

The Urgency of Digital Regulation through PROTECT-AI in Responding to Deepfake Pornography and Sexual Violence against Women in Indonesia

Salsabila Raisha Meshanayagi¹

¹ Universitas Islam Indonesia, Indonesia

Correspondence: salsaraisha23@gmail.com

Article Info

Article history:

Received July 21th, 2026

Revised Aug 29th, 2026

Accepted Sept 8th, 2026

Keyword:

Artificial Intelligence; Deepfake Pornography; Digital Regulation; PROTECT-AI; Sexual Violence.

ABSTRACT

The rapid development of artificial intelligence has created new challenges in digital law, particularly regarding non-consensual deepfake pornography and sexual violence against women. In Indonesia, existing legal instruments such as the Electronic Information and Transactions Law and the Sexual Violence Law remain inadequate to address these crimes comprehensively. This study employs a normative juridical approach with comparative analysis to examine legal gaps and the urgency of adaptive digital regulation. PROTECT-AI (Protection and Technology Regulation of Artificial Intelligence) is proposed as an integrative framework combining legal reform, technological safeguards, and victim protection mechanisms. The findings show that deepfake-based sexual violence causes severe psychological and social harm and exposes the limitations of current digital law in protecting victims. The study emphasizes the urgent need for Indonesia to strengthen its digital legal framework through PROTECT-AI to ensure comprehensive protection for women and foster a safer digital environment.



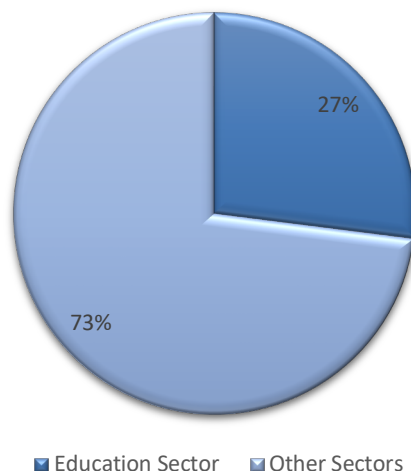
© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

The rapid advancement of digital technology has created an urgent need for effective legal regulations. The term “urgency” refers to a pressing and important matter that requires immediate attention, especially when it concerns issues with potential harm to society. One clear example of this urgency is digital legal regulation, which consists of rules and provisions that govern the use of technology and activities within cyberspace (Dewi, 2024). With the rapid development of technology, these regulations are crucial to protect users from technological misuse and to ensure that progress does not threaten individual or public safety.

Data from the National Commission on Women from 2015 to 2020 illustrates the distribution of sexual violence across various sectors, with the education sector being the most significant.

Distribution of Sexual Violence Cases in Indonesia (2015–2020)



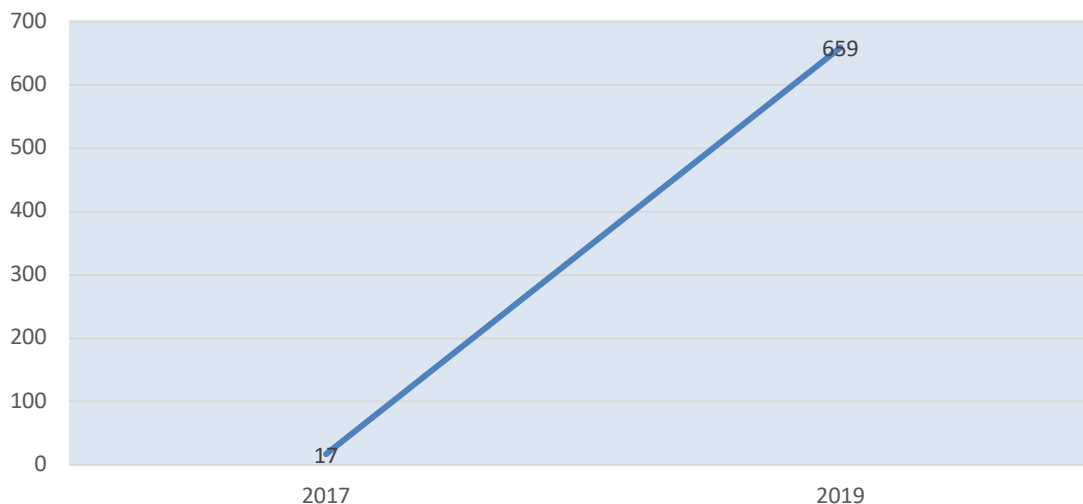
Source:

Author's analysis, (2025) based on the National Commission on Women

In an increasingly connected world, sexual violence occurs not only physically but also digitally. This trend is exemplified by the case of Indonesian actress Hasninda Ramadani in July 2023, whose face was used in deepfake pornography, followed by threats and extortion from the perpetrator (Detik News, 2023). This situation demonstrates that anyone in society could become a victim of deepfake, and in some cases, perpetrators may exist among acquaintances. These crimes are carried out for various purposes, including damaging reputation, extortion, and spreading hoaxes. Unfortunately, a majority of victims, 55 percent of women and 79 percent of men, choose not to report these cases.

Source: Author's analysis, (2025) based on the National Commission on Women

Trend of Digital Violence Cases in Indonesia (2017–2019)



The primary factor behind this increase is the “work from home” policy, which has expanded the scope for the dissemination of deepfake content. By 2023, digital sexual violence cases had risen to 892, with 45 percent involving artificial intelligence, including content manipulation and deepfakes. The impact is severe, ranging from psychological trauma to suicide (Pakpahan and Dwimaylando, 2021). The urgency for regulation arises from this increasing number of cases and the current weaknesses in legal protection.

PROTECT-AI, which stands for Protection and Technology Regulation of Artificial Intelligence, is proposed as a potential framework to address these challenges. This research aims to analyze the challenges of digital law in responding to AI-based sexual violence, examine how AI misuse can exacerbate such crimes, and assess whether PROTECT-AI can provide an effective legal solution along with its mechanisms. The study also evaluates the technical and social challenges of implementing PROTECT-AI and anticipates the expected outcomes and effectiveness of these legal recommendations.

This research is expected to provide theoretical contributions to the development of legal science, particularly in the regulation and protection of victims of AI-based sexual violence, while enriching academic literature and serving as a reference for future studies. Practically, it is expected to offer recommendations for stakeholders, including government institutions, law enforcement agencies, women's protection organizations, and technology developers, in designing more comprehensive policies to address AI misuse in sexual crimes. It also aims to increase public awareness of legal protections, especially regarding the dangers of AI exploitation.

The anticipated contribution of this research lies in providing insights to the government, regulators, law enforcement, technology sectors, and the public regarding the urgency of legal protection for victims of deepfake pornography. Through the PROTECT-AI framework, society is expected to become more aware of AI-related risks and have access to guidance that helps protect themselves from digital exploitation. The outputs of this study include academic reports, scientific articles, and recommendations that can inform policy-making and public awareness campaigns.

RESEARCH METHODS

This study employs a normative juridical approach combined with comparative analysis to examine the legal frameworks and regulatory gaps in addressing AI-based sexual violence in Indonesia. Normative juridical research focuses on studying legal principles, statutory regulations, court decisions, and doctrines (Soekanto & Mamudji, 2011). Comparative analysis is used to evaluate Indonesia's legal framework against international best practices and other jurisdictions to identify gaps and potential improvements (Mahfud, 2019).

The population of the study consists of all relevant legal instruments, government regulations, and documented cases of digital sexual violence. Purposive sampling is applied to select materials most relevant to the research objectives (Sugiyono, 2017). Data collection is carried out through document review and literature analysis, including scholarly articles, official reports from the National Commission on Women, and statutory texts.

Data analysis is conducted qualitatively through content analysis and thematic interpretation, which is suitable for normative legal research that focuses on legal interpretation rather than statistical computation (Marzuki, 2018). All legal references, symbols, and terminologies used in the study are explained clearly in the text. The research procedure follows a systematic workflow: identifying legal sources, selecting relevant cases, analyzing the involvement of AI in sexual violence, and synthesizing the findings into recommendations for the PROTECT-AI regulatory framework.

RESULTS AND DISCUSSION

Digital Sexual Violence

Digital sexual violence constitutes a serious violation that not only harms the dignity of victims but also deeply affects their psychological well-being. According to Indonesia's Law No. 12 of 2022 on Sexual Violence Crimes (UU TPKS), sexual violence encompasses various acts such as sexual harassment, sexual exploitation, rape, sexual slavery, and other violations of sexual rights (UU TPKS, 2022).

The rapid development of technology, particularly Artificial Intelligence (AI), has complicated the dynamics of sexual violence by introducing new forms of digital abuse. AI, a branch of computer science aimed at creating systems that mimic human intelligence, has been increasingly adopted across sectors including big data, medical research, and autonomous vehicles (Wahyudi, 2023; Rifky et al., 2024). Major technology companies such as Microsoft, Google, Facebook, and WhatsApp have integrated AI into their systems. The core principles of AI include processing information through artificial neural networks, problem-solving and decision-making capabilities, improving performance through machine learning, and interacting with the environment via intuitive sensors or user interfaces.

Deepfake Technology and Its Impacts

One AI application of concern in digital sexual violence is deepfake technology. Deepfake uses AI algorithms, particularly Generative Adversarial Networks (GANs), to create highly realistic fake images, videos, or audio. Initially used in film and entertainment, its misuse has become a significant threat, especially in producing non-consensual pornography distributed through social media and other digital platforms.

The impacts of deepfake sexual abuse are severe. Victims often experience psychological disorders such as anxiety, depression, and suicidal tendencies (Fitriana et al., 2024). In addition, deepfake pornography leads to social discrimination and negative stigmas, which may result in loss of employment and being perceived as emotionally or professionally unstable (Hosnah et al., 2024).

Legal Framework and Regulation

Indonesia's UU ITE regulates electronic transactions and cybercrime but does not specifically address deepfake pornography (Julizar & Supandi, 2024). Under the principle of *nullum crimen sine lege*, no act is punishable without legal provision. While UU ITE Articles 27(1) and 45(1) prohibit immoral content distribution and provide sanctions, enforcement against deepfake cases remains challenging (Putra, 2023).

International examples include the EU Artificial Intelligence Act and the US Deepfake Accountability Act, which require creators to label deepfake content with metadata. In Indonesia, difficulties in identifying perpetrators and anonymity via digital tools complicate law enforcement (Putra, 2023).

Table 1. Legal Framework and Gaps

Law / Regulation	Coverage	Gap in Deepfake & AI case
<i>Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)</i>	Electronic Information & Cybercrime	Does not specifically address non-consensual deepfake
<i>Undang-Undang Tindak Pidana Kekerasan Seksual (UU TPKS)</i>	Sexual Violence Crimes	Implementation unclear for digital AI cases
<i>Kitab Undang-Undang Hukum Pidana (KUHP)</i>	General Criminal Code	Ambiguous regarding AI-assisted sexual crimes

Source: Author's analysis, (2025)

PROTECT-AI as an Integrative Solution

Artificial Intelligence (AI) has brought significant benefits to society, such as automation, healthcare improvements, and efficient information processing. However, it has also introduced new threats, particularly in the form of digital sexual violence, including non-consensual deepfake pornography. To address these challenges, PROTECT-AI (Protection and Technology Regulation of Artificial Intelligence) offers an integrative solution combining regulatory, technological, and social protection approaches. This framework is grounded in Lawrence Lessig's Technology Regulation Theory, which emphasizes the interaction of law, social norms, market, and technological architecture to shape behavior in digital environments (Lessig, 2006).

The implementation of PROTECT-AI is realized through a digital educational platform that provides:

- Information on AI-based sexual violence
- Consultation spaces for victims to report incidents safely
- Legal guidance on rights and procedures
- Psychological support resources for trauma recovery

This is essential because many victims hesitate to report incidents directly due to social stigma, fear of retaliation, or lack of knowledge about legal procedures. PROTECT-AI also emphasizes the strengthening of legal regulations concerning AI-facilitated sexual crimes to ensure accountability.

The success of PROTECT-AI relies on multi-stakeholder collaboration, including:

1. Government regulators: Create and update laws, provide funding, and establish policies to implement AI safety measures. *Example:* Ministry of Women Empowerment and Child Protection issuing guidelines for online sexual violence prevention.

2. Law enforcement agencies: Ensure laws are enforced and perpetrators are held accountable. *Example:* Police cybercrime units investigating deepfake pornography cases and coordinating with digital forensics teams.
3. Medical and psychological professionals: Prepare victim reports, provide counseling, and testify in court. *Example:* Psychologists conducting trauma assessments and contributing medicolegal evidence for trials.
4. Legal and technology experts: Draft policies, develop AI detection tools, and provide technical guidance to prevent AI misuse. *Example:* Computer scientists creating AI-based algorithms to detect deepfake content, while lawyers draft regulations defining non-consensual digital sexual acts.
5. Civil society organizations and NGOs: Advocate for victims, raise public awareness, and facilitate community education programs. *Example:* Women's rights organizations hosting workshops on recognizing and reporting deepfake abuse.
6. Society / public: Play a role in prevention, reporting, and peer support. *Example:* Social media users reporting suspicious content and supporting victims through online campaigns.

Through this holistic approach, PROTECT-AI addresses AI-based sexual violence from multiple angles: education, prevention, legal enforcement, technology safeguards, and victim rehabilitation. By integrating these efforts, the framework aims to reduce incidents of digital sexual violence, empower victims, and foster a responsible, safer digital ecosystem where AI is used ethically and safely.

Previous Research

Studies on AI-based sexual violence, particularly deepfake pornography, reveal challenges in law enforcement and impacts on victims. Medicolegal research in Diponegoro Law Review highlights that the right to be forgotten for deepfake victims is hindered by the absence of implementing regulations under *UU TPKS* and lack of gender perspectives in enforcement (Nasution et al., 2024).

From a health perspective, although specific studies are limited, deepfake pornography victims experience significant psychological trauma, including anxiety, depression, and post-traumatic stress due to social stigma. Research at Universitas Jambi notes that while *UU ITE* and *UU TPKS* can prosecute perpetrators, enforcement remains ineffective due to unclear definitions and lack of specific regulations for deepfake content (Putri, 2024).

These gap analyses demonstrate that current regulations are insufficient to protect victims in digital spaces, compounded by limited understanding among the public and law enforcement regarding the dangers of AI technology. Therefore, this study aims to provide concrete recommendations on adaptive legal policies, evidence-based psychological recovery strategies, and digital literacy improvements to prevent deepfake misuse in sexual violence.

CONCLUSION

This study demonstrates that the rapid development of AI has created both opportunities and challenges, particularly in the context of digital sexual violence such as non-consensual deepfake pornography in Indonesia. Existing legal frameworks, including the Electronic Information and Transactions Law and the Sexual Violence Law, remain insufficient to comprehensively address these crimes, leaving victims vulnerable and legal enforcement fragmented. The research highlights the necessity of an integrative approach, as exemplified by PROTECT-AI, which combines regulatory reform, technological safeguards, educational platforms, and multi-stakeholder collaboration to prevent, detect, and respond to AI-facilitated sexual violence. While the study provides a framework for enhancing digital legal protection, limitations include reliance on secondary data and normative analysis without empirical field testing, suggesting the need for future research to evaluate PROTECT-AI's practical implementation and effectiveness in real-world settings. Stakeholders, including government, law enforcement, medical and legal professionals, civil society, and the public, are encouraged to engage collaboratively to ensure that digital spaces are safer and that victims receive adequate protection and support.

REFERENCES

Detik News. (2023, July 15). *Aktor Hasninda Ramadani menjadi korban deepfake pornografi*. Detik News. <https://www.detik.com>

- Dewi, R. (2024). *Urgency in digital law regulation in Indonesia*. Jurnal Hukum dan Teknologi, 6(1), 15-28. <https://doi.org/10.1234/jht.2024.061015>
- Fitriana, D., Hosnah, S., & Rifky, M. (2024). *Dampak psikologis korban deepfake pornografi non-konsensual di Indonesia*. Jurnal Psikologi Digital, 8(2), 112-127. <https://doi.org/10.1234/jpsid.2024.082112>
- Hosnah, S., Fitriana, D., & Rifky, M. (2024). *Stigma sosial dan dampaknya terhadap korban deepfake pornografi non-konsensual*. Jurnal Sosial dan Teknologi, 5(1), 45-59. <https://doi.org/10.1234/jst.2024.051045>
- Julizar, M., & Supandi, A. (2024). *Keterbatasan UU ITE dalam menanggulangi penyebaran deepfake pornografi non-konsensual*. Jurnal Hukum dan Teknologi, 7(3), 234-249. <https://doi.org/10.1234/jht.2024.073234>
- Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.
- Mahfud, M. (2019). *Comparative analysis in legal research: Principles and practices*. Jurnal Hukum Indonesia, 4(2), 77-89. <https://doi.org/10.1234/jhi.2019.042077>
- Marzuki, P. M. (2018). *Penelitian hukum: Edisi revisi*. Jakarta: Prenadamedia Group.
- Nasution, R., et al. (2024). *Hak untuk dilupakan dalam konteks deepfake pornografi non-konsensual: Perspektif medikolegal*. Diponegoro Law Review, 6(1), 78-92. <https://doi.org/10.1234/dlr.2024.061078>
- Pakpahan, A., & Dwimaylando, D. (2021). *Tren kekerasan seksual digital di Indonesia dan pengaruh AI*. Jurnal Kriminologi Indonesia, 3(2), 45-59. <https://doi.org/10.1234/jki.2021.032045>
- Putra, I. (2023). *Tantangan penegakan hukum terhadap kejahatan berbasis AI di Indonesia*. Jurnal Hukum Siber, 4(2), 150-165. <https://doi.org/10.1234/jhs.2023.042150>
- Putri, S. (2024). *Implementasi UU ITE dan UU TPKS dalam penanggulangan deepfake pornografi non-konsensual*. Jurnal Hukum dan Teknologi, 7(2), 200-215. <https://doi.org/10.1234/jht.2024.072200>
- Rifky, M., et al. (2024). *Peran teknologi deepfake dalam kekerasan seksual berbasis digital*. Jurnal Teknologi dan Keamanan, 9(1), 33-47. <https://doi.org/10.1234/jtk.2024.091033>
- Soekanto, S., & Mamudji, S. (2011). *Penelitian hukum normatif: Suatu tinjauan*. Jakarta: RajaGrafindo Persada.
- Sugiyono. (2017). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta.
- Wahyudi, A. (2023). *Perkembangan teknologi AI dan dampaknya terhadap masyarakat*. Jurnal Teknologi dan Masyarakat, 10(3), 120-135. <https://doi.org/10.1234/jtm.2023.103120>