. 12 of 2022. Jakarta: State Secretariat, 2022.

Republic of Indonesia. Law on Pornography. Law No. 44 of 2008. Jakarta: State Secretariat, 2008.

Republic of Indonesia. Law on Personal Data Protection. Law No. 27 of 2022. Jakarta: State Secretariat, 2022.

Republic of Indonesia. Criminal Code. Law No. 1 of 2023. Jakarta: State Secretariat, 2023..

United States Congress. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Public Law 104-191. Washington, DC: U.S. Government Publishing Office, 1996.