Electronic Journal of Education, Social Economics and Technology
Vol. 7, No. 1, (2026), e1453
ISSN 2723-6250 (online)
DOI: https://doi.org/10.33122/ejeset.v7i1.1453

Research Article

Reformulating Legal Protection for Victims of Artificial Intelligence-Based Deepfake Pornography: A Digital Victimology Perspective in Indonesia

Abdul Muftar Rifki Maulana*, and Indah Sri Utari

Department of Law, Universitas Negeri Semarang, Semarang, Jawa Tengah, 15417, Indonesia
*Corresponding Author: abdulmuftar67@gmail.com | Phone: +6287766908519

ABSTRACT

The rapid development of artificial intelligence (AI) based deepfake technology has created a new form of digital sexual violence: non-consensual synthetic pornographic content that algorithmically places victims in explicit material without their involvement. Indonesia's positive legal framework spanning the Electronic Information and Transactions Law, the Pornography Law, the Sexual Violence Crimes Law, and the new Criminal Code has yet to provide a comprehensive protection mechanism specifically addressing the rights of deepfake pornography victims. This normative legal study employs statutory, conceptual, and case approaches to analyze: (1) the characteristics of digital victimization experienced by deepfake pornography victims, and (2) a reformulation model of legal protection responsive to victims' recovery needs. Drawing on Satjipto Rahardjo's legal protection theory and Karuppannan Jaishankar's Cyber Victimology framework, this study reveals three fundamental gaps: the absence of AI-specific criminal provisions, the lack of restorative mechanisms (content take-down, right to be forgotten, psychological rehabilitation), and normative uncertainty from ongoing legislative transition. As its primary novelty, this study proposes a three-tiered protection model preventive, repressive, and restorative as a victim-centred normative architecture for the Indonesian legal system.

Keywords: deepfake pornography; digital victimology; legal protection; artificial intelligence; sexual violence

1. INTRODUCTION

Technological transformations based on artificial intelligence have given rise to a new form of visual manipulation known as “deepfakes” an audiovisual engineering technique that uses deep neural networks to algorithmically superimpose a person’s face, voice, or body onto content that appears authentic but is entirely digitally fabricated (Tolosana et al. 2023). Deepfake pornography refers to sexually explicit audiovisual content produced by manipulating a victim’s visual identity without their consent. Unlike revenge porn, which requires original material from the victim, deepfake pornography allows perpetrators to create explicit illusions using only the victim’s publicly available photos or videos, meaning someone can become a victim of a sexual crime without ever having participated in the acts depicted (Rousay 2023).

Global data confirms the scale of this phenomenon. A multinational study of ten countries found that the practice of technology-based manipulation of intimate images continues to rise and has serious psychological consequences for victims, including anxiety, depression, and a loss of sense of security in the digital space (Umbach and Henry n.d.). Women are disproportionately targeted, as reported by international organizations that have highlighted the surge in the use of AI in the production of non-consensual sexual content (Geneva n.d.). Data from the National Commission on Violence Against Women (Komnas Perempuan) shows that there were 1,791 cases of online gender-based violence (KBGO) in 2024, a 40.8 percent increase from the previous year (Komnas n.d.). National law enforcement agencies, in collaboration with the UNDP, have officially warned of a surge in the misuse of AI in the context of digital violence against women in Indonesia (Police n.d.). One of the most significant judicial precedents is the case of Chiko Radityatama Agung Putra in Semarang, in which deepfake technology was used to produce sexual content by superimposing the victim’s face without her consent, and the case has resulted in a final and binding court ruling (Jateng.jppn 2026; Tempo n.d.). However, the judicial process revealed systemic limitations: charges must be based on general legal principles that were not designed to address AI-based crimes, resulting in the victims’ rights not being adequately addressed.

Indonesia’s positive legal framework has, in fact, provided several potentially relevant instruments, including the ITE Law and its amendments, the Pornography Law, the Personal Data Protection Law, the Sexual Violence Crimes Law, and the new Criminal Code (Law No. 1/2023). However, all of these instruments share a common orientation: they focus on

punishing perpetrators and neglect the need to restore victims' rights (Rahel Octora& 2025). None of them include mechanisms that specifically guarantee victims' rights to content takedown, restoration of reputation, or psychological rehabilitation.

The research gap that justifies this study is twofold. Normative gap: existing regulations do not yet comprehensively address mechanisms for restoring victims' rights, while legislative transitions (the repeal of several provisions of the ITE Law by the new Criminal Code without adequate replacement provisions) have exacerbated legal uncertainty. Epistemological gap: existing legal studies remain focused on the criminalization of perpetrators, thereby failing to capture the true nature of the victimization experienced by victims namely, victimization that is permanent, multidimensional, and ongoing even after the legal process has concluded(Iqrar 2026).

Research on deepfake pornography from a legal perspective has begun to emerge, but it shows a consistent trend: the majority of studies focus their analysis on the criminalization of perpetrators, the formulation of criminal offenses, and comparisons of regulations across countries. (Irawati 2025) In her thesis on the criminal liability of perpetrators of deepfake pornography, which draws on a comparative study of Indonesia, Australia, and South Korea, she makes an important contribution to mapping comparative legal practices, but does not systematically elaborate on the dimension of victimization. (Sonia 2025) examining the legal vacuum regarding the regulation of deepfake crimes in the Indonesian legal system using a regulatory inventory approach, without specifically addressing the actual impacts experienced by victims.

(Hidayat 2024) dan (Pratiwi 2025) Each examines the legal definition of cyberpornography and the reform of regulations on online sexual violence, but neither has addressed the specific characteristics of AI-based deepfakes as a new form of digital victimization. (Aruan 2025) In its journal article on legal protection for victims of AI misuse in pornography-related crimes, Indonesia offers an analysis that aligns more closely with the focus of this study; however, it remains limited to a normative legal approach without integrating a digital victimology framework as the basis for constructing legal protection. Studies on efforts to combat deepfake pornography in Indonesia address law enforcement dimensions but have not yet offered an operational normative model for victim protection (Andira and Susila 2024).

This study differs substantively from all of the above studies in three ways. First, it focuses on victims rather than perpetrators as the primary subjects of analysis. Second, it integrates the perspective of cyber victimology. (Jaishankar 2020) as a coherent analytical framework for examining Indonesian positive law. Third, to develop a concrete, three-tiered model of legal protection (preventive, repressive, and restorative) that is oriented toward victim recovery, going beyond a descriptive analysis of legal gaps.

1. Satjipto Rahardjo's Theory of Legal Protection

(Rahardjo 2014) defines legal protection as an effort to safeguard a person's interests by granting them the authority to act in pursuit of those interests. Rahardjo distinguishes between two forms of protection: preventive (preventing violations through regulations that impose obligations and set guidelines) and repressive (restoring rights through dispute resolution and sanctions). As the concept has evolved, legal protection that responds to digital crimes requires a third dimension: restorative that is, mechanisms that actively restore the victim's position, including the erasure of digital traces, psychological rehabilitation, and restoration of reputation (Mulyanti 2025).

In the context of deepfake pornography, Rahardjo's theory identifies systemic inadequacies: Indonesian law only partially addresses the repressive dimension (punishment of perpetrators), while the preventive and restorative dimensions particularly those related to digital identity and victim recovery are virtually absent from the existing legal framework. This situation places victims in a structurally vulnerable position because the law has not yet been able to empower victims to take action to protect their own interests.

2. Cyber Victimology Jaishankar Karuppananna

(Jaishankar 2020) developing Cyber Victimology as a new subdiscipline of 21st-century victimology that specifically examines victims of crime in cyberspace. This framework is relevant for understanding the three unique characteristics of deepfake pornography victimization that are not captured by conventional legal approaches.

First, unawareness of victimization: victims of deepfake pornography often do not realize they have become the target of a crime until the content has already been widely circulated. There is no moment of physical contact or direct interaction that could alert the victim to the risk. Second, repeated and permanent revictimization: unlike physical crimes that are concluded in a single incident, deepfake content can be copied, redistributed, and modified indefinitely. Every new user who accesses the content represents another episode of revictimization for the victim—a dimension of suffering not captured by conventional criminal law concepts (Rousay 2023). Third, the multidimensional nature of the harm: victims experience psychological harm (trauma, anxiety, depression), social harm (stigma, isolation), reputational harm (loss of employment, social relationships), and economic harm (recovery costs), all of which reinforce one another in a continuous cycle of digital victimization (Lewoba 2024).

The integration of the Jaishankar framework into an analysis of Indonesian positive law opens up a new perspective: a legal protection system cannot be evaluated solely based on the presence or absence of criminalization norms, but must be measured by its ability to break the cycle of revictimization, restore victims' control over their digital identities, and deliver substantive justice that goes beyond criminal convictions of perpetrators.

Based on the identification of these gaps, this study aims to: (1) analyze the characteristics of digital victimization among victims of AI-based deepfake pornography and the shortcomings of mechanisms for restoring victims' rights under Indonesian positive law; and (2) formulate a model for reformulating legal protection that is responsive to the needs of restoring victims' rights within the Indonesian legal system.

2. RESEARCH METHOD

This study employs the method of normative legal research (doctrinal legal research), which treats law as norms, principles, or doctrines that are examined systematically and analytically (Soemitro 1990). The choice of this method is based on the nature of the issues under investigation: the gaps and inadequacies in Indonesia's positive legal norms in accommodating the specific characteristics of AI-based deepfake pornography crimes and the protection of victims' rights.

This study combines three approaches in an integrated manner. The statutory approach is used to systematically examine all relevant positive legal instruments, including the ITE Law and its amendments, the Pornography Law, the Personal Data Protection Law, the Sexual Violence Crimes Law, and the new Criminal Code (Law No. 1/2023), in order to identify normative gaps in a structured manner. The conceptual approach was used to construct a theoretical framework for legal protection based on Satjipto Rahardjo's theory and Jaishankar's Cyber Victimology as an analytical foundation. The case approach was used to analyze the case of Chiko Radityatama Agung Putra in Semarang as the first judicial precedent involving deepfake pornography in Indonesia that has become final and binding.

Legal sources consist of three tiers. Primary legal sources include the laws and regulations mentioned above, as well as the 1945 Constitution. Secondary legal sources include recent academic literature (2020–2026), such as theses, national and international journals, and reports from human rights institutions and state commissions relevant to the phenomena of deepfake pornography and digital victimology, including all references used in this study. Tertiary legal sources include legal dictionaries, encyclopedias, and electronic sources that support the understanding of technical concepts.

The collection of legal materials was conducted through systematic library research, utilizing national and international academic databases. The analysis was conducted using a prescriptive-analytical approach: identifying and describing existing normative conditions, critically analyzing gaps through the lens of the selected theory, and then formulating a more comprehensive model of legal protection as the research's normative contribution.

3. Characteristics of Digital Victimization Among Victims of Deepfake Pornography

3.1 Typology of Digital Victimization in AI-Based Deepfake Porn Crimes

AI-based deepfake pornography presents a form of victimization that is structurally different from conventional digital sexual crimes. In revenge porn, the victim has previously produced material that is later misused. In deepfake pornography, no original material from the victim is used; instead, the perpetrator constructs the entire content algorithmically from the victim's publicly available photos or videos. This creates a fundamental legal paradox: the victim never actually performed the acts depicted, yet suffers the consequences as if they had (AlfaniRahman, Alif & 2025).

Based on an analysis of the available literature and case studies, there are four dimensions of victimization that consistently emerge among victims of deepfake pornography. First, psychological victimization: victims experience deep trauma, shame, chronic anxiety, and depression. Research (Rousay 2023) shows that some victims experience prolonged psychological distress due to their inability to erase digital traces that have already spread. Second, social and reputational victimization: the victim's social identity is distorted through false content, resulting in the breakdown of personal, professional, and community relationships. Third, economic victimization: victims bear the psychological, legal, and technical costs of recovery efforts that are often not fully successful. Fourth, permanent and repeated revictimization: the unique characteristics of digital media allow content to continue to be circulated, re-downloaded, and modified by new parties without the victim's knowledge, creating a cycle of victimization with no clear end in sight (Umbach and Henry n.d.).

It is this fourth dimension that is the most critical yet the most overlooked by the Indonesian legal system. The cycle of revictimization does not end with the imposition of a criminal sentence on the perpetrator. As long as the content remains accessible in the digital space, the victim continues to suffer. The Indonesian legal system does not yet have mechanisms to effectively break this cycle.

3.1.1 The Chiko Radityatama Case: Precedents and Limitations

The case of Chiko Radityatama Agung Putra, which is being heard in the Semarang District Court, is one of the first judicial precedents to directly address the issue of deepfake pornography in the context of Indonesian criminal law enforcement

(Jateng.jppn 2026; Tempo n.d.). The defendant was found guilty and sentenced to prison, but an analysis of the judicial process revealed significant shortcomings.

First, the charges rely on general legal provisions (Article 27 of the ITE Law and the Pornography Law) that were not designed to accommodate the complexities of AI technology. There are no provisions that explicitly regulate non-consensual AI-generated synthetic content, so the classification of criminal offenses must be done by analogy a process prone to uncertainty. Second, the court's ruling does not include mechanisms for restoring the victim's rights: there is no order to remove the content, no restoration of reputation, and no psychological restitution. The victim emerges from the judicial process without any certainty that the content causing them harm has been removed from digital circulation. Third, the technical aspects of AI-based crimes such as identifying the deepfake model used, tracing the distribution of content, and determining the locus delicti in the digital space are not adequately addressed in the evidentiary process (Kartadinata 2026).

This precedent empirically confirms that a legal vacuum is not merely a theoretical issue: it results in tangible consequences in the form of protection for victims that is disproportionate to the harm they have suffered.

3.1.2 Analysis of Gaps in Indonesia's Positive Law

Table 1. Comparative Analysis of Indonesian Legal Instruments Regarding Deepfake Pornography

Legal Instruments	Relevant Provisions	Scope of Deepfake AI	Victim Redress Mechanisms	Key Gaps
UU ITE (UU No. 11/2008 jo. UU No. 1/2024)	Article 27, paragraphs (1) and (4); Article 45, paragraph (1)	Does not explicitly depend on the interpretation of moral content	None	Does not regulate AI-generated synthetic content without a specific takedown mechanism.
UU Pornography (UU No. 44/2008)	Article 1, item 1; Article 4; Article 29	Partial; the definition of pornography does not include synthetic content	None	The definition is limited to real-world material; it does not include synthetic deepfakes.
UU TPKS (UU No. 12/2022)	Article 14 (KBGO), Articles 30–36 (victims' rights)	Potential; KBGO may include deepfakes	Restitution and Rehabilitation (Article 30)	Does not specifically mention AI content; takedown procedures are not regulated.
KUHP New (UU No. 1/2023)	Article 400-407 (Pornography)	Not yet fully effective; does not mention AI	None	Replacing the ITE offense without specific AI-related provisions; a legislative transition gap.
UU PDP (UU No. 27/2022)	Articles 65 and 66 (Prohibition on Data Processing)	The Potential for Digital Identity	Compensation (Article 68)	Focusing on personal data, not specifically on synthetic sexual content

Based on the analysis in **Table 1**, there are three fundamental systemic gaps. The first gap is the absence of specific criminal offenses for AI-generated synthetic sexual content. All existing legal instruments define pornographic material or sexual content in the context of real, rather than synthetic, material. This creates a space of normative uncertainty that is exploited by perpetrators and hinders law enforcement from effectively prosecuting deepfake cases (Lestari 2024; Mulyanti 2025).

The second gap is the absence of restorative mechanisms based on victims' rights. Although the TPKS Law addresses the rights of sexual violence victims to redress in general, there are no provisions that technically and operationally regulate mechanisms for taking down AI-generated content, a legally enforceable "right to be forgotten," or the obligation of digital platforms to respond to removal requests within a specified timeframe (Ardiansyah 2024; Rahel Octora& 2025).

The third gap is normative uncertainty resulting from the legislative transition. The enactment of Law No. 1/2023 on the Criminal Code, which will replace several provisions of the ITE Law, has not been accompanied by replacement provisions that explicitly address AI-based crimes. This transitional period creates a normative vacuum that directly impacts cases currently being processed or those that will be processed in the future (Aryawan 2026; Hidayat 2024).

3.1.3 A Model for Reformulating the Three-Tier System of Legal Protection

Based on the above gap analysis and drawing on Rahardjo's theory of legal protection and Jaishankar's Cyber Victimology, this study formulates a three-tiered, victim-centered model for the reformulation of legal protection. This model represents a novel contribution to the field, distinguishing it from previous studies that stopped at identifying normative weaknesses without offering operational alternative frameworks.

Table 2. A Reformulated Model of Three-Tiered Legal Protection Based on Digital Victimology

Dimension	Component	Specific Mechanism	Proposed Normative Basis
Preventive	Digital literacy & platform governance	Platforms' obligation to implement a system for detecting synthetic AI-generated content; public education; digital watermarks on synthetic content.	Addition of Articles in the Revision of the ITE Law and the Criminal Code: Platform Responsibilities and Digital Literacy
Repressive	Specific criminalization of AI-based deepfake pornography	Specific offense: the creation, distribution, or possession of non-consensual sexual deepfake content, punishable by appropriate criminal penalties and with aggravating circumstances if the victim is a child or a woman	Specific provisions in Book II of the Criminal Code or the TPKS Law (amendment)
Restorative	Comprehensive restoration of victims' rights	Mandatory removal of content within 24 hours; a legally enforceable "right to be forgotten"; restitution by the perpetrator; free psychological rehabilitation services provided by the government; legal assistance for victims.	Amendments to the TPKS Law & Technical Government Regulations for Implementation

3.1.4 Preventive Dimensions of Platform Governance and Digital Literacy

The preventive dimension of this model is not limited to public education but includes a legal obligation for digital platforms to proactively implement systems for detecting synthetic AI content. This means that platforms such as social media, video platforms, and messaging apps must be legally required to: (1) implement continuously updated deepfake detection technology; (2) provide reporting mechanisms for synthetic content that are easily accessible to victims; (3) apply digital watermarks to legitimate synthetic content (Fathurrahim 2025).

The necessary legislative reform involves adding provisions to the revised ITE Law or the Criminal Code that explicitly establish platform liability regarding non-consensual AI-generated content. This model could draw on the UK's Online Safety Act 2023, which requires platforms to have proactive systems in place to identify and remove non-consensual intimate image deepfakes (Irawati 2025).

3.1.4 The Repressive Dimensions of the Criminalization of AI-Based Deepfake Pornography

The repressive dimension requires the creation of a specific criminal offense that accommodates the unique characteristics of AI-based deepfake crimes. The offense as formulated must include elements not found in conventional pornography laws: (1) the use of artificial intelligence technology or other digital methods in the creation of content; (2) the superimposition of the victim's visual identity without consent; (3) a sexual or exploitative purpose; and (4) distribution or the threat of distribution (Inna et al. 2025; Sy 2025).

Provisions should also be made for aggravating circumstances when the victim is a child or in a vulnerable situation, given that deepfake crimes against children constitute a form of sexual exploitation based on artificial intelligence technology in the creation of content, the use of the victim's visual identity without consent, for sexual purposes or exploitation, and the distribution or threat of distribution (Nadya et al. 2025).

This offense can be established either by amending the TPKS Law to include a provision specifically addressing AI-generated KBGO, or by adding a provision to Book II of the Criminal Code. It is also necessary to establish aggravating circumstances when the victim is a child or a woman in an unequal power dynamic, as well as when the content is disseminated on a massive scale. This approach is in line with the South Korean model, which has proven effective in reducing incidents while increasing victims' trust in the legal system (Irawati 2025).

3.1.4 The Restorative Dimension of Comprehensive Restoration of Victims' Rights

The restorative dimension is both the most critical and the most lacking component of the current Indonesian legal system. Based on the principles of Cyber Victimology (Jaishankar 2020), victim restoration must include four complementary elements.

First, mandatory content takedown: digital platforms must be legally required to remove non-consensual deepfake content within a maximum of 24–72 hours after a report from a verified victim, with significant administrative penalties for platforms that fail to comply. This mechanism can be implemented through an independent regulator (such as Australia's eSafety Commissioner model) granted enforcement authority. Second, an enforceable "right to be forgotten": victims must have an enforceable legal right to request the permanent removal of all replicas of the content from search engine indexes and platforms, with the burden of proof reversed onto the platforms. Third, comprehensive restitution: perpetrators must be required to pay restitution covering not only material damages but also psychological harm, recovery costs, and lost economic opportunities. Fourth, state-funded psychological rehabilitation: the state must guarantee victims' access to competent and free counseling and psychological rehabilitation services, with the duration tailored to the victims' needs (Kamaluddin et al. 2024; Yusuf et al. 2025).

3.1.4 Comparative Analysis with the Legal Systems of Other Countries

To strengthen the case for reformulation, **Table 3** presents a comparison of regulations on deepfake pornography in countries that have developed more comprehensive legal frameworks:

Table 3. Comparison of Regulations on Deepfake Pornography in Several Countries

Country	Research Instruments	Specific Offenses Related to AI/Deepfakes	Victim Redress Mechanisms	Relevance to Indonesia
South Korea	Act on Special Cases Concerning the Punishment of Sexual Crimes (2020 amend.)	Yes, explicitly criminalize non-consensual sexual deepfakes	Mandatory content removal; government-provided psychological support	Specific criminalization models that can be adapted
Australia	Online Safety Act 2021; Criminal Law Consolidation Act (SA)	Yes, image-based abuse includes AI-generated content	The eSafety Commissioner has the authority to order a takedown	Takedown mechanism based on an independent regulator
England	Online Safety Act 2023	Yes, non-consensual sexual deepfakes are criminalized	Platform obligations; restitution to victims	Relevant platform liability approaches
Indonesia	UU ITE, UU Pornography, UU TPKS, KUHP Baru	There is no specific offense related to deepfakes or AI	Limited to the TPKS Law; there are no AI-specific mechanisms	A regulatory gap that must be addressed immediately

The comparison in **Table 3** shows that South Korea, Australia, and the United Kingdom have moved beyond a general normative approach toward specific criminalization and operational victim restitution mechanisms. Indonesia, despite having more instruments in terms of quantity, lags behind in terms of the specificity of its norms and restorative mechanisms. This gap is not merely a technical legislative issue, but reflects a difference in paradigms: the legal systems of these countries have shifted from being offender-oriented to victim-centered, while Indonesia remains within the old paradigm (Darmawan, Junaidi, and Khaerudin 2025; Lewoba 2024)

The relevance of this comparison for Indonesia is selective and adaptive: it does not involve adopting other countries' models wholesale, but rather extracting principles that can be integrated into Indonesia's legal system while taking into account the sociocultural context, institutional capacity, and available digital infrastructure (Fauzyah, Hafidati, and Sunarya 2024).

4. CONCLUSION

Self-efficacy The novelty of this study lies in the integration of three contributions that have not previously appeared simultaneously in the Indonesian legal literature on deepfake pornography. The first contribution is paradigmatic: this study explicitly shifts the unit of analysis from the perpetrator to the victim, positioning the experience of digital victimization as the starting point rather than a side effect of the entire framework of legal protection. The second contribution is theoretical: the integration of Jaishankar's Cyber Victimology as a coherent academic subdiscipline into the analysis of Indonesian positive law opens the door for the development of criminal law studies that are more responsive to the characteristics of 21st-century digital crimes. The third contribution is normative prescriptive: the resulting three-tier

reformulation model is not merely a description of existing weaknesses but offers a concrete normative architecture with components that can be implemented through identified legislative channels.

The practical implications of this research operate on three levels. For legislators, this research provides a structured normative framework for developing amendments to the TPKS Law or adding specific offenses to the Criminal Code. For law enforcement officials, the analytical framework developed here offers guidance for more accurately classifying deepfake crimes within the existing normative framework. For victims and support organizations, the understanding of the characteristics of digital victimization generated by this study can strengthen their advocacy position in demanding rights to redress that have not yet been accommodated.

ACKNOWLEDGEMENTS

This study yields two fundamental findings. First, victims of AI-based deepfake pornography experience victimization that is permanent, multidimensional, and perpetually recurring exceeding the framework of conventional crime captured by Indonesian positive law. Revictimization does not end upon criminal conviction: so long as content remains accessible in digital space, the victim's cycle of suffering continues without limit. Indonesian positive law provides no specific offense for non-consensual AI-generated synthetic content, no legally enforceable take-down obligation, and no state guarantee of psychological rehabilitation a deficit exacerbated by the normative uncertainty introduced by the new Criminal Code's legislative transition.

Second, the three-tiered reformulation model developed in this study preventive (platform obligations and digital literacy), repressive (specific AI-based deepfake offense with aggravating circumstances), and restorative (mandatory take-down, right to be forgotten, comprehensive restitution, state-funded psychological rehabilitation) offers a victim-centred normative architecture implementable through identified legislative pathways, principally amendment of UU TPKS and addition of provisions in a revised ITE Law. Three priority steps are recommended: short term, issuance of a Technical Government Regulation under UU TPKS explicitly governing AI-based KBGO victim-recovery mechanisms; medium term, amendment of UU TPKS to criminalize non-consensual AI-generated sexual content with prescribed aggravating circumstances; and long term, development of comprehensive digital-security legislation integrating AI-crime victim protection as a coherent, unified normative framework, drawing selectively on the South Korean and Australian models. The limitation of this study is the scarcity of available judicial precedents; further empirical research on victims' direct experiences would enrich and validate the normative model formulated here.

REFERENCES

AlfaniRahman, Alif &, Doni Noviantama. 2025. “Deepfake: A Review from The Victimology Perspective.” 1(June):107–28.

Andira, Sindi Ayu, and M. Endriyo Susila. 2024. “Overcoming Deepfake Porn Crimes In Indonesia.” 23(1):2796–2809.

Ardiansyah, Khansa Farinda Khalishah Laely Wulandari Ruli. 2024. “Perlindungan Hukum Terhadap Perempuan Korban Balas Dendam Pornografi Dengan Mempergunakan Aplikasi ‘Deepfake’ Sebagai Kekerasan Berbasis Gender Online.” (62):1–14.

Aruan, Juandry. 2025. “Legal Protection for Victims of Photo Abuse through Artificial Intelligence Technology in Pornography Crimes in Indonesia.” 5(2):1831–62.

Aryawan, I. Putu Gede. 2026. “Kekosongan Norma Hukum Dalam Penanganan Deepfake Sebagai Alat Kejahatan Siber : Studi Yuridis Di Wilayah Polri Klungkung.” 2(April):295–307.

Darmawan, Muh Taufik, Amir Junaidi, and Ariy Khaerudin. 2025. “Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence Di Indonesia.” 18(01):42–54.

Fathurrahim, Nurhayati Chalil. 2025. “Legal Protection of Women’ s Dignity and Privacy From.” 6(12):1–28.

Fauzyah, Rizgita Nurul, Putri Hafidati, and Sunarya Sunarya. 2024. “Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence (Ai) DI Indonesia.” 3(November):74–88.

Geneva, The United Nations Office at. n.d. “‘Deepfake Abuse Is Abuse,’ UNICEF Warns _ The United Nations Office at Geneva.”

Hidayat, Izil Putra. 2024. “Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelegence (AI) Berupa Deepfake Porografi Menurut Peraturan Perunndang-Undangan.” Universitas Jambi.

Inna, Yurike, Rohmawati Ciptaningrum, Moh Muhlisin, I. Gede Widhiana Suarda, and Triana Ohoiwutun. 2025. “Kriminalisasi Deepfake Pornography Berbasis AI Dalam Perspektif.” 2:840–55.

Iqrar, Rini &. Alfian. 2026. “Perlindungan Hukum Korban Kejahatan Kecerdasan Buatan Dalam Bentuk Deepfake Porn Dari Perspektif Hukum Pidana.”

Irawati, Nurulhuda. 2025. "Pertanggungjawaban Pidana Terhadap Pelaku Deepfake Porn Berbasis Artifical Intelligence (Studi Perbandingan Pengaturan Di Indonesia Dengan Australia Dan Korea Selatan)." Universitas Andalas Padang.

Jaishankar, K. 2020. "Cyber Victimology : A New Sub-Discipline of the Twenty-First Century Victimology." 3–19.

Jateng.jppn. 2026. "Mahasiswa Undip Divonis 1 Tahun Penjara Dalam Kasus Video Deepfake Pornografi - JPNN."

Kamaluddin, Moh, Ratih Dwi Pangestu, Muhammad Darrin Zuhri, Universitas Mayjen, Sungkono Mojokerto, and Universitas Madura. 2024. "Perlindungan Hukum Korban Kejahatan Dalam Perspektif Viktimologi Dan Upaya Pemulihan Melalui Kompensasi." 9(1):33–42.

Kartadinata, Andriansyah. 2026. "Rekonstruksi Delik Pidana Dalam Kejahatan Deepfake : Tantangan Pembuktian Dan Perlindungan Korban." 36–48.

Komnas, Perempan. n.d. "Siaran Pers Komnas Perempuan Memperingati Hari Kebangkitan Teknologi Nasional 2025."

Lestari, Nabila Syahrani. 2024. "Kebijakan Formulasi Hukum Pidana Atas Praktik Deepfake Dilihat Dari Perspektif Kejahatan Siber Dan Pornografi."

Lewoba, Mira Aurela &. Kayus Kayowuan. 2024. "Pornografi Dalam Perspektif Viktimologi Mira Aurelita , Fakultas Hukum Universitas Pembangunan Nasional Veteran." 12(12):3382–96.

Mulyanti, Hayya Zafna Haefani&Asti Sri. 2025. "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." 12–26.

Nadya, Putu, Tasya Putri, Anak Agung, Ayu Ngurah, and Tini Rusmini. 2025. "Pengaturan Hukum Dalam Penanggulangan Deepfake Artificial Intelligence (AI) Terhadap Anak Sebagai Korban Kejahatan Siber Di Indonesia." 713–28. doi: 10.24843/JMHU.2025.v14.i03.p09.

Police, Indonesian National. n.d. "Deepfake Violence Against Women Soars_ UNDP Warns of 'Alarming AI Misuse' _ INP _ Indonesian National Police."

Pratiwi, Putri Fransiska Purnama. 2025. "Rekonstruksi Regulasi Perlindungan Hukum Terhadap Perempuan Korban Tindak Pidana Kekerasan Seksual Online Berlandaskan Keadilan." Universitas Islam Sultan Agung Semarang.

Rahardjo, Satjipto. 2014. Ilmu Hukum. edited by Awaludin Marwan. PT Citra Aditya Bakti.

Rahel Octora&, Priscilla Adi Wijaya Adriana Putri. 2025. "Harmonisasi Regulasi Penghapusan Konten Deepfake Pornografi Di Indonesia." 10844–55.

Rousay, Victoria. 2023. "Sexual Deepfakes and Image-Based Sexual Abuse : Victim-Survivor Experiences and Embodied Harms."

Soemitro, Ronny Hanitijo. 1990. "Ronny Hanitijo Soemitro, Metodologi Penelitian Hukum Dan Jurimetri (Bandung, 1990), Halaman 34 33." 33–37.

Sonia. 2025. "Pengaturan Tindak Pidana Deepfake Porn Artifical Intelegence (AI) Dalam Perspektif Peraturan Perundang-Undangan Di Indonesia." Universitas Jambi.

Sy, Muhammad Faturrachman. 2025. "DEEPFAKE PORNOGRAFI : STUDI KONSTITUSI DAN PENEGAKANNYA DI INDONESIA." 8(2):113–28.

Tempo. n.d. "Pelaku Konten Pornografi Di Semarang Divonis Setahun Penjara _ Tempo."

Tolosana, Ruben, Ruben Vera-rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-garcia. 2023. "DeepFakes and Beyond : A Survey of Face Manipulation and Fake Detection." 1–23.

Umbach, Rebecca, and Nicola Henry. n.d. Prevalence and Impacts of Image-Based Sexual Abuse Victimization : A Multinational Study. Vol. 1. Association for Computing Machinery.

Yusuf, Muhammad, Isa Pratama, Hanuring Ayu, Ardhani Putri, Yulian Dwi Nurwanti, Muhammad Yusuf, Isa Pratama, Muhammad Yusuf Isa, and Hanuring Ayu Ardhani. 2025. "The Urgency of Regulatory Accountability for Protecting Victims of Sexual Violence in Cyberspace Parallel with the Rising Incidence of Sexual Violence in Digital Spaces . According to the 2022 Annual Report of the National Commission on Violence Against Women , the Year 2021 Marked the Highest Number of Gender-Based Violence." 7(1):151–67. doi: 10.46924/jihk.v7i1.285.