Semarang State University
Undergraduate Law & Society Review
ISSN 2807-8225 (Print) 2807-8683 (Online)
Vol. 5 Issue 2 (2025) 1831-1862
DOI: https://doi.org/10.15294/lsr.v5i2.38347
Available online since: December 8, 2025

Legal Protection for Victims of Photo Abuse through Artificial Intelligence Technology in Pornography Crimes in Indonesia

Juandry Aruan [a]✉

[a] Faculty of Law, Universitas Negeri Semarang, Indonesia

✉ Corresponding email: *aruanjuandry@students.unnes.ac.id*

Abstract

The development of artificial intelligence (AI) technology has given birth to a new form of crime in the form of deepfake pornography, which is the production of sexual content that is digitally manipulated without the consent of the subject. This article discusses legal protection for victims of deepfake pornography in Indonesia through normative juridical approaches and case studies, particularly by highlighting the case of Udayana University students who produced deepfake content against dozens of female students. The results of the study show that Indonesia's positive law—through the Pornography Law, the ITE Law, and the TPKS Law—has not specifically regulated the crime of producing AI-engineered content, so law enforcement officials often have difficulty in ensnaring perpetrators optimally. In addition, technical constraints, weak digital forensic capacity, social stigma, and low digital literacy worsen the position of victims. This article recommends a reformulation of regulations that include explicit definitions of deepfake content, strengthening impact-based criminal sanctions, restitution for victims, national digital education, and the establishment of international cooperation through the ratification of the Budapest Convention. With a comprehensive legal approach and oriented towards victim protection, it is hoped that the Indonesian legal system will be able to answer the challenges of digital crime in the era of artificial intelligence.

KEYWORDS *Deepfakes, Digital Pornography, Artificial Intelligence, Legal Protection, Victim Restitution*

Introduction

In today's modern era, technology has become an indispensable part of human life. Rapid advances in technology have changed almost all aspects of life, especially since the emergence of the Industrial Revolution 4.0 or known as The Fourth Industrial Revolution. This concept refers to the major changes in the industrial world marked by the integration between digital technology, physical systems, and the internet in the production process. Angela Merkel, a German Chancellor, stated in 2014 that the Industrial Revolution 4.0 is a comprehensive transformation of all aspects of industrial production through the combination of digital technology and internet networks with traditional industries. This approach allows for the creation of a smarter and more integrated production system. The Industrial Revolution 4.0 also involves the implementation of the Cyber Physical System (CPS), which is a system in which the physical and virtual worlds are connected to each other in real-time through information networks. With this system, every component in the production process can be monitored, controlled, and optimized automatically and efficiently. Machines that are connected to each other are also able to work collaboratively with a high level of artificial intelligence. The ten main technologies that are pillars in the Industrial Revolution 4.0 include various innovations that play a major role in accelerating digital transformation in the industrial sector, including:

1. Internet of Things (IoT);

2. Big Data;
3. Artificial Intelligence (AI);
4. Cloud Computing;
5. Augmented Reality;
6. Additive Manufacturing (3D Printing);
7. Autonomous Robots;
8. Simulation;
9. Cyber Security; dan
10. Horizontal and Vertical System Integration.

These technologies not only revolutionize the way goods and services are produced, but also have a great influence on social, economic, and even legal interactions. One of the important aspects that is also affected by technological advances is the field of digital information and data security, especially related to the rampant use of artificial intelligence (AI) technology in daily life. AI has been used in various sectors such as education, transportation, health, and entertainment. However, in addition to providing great benefits, this technology also poses new challenges, especially in terms of misuse of personal data, including in the form of visual manipulation such as deepfakes. Deepfake pornography first emerged in late 2017 when a Reddit user manipulated the faces of Hollywood celebrities like Gal Gadot into explicit videos. The technology then spread to closed platforms such as Telegram and Discord, with 96% of the content targeting women. The Deeptrace report (2023) recorded a 550% increase in deepfake pornography cases since 2019, reaching 95,820 illegal videos in 2023.[1] In Indonesia, the latest case in 2025 involves students of Udayana University (Unud) who stole photos of 35 female students from Instagram and turned them into pornographic content using AI bots.[2] This case not only violates the privacy of victims, but also

[1] Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "The Urgency of Regulation of Deepfake Pornography in Indonesia," *Kertha Wicara: Jurnal Hukum* 13, no. 10 (2024): 530–541, doi:10.24843/KW.2024.v13.i10.p5

[2] "The Revelation of the Case of Deepfake Porn Content of Udayana University Students," *Spindle*, accessed May 19, 2025, https://kumparan.com/kumparannews/terungkapnya-kasus-konten-porno-deepfake-mahasiswi-unud-24xOaAR2Ntv/full.

reflects the vulnerability of the legal system in protecting the basic rights of individuals in the digital age.

Indonesian legal regulations, such as the Pornography Law and the ITE Law, are the main basis for handling digital pornography cases. Article 4 of the Pornography Law prohibits the creation, dissemination, or trade of pornographic content, while Article 27 Paragraph (1) of the ITE Law threatens criminal penalties for the dissemination of immoral content. However, these two regulations have structural weaknesses. The Pornography Act does not distinguish between original content and AI-engineered content, making it difficult to prove the element of "creation" of content.[3] Current regulations also emphasize more sanctions for perpetrators, but ignore the restitution or rehabilitation mechanism for victims. In addition, the ITE Law, which was last revised in 2016, has not accommodated manipulative technologies such as generative adversarial networks (GANs), which are the basis for deepfakes. A study by Solichah et al. (2023) confirms that 70% of deepfake pornography cases in Indonesia fail to be processed by law due to the absence of court-recognized digital evidence.[4] The absence of the Right To Be Forgotten in the Indonesian legal system also prolongs the suffering of victims, as illegal content can continue to circulate indefinitely.

Law enforcement against deepfake pornography crimes in Indonesia faces three main challenges. Starting from the limited technical capacity of the apparatus, the majority of law enforcement officials do not have the expertise to track the perpetrators on anonymous platforms such as Telegram or dark web forums. Digital footprint tracking is often hampered by data encryption and the use of virtual private networks (VPNs) by perpetrators. There is legal ambiguity, the Criminal Code and the ITE Law do not explicitly categorize deepfakes as specific criminal acts. For example, Article 310 of the Criminal Code on defamation only applies if the victim can prove the existence of an "*intention to degrade honor*",

[3] Rizgita Nurul Fauzyah, Putri Hafidati, and Sunarya, "Legal Protection for Victims of Artificial Intelligence-Based Deepfake Porn Videos in Indonesia," *Lex Veritatis* 3, no. 3 (2024): 74–88.

[4] Siti Nurjanah, "Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia," *International Journal of Multicultural and Multireligious Understanding* 10, no. 1 (2023): 1–13, doi:10.18415/ijmmu.v10i1.4409.

which is difficult to apply to AI-generated content. And also from social stigma, many victims are reluctant to report for fear of being ostracized or considered "provocative".

Victims of deepfake pornography face multidimensional impacts, ranging from psychological trauma, declining socio-economic reputation, to lack of access to legal assistance. A clear example can be seen in the case of a 2025 Udayana University student who lost a scholarship due to the spread of illegal content[5]. Victim protection requires a holistic approach that includes preventive, repressive, and curative aspects. Digital literacy education is needed to increase public awareness about the risks of sharing personal photos. On the legal side, revisions to the ITE Law and the Pornography Law are needed to include the definition of deepfakes, progressive criminal sanctions, and the obligation of digital platforms to verify content. The establishment of special institutions such as the Cyber Victim Support Center is also a solution to provide legal and psychological assistance.[6]

Considering the complexity of the threat posed by the misuse of Artificial Intelligence technology in the form of non-consensual pornographic content, as well as the weak legal protection for victims in Indonesia, an in-depth legal study is needed to examine the extent to which positive laws in Indonesia are able to provide effective protection for victims. In addition, it is also important to identify various obstacles faced in the law enforcement process, both in terms of legal substance, law enforcement apparatus, and socio-cultural aspects that affect the courage of victims in reporting. Based on this background, this research is directed to answer two main problems, namely (1) How does positive law in Indonesia regulate the protection of victims of photo abuse using Artificial Intelligence in pornographic crimes? (2) What are the obstacles and efforts of law enforcement in providing protection to victims of these crimes?

[5] KOMPAS, "Udayana University Bali Students Suspected of Creating AI-Based Fake Porn Content," Kompas.com, April 25, 2025, https://denpasar.kompas.com/read/2025/04/25/131021978/mahasiswa-universitas-udayana-bali-diduga-bikin-konten-porno-palsu-berbasis.

[6] Cindy Natalia and I Wayan Bela Siki Layang, "Legal Protection for Victims of Deepfake Pornography in the Context of Indonesian Law," *Kertha Semaya* 12, no. 5 (2024): 4462–4473.

Method

This research uses a qualitative approach with a type of normative (doctrinal) juridical law research. This approach was chosen to comprehensively examine the legal dynamics that arise in the case of photo abuse based on Artificial Intelligence (AI) technology, especially in relation to pornographic crimes in Indonesia. Normative juridical research relies on the analysis of legal norms contained in laws and regulations, legal doctrines, court decisions, and relevant legal principles.[7] This normative juridical approach examines law as a system of norms that is prescriptive. The focus lies on the evaluation of Indonesia's positive legal provisions, such as Law Number 44 of 2008 concerning Pornography, Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and its amendments, as well as relevant provisions in the Criminal Code (KUHP). In addition, a review of various court decisions, implementing regulations, and policy documents related to information technology-based crimes was conducted.

Secondary data is the main source in this study and is obtained through library research, which includes primary, secondary, and tertiary legal materials. Primary legal materials include applicable laws and regulations, while secondary legal materials are in the form of legal literature, results of previous research, and scientific articles both nationally and internationally that discuss the phenomenon of deepfake pornography, cybercrime regulations, and protection for victims of digital crime. Tertiary legal materials in the form of legal dictionaries, encyclopedias, and other supporting references are used to strengthen conceptual understanding. Data analysis is carried out in a thematic manner, namely by identifying and categorizing key legal issues, such as regulatory loopholes, challenges in law enforcement, and normative implications for victim protection. This analysis aims to uncover the consistency and inconsistency between written legal norms and implementation in the field.

[7] Zainal Arifin Hoesein, *Metode Penelitian Hukum Normatif dan Empiris* (Jakarta: Prenada Media, 2020), 24–27.

Positive Legal Protections in Protecting Victims Against Photo Misuse Using Artificial Intelligence in Pornographic Crimes

In recent decades, the advancement of digital technology has experienced very rapid development and has a direct impact on various aspects of human life. One of the biggest breakthroughs in this field is the presence of artificial intelligence (AI), which has now been widely applied in the industrial, educational, economic, health, and legal systems. AI is designed to mimic the way humans think through data processing, pattern recognition, and automated decision-making. Its presence brings efficiency and convenience in various fields, but on the other hand it also raises new concerns, especially when this technology is used for adverse purposes. One form of deviation that emerges is the use of AI in producing fake or deepfake digital content, which is the manipulation of photos and videos realistically to resemble certain individuals, without the consent or direct involvement of the person displayed.[8]

One form of AI abuse that is now a serious concern is the phenomenon of deepfakes, especially in the form of deepfake pornography. Deepfakes are the result of digital engineering that utilizes deep learning technology and generative adversarial networks (GANs) to create visual or audio content that is very similar to the original, making it difficult for ordinary humans to distinguish.[9] In the case of deepfake pornography, AI is used to attach a person's face to another person's body in a pornographic video or image, making it as if the individual is involved in a scene that was never actually done. This phenomenon not only raises serious problems related to the privacy and dignity of individuals, but also

[8] Olivia Novera and Yenny Fitri Z., "Analysis of Criminal Law Arrangements on the Abuse of Image Manipulation Technology (Deepfake) in the Dissemination of Pornographic Content Through Social Media Accounts," *El-Faqih: Journal of Islamic Thought and Law* 10, no. 2 (2024): 460–474, doi:10.58401/faqih.v10i2.1539

[9] Raihani Latifatunnisa and Made Wira Yudha, "The Urgency of Regulatory Reform in Tackling the Misuse of Artificial Intelligence and Deepfake Technology in Indonesia: Perspectives on the Protection of Privacy Rights," *Causa: Journal of Law and Citizenship* 11, no. 1 (2025): 21–30, doi:10.3783/causa.v11i1.11617

has the potential to become a tool of crime that damages the reputation and psychology of the victim. The spread of deepfake pornography is a major challenge for law enforcement, as this technology is developing very quickly and is difficult to detect conventionally. Therefore, an adaptive legal approach and cross-disciplinary collaboration are needed to address the negative impact of the abuse of AI in the realm of pornography, while ensuring that technological advances remain within the ethical and legal corridors that protect human rights.

The deepfake phenomenon is a real example of how technology can transcend ethical and legal boundaries. When this technology is used to create pornographic content that drags a person's name and face illegally, it raises serious problems in the realm of legal protection of individual privacy, dignity, and reputation. Therefore, it is important to understand the development of AI not only from its technological aspects, but also from its potential misuse that can disrupt legal order and social justice in the digital age. The deepfake phenomenon allows the manipulation of a person's face into pornographic content in a very realistic manner without the consent of the individual. In the context of Indonesian law, the protection of victims of AI image abuse still depends on general legal instruments, such as the Pornography Law, the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and the Criminal Code, but it does not explicitly regulate forms of technology-based crimes such as deepfakes.

A. Regulations Related to Pornography and Digital Crime

Law Number 44 of 2008 concerning Pornography (Pornography Law) is the main legal framework in regulating the crime of pornography in Indonesia. Article 4 of this Act expressly prohibits any person from producing, creating, reproducing, duplicating, disseminating or providing pornography in any form, including digital content that contains sexually exploitative or obscene content. The definition of "*pornography*" in Article 1 encompasses a wide range of media, such as moving images, animations, or gestures, which can be implicitly interpreted to include digital content.

However, this law does not explicitly mention digital engineering technologies such as deepfakes or artificial intelligence (AI), thus creating ambiguity in law enforcement.[10] In practice, the absence of specific clauses on AI engineering makes it difficult for law enforcement officials to classify deepfake pornography as a standalone crime. For example, in the case of the misuse of photos of Udayana University students (2025), the judge must carry out an extensive interpretation of Article 4 to ensnare the perpetrator, even though the element of "digital content creation" is not clearly regulated. This limitation is exacerbated by the formulation of the element of delicacy that requires proof of "intention to commercialize" or "disseminate widely". As a result, perpetrators who create deepfake content for personal consumption are difficult to be caught, while victims have difficulty getting justice. The Pornography Law broadly defines pornography as any form of message through the media or public performances that contain obscene content. While this definition can technically include digital content, the absence of explicit mention of AI technology or deepfakes creates legal uncertainty. Many cases fall into gray areas, such as the difficulty of proving the perpetrator's "malicious intent" when content is uploaded anonymously on a closed platform. For example, in the case of deepfakes targeting Indonesian celebrities (2024), the authorities have difficulty distinguishing between AI-engineered content and conventional content, because the law does not provide clear technical criteria. Although Article 4 paragraph (1) of the Pornography Law can be interpreted to ensnare deepfakes as "creators" of pornography, the evidentiary challenge remains great. According to Haida & Nuriyatman (2024), a revision of this law is needed to include the definition of "digitally engineered content" and expand the scope of criminal offenses, including the production of AI content without the victim's consent.[11] This update must be accompanied by sanctions that

[10] Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "The Urgency of Regulation of Deepfake Pornography in Indonesia," *Kertha Wicara: Journal of Law* 13, no. 10 (2024): 530–541, doi:10.24843/KW.2024.v13.i10.p5

[11] Haida Fadhilah and Dedy Nuriyatman, "The Norm Gap for the Production of Deepfake Pornography in Indonesia: A Review of the ITE Law and the Pornography Law," *Journal of Law and Criminology 9, no. 1* (2024): 101–117, doi:10.31849/respublica.v24i01.23327.

take into account the more massive psychological and social impact of deepfakes than conventional pornography. Thus, although the Pornography Act is a relevant legal basis, its approach is still too generic and unresponsive to technological developments. Amendments are needed to accommodate the complexity of digital crime, including the right to be forgotten removal mechanism and digital platform verification obligations.[12] Without these steps, victims of deepfake pornography will continue to face systemic injustices amid rapid technological advancements.

The Electronic Information and Transaction Law (UU ITE) Number 19 of 2016 is an important instrument in regulating cybercrime, including the spread of digital pornographic content. Article 27 Paragraph (1) of the ITE Law explicitly prohibits everyone from distributing, transmitting, or making accessible information or electronic documents that contain immoral content. In the context of deepfake pornography, this article is used as a legal basis to ensnare perpetrators of the dissemination of illegal content, such as the case of manipulating public photos into explicit content targeting public figures. However, the ITE Law has a crucial structural flaw in that there are no provisions that specifically regulate the production of illegal AI engineering content. Perpetrators who only create deepfakes without spreading them cannot be charged under this law, thus creating a legal loophole that is used to avoid criminal liability. The main weakness lies in the formulation of the delicacy element of Article 27 Paragraph (1) which focuses more on "distribution" than "production" of content. In practice, content that has been created but has not been disseminated does not fall within the scope of the crime, even though the creation process itself has violated the privacy and rights of the victim. For example, in the case of deepfakes targeting female students in Jakarta (2024), law enforcement officials were only able to ensnare content spreaders, while the creators escaped legal bondage due to the absence of an article criminalizing the production of

[12] Linda Astuti, Wiwit Ariyani, dan Bayu Aryanto, "Urgency Right to Be Forgotten as a Legal Protection for Deepfake Pornography Victims by Artificial Intelligence Technology in Social Media," *International Journal of Law, Government and Communication* 9, no. 37 (2024): 45–58, doi:10.35631/IJLGC.937006.

AI content.[13] This reflects the inability of the ITE Law to accommodate the dynamics of modern digital crime, where the production of illegal content—although not yet disseminated—has caused psychological and social harm to victims. Another challenge arises from the lack of a legal definition of AI-based digital engineering. Law enforcement officials often get caught up in subjective interpretations of categorizing deepfakes as "*immoral content*," especially when they don't involve conventional sexual exploitation. Academics such as Haida & Nuriyatman (2024) emphasize the need for amendments to the ITE Law to include elements of "*digital engineering content creation*" as an independent criminal offense, accompanied by an explicit definition of deepfakes and sanctions that consider the holistic impact on victims.[14]

Law Number 12 of 2022 concerning the Crime of Sexual Violence (TPKS Law) is a progressive legal breakthrough that recognizes electronic-based sexual violence, including the dissemination of non-consensual pornographic content. Article 5 of the TPKS Law explicitly stipulates that any person who distributes intimate recordings or images without the victim's consent can be sentenced to a maximum of 10 years in prison. This provision is particularly relevant in the context of deepfake pornography, especially when the victim's face is affixed to another person's body in explicit content, as in the case of the widespread manipulation of photos of women or children on social media platforms. The advantage of this law lies in the victim-centered approach, which guarantees the victim's right to request the removal of illegal content, financial restitution, and psychological and medical recovery through the mechanisms stipulated in Articles 10 to 15. Although the TPKS Law provides comprehensive legal recognition, its implementation in the field still faces significant obstacles. Starting from the technical capacity of law

[13] Angelica Vanessa Audrey Nasution, Suteki Suteki, and Anggita Doramia Lumbanraja, "Prospects for Fulfilling the Right to Be Forgotten for Victims of Deepfake Pornography Due to Artificial Intelligence Abuse in Indonesia," *Diponegoro Law Journal* 13, no. 2 (2024): 150–165.

[14] Haida Fadhilah and Dedy Nuriyatman, "The Norm Gap for the Production of Deepfake Pornography in Indonesia: A Review of the ITE Law and the Pornography Law," *Journal of Law and Criminology* 9, no. 1 (2024): 101–117, doi:10.31849/respublica.v24i01.23327.

enforcement officials in identifying and removing deepfake content is still limited. Many members of the police and prosecutor's offices do not understand the technical characteristics of AI-engineered content, such as the use of generative adversarial networks (GANs) algorithms, so they often consider the content to be the result of victim consent or conventional engineering. Social stigma and the victim's ignorance of legal rights are the main barriers to reporting. And also, the availability of integrated recovery services is still minimal. Only 30% of regions in Indonesia have specific psychological and legal services for victims of digital violence, while mechanisms for removing illegal content are often slow due to suboptimal coordination between digital platforms and the authorities.[15] To overcome these challenges, strategic steps are needed, such as technical training of the apparatus in digital evidence analysis, legal literacy campaigns to increase victim awareness, and the establishment of a Cyber Victim Support Center that provides holistic assistance. By strengthening the synergy between the TPKS Law, the ITE Law, and the Pornography Law, Indonesia can create a victim protection system that is responsive to the dynamics of AI-based digital crime.

B. Legal Gaps in AI and Deepfake Settings

In reality, Indonesian regulations still show a lack of definition regarding digital manipulation technology such as deepfakes, because Law Number 44 of 2008 concerning Pornography only contains the definition of pornography as *"... photographs, writings, sounds, sounds, moving images..."* without mentioning digital engineering technologies such as Generative Adversarial Networks that produce hyper-realistic content, as well as Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) article 27 prohibiting the dissemination of content that violates morality does not discuss aspects of AI engineering. As a result, in the case of deepfake pornography of Udayana University students (2025), the PPKS Task Force (Task Force for the Prevention and

[15] Angelica Vanessa Audrey Nasution, Suteki Suteki, and Anggita Doramia Lumbanraja, "Prospects for Fulfilling the Right to Be Forgotten for Victims of Deepfake Pornography Due to Artificial Intelligence Abuse in Indonesia," *Diponegoro Law Journal* 13, no. 2 (2024): 150–165.

Handling of Sexual Violence) has difficulty categorizing fabricated content as "pornography" because there is no legal definition that specifically accommodates AI manipulation[16]. In addition, the ambiguity of the criminal element is even more complicated, because the New Criminal Code (Law No. 1 of 2023) Articles 433–435 require proof of "intent to degrade honor" (*opzettelijk*) as the main element, even though the identity and motives of deepfakes are often hidden behind anonymous accounts and VPNs—as happened in the spread of celebrity deepfakes in 2024—so that it is easier for the authorities to rely on Article 27A ITE or defamation of Article 310 of the Criminal Code, which is general and not specific Regulating digital engineering.

Furthermore, Indonesia's regulations are somewhat less adaptive to the pace of AI innovation, the ITE Law was last revised in 2024, never specifically anticipating the emergence of deepfakes, machine learning, or neural networks, while in many other countries, such as the United Kingdom, in the Crime and Policing Bill (2025) will criminalize the creation and dissemination of non-consensual pornography deepfakes with a threat of two years in prison.[17] This creates a legal vacuum where perpetrators are free to experiment without proportionate legal risk, while victims are forced to take legal analogy paths that are not designed to handle the complexity of digital evidence, such as metadata or digital footprint, as well as the lack of psychological recovery protection and personal data.

[16] ANTARA News, "Udayana University Investigates Case of Alleged Online Sexual Harassment," Antara News, accessed on May 23, 2025, https://www.antaranews.com/berita/4802537/universitas-udayana-investigasi-kasus-dugaan-pelecehan-seksual-daring.

[17] United Kingdom, *Crime and Policing Bill 2025*, HC Bill (2025) 123, Parliament of the United Kingdom, diakses pada 19 Mei 2025, https://bills.parliament.uk/bills/3123.

C. Case Studies as a Reflection of Legal Gaps: Deepfake Case Analysis at Udayana University (2025)

In 2025, the case of the misuse of photos of 35 female students of Udayana University (Udayana University) to create pornographic deepfake content through an AI bot[18] on Telegram highlights Indonesia's legal unpreparedness in dealing with artificial intelligence (AI)-based digital crimes. The perpetrator (with the initials SLKDP) used photos from the victim's Instagram account to engineer an explicit video which was then spread in a closed group chat. Although the authorities managed to arrest the perpetrators under Article 4 of the Pornography Law and Article 27 Paragraph (1) of the ITE Law, the legal process faced significant challenges from the unsynchronization of the Pornography Law with digital evidence as seen from the absence of an explicit clause on AI engineering, forcing judges to use broad interpretations to categorize deepfakes as "pornography-making". The limited evidence makes it difficult for forensic teams to track the digital footprint of the perpetrators because the content is uploaded through overseas servers and encrypted, so proving "malicious intent" relies only on the metadata of a legally weak fake Telegram account. The sanction received by the perpetrator was officially issued from Udayana University which had been confirmed by the campus. The perpetrator should have been sentenced to 2 years in prison, but this sanction was also considered disproportionate to the psychological impact experienced by the victim. From initially reporting 35 female students as victims, an in-depth investigation found a total of about 37 victims in this case. Some suffer from severe depression and drop out, while illegal content continues to circulate on closed platforms.

According to Haida & Nuriyatman (2024), the revision of the Pornography Law to include the definition of "*digitally engineered content*"

[18] Metro TV. *A student who has been accused of sexually abusing child pornography*, YouTube video, 2:20, April 27, 2025, https://www.youtube.com/watch?v=QIIH3DBgt9U, accessed May 19, 2025.

and the imposition of sanctions is urgent.[19] Without this step, Indonesia will continue to lag behind in protecting victims' rights in an era of exponentially developing technology. Within the framework of Satjipto Rahardjo's theory of legal protection, the law is not just a collection of rigid norms, but becomes a vital instrument to provide protection and empowerment to those in vulnerable positions, including victims of deepfake pornography. Rahardjo emphasized that true legal protection requires the state to proactively present norms that are responsive to social and technological changes.[20] But in practice, Indonesia's positive law—through the Pornography Law and the ITE Law—still suffers from a lack of definitions regarding AI-engineered content, so victims do not find an adequate "legal umbrella" to demand the restoration of rights and justice. This condition encapsulates the victim in uncertainty, because the existing norm only regulates the distribution of obscene content, not the production of digitally engineered content that undermines the dignity and human rights of individuals.

From Rahardjo's perspective, the function of law must be progressive, by placing substantive justice above normative formalities. This means that when deepfake technology produces pornographic content without the subject's consent, the state is obliged to fill the regulatory gap—for example by adding a special article on "illegal production of AI-engineered content"—because an undeveloped law will fail to perform its function as a tool to liberate victims from a series of psychological and social sufferings. Furthermore, Rahardjo's theory emphasizes the importance of strengthening the capacity of law enforcement officials and empowering victims through a rapid restitution mechanism, so that legal protection is not just a promise on paper, but a reality that is directly felt by victims in the field. This analysis shows how far Indonesia's positive law must be improved to match the spirit of *rechtssociologie* that Rahardjo carries—which is to humanize the law and

[19] Haida Fadhilah and Dedy Nuriyatman, "The Norm Gap for the Production of Deepfake Pornography in Indonesia: A Review of the ITE Law and the Pornography Law," *Journal of Law and Criminology* 9, no. 1 (2024): 101–117, doi:10.31849/respublica.v24i01.23327.

[20] Satjipto Rahardjo, *Legal Science: The New Paradigm and Its Development Dynamics* (Yogyakarta: Genta, 2020), pp. 87–89.

make it a "friend" to victims of deepfake pornography, not an "enemy" that shackles them in a long process without certainty. Without regulatory reforms that include explicit definitions of deepfakes and victim-centric mechanisms, the law will continue to lose relevance and fail to realize the ideals of social justice for every citizen.

Obstacles and Enforcement Efforts of Deepfake Pornography

A. Law Enforcement Obstacles

1. *Technical Constraints*

In practice, the technical capacity of Indonesian law enforcement officials in handling deepfake pornography cases is still very limited, where most members of the police and prosecutor's office have not received adequate training to use advanced digital forensic tools such as AI-based deepfake detection devices and blockchain-based tracking software. As an illustration, in the case of the spread of deepfakes by Universitas Airlangga (2024), investigators had difficulty identifying the digital footprint of the perpetrators because the content was uploaded through closed platforms such as Telegram—where the end-to-end encryption function is only available on "Secret Chats" that are not active by default—as well as through dark web networks that use advanced anonymization protocols.[21]

The Telegram app requires manual activation for end-to-end encryption features, so many conversations remain vulnerable to interception and investigations are hampered due to a lack of cooperation and transparency from the platform provider. In addition, the use of end-to-end encryption and anonymity techniques on the dark web substantially hampered electronic evidence attribution and collection, forcing authorities to rely on conventional methods that were often inadequate. This obstacle is exacerbated by the lack of budget for the

[21] Rizgita Nurul Fauzyah, Putri Hafidati, and Sunarya, "Legal Protection for Victims of Artificial Intelligence-Based Deepfake Porn Videos in Indonesia," *Lex Veritatis* 3, no. 3 (2024): 74–88.

procurement of deepfake detection software licenses and digital forensic infrastructure in cybercrime units, so that purchase priorities often fall on daily operational needs rather than cutting-edge investigative technology. Meanwhile, illegal content can spread to thousands of users in minutes through closed groups and cloud-based channels, making it nearly impossible to take down and recover victim data if it relies on the internal capacity of state institutions. This uneven technical condition not only slows down the law enforcement process, but also prolongs the psychological suffering of victims, underscoring the urgency of fulfilling investments in digital forensic training, increasing technology budgets, and cross-sector collaboration between law enforcement, academia, and the technology industry.

2. Regulatory Constraints

In Indonesia's positive legal framework, Article 27 paragraph (1) of the ITE Law only criminalizes the activity of "distributing, transmitting, and/or making accessible Electronic Information and/or Electronic Documents that have content that violates morality" without touching the act of producing content independently. This provision ensnares only disseminators or distributors—with a maximum penalty of six years in prison and/or a fine of up to one billion rupiah—while illegal AI content producers who do not distribute them are completely exempt from the law. The vacuum of the norm opens a loophole for deepfakes to assemble non-consensual pornographic material without fear of being punished, as long as they hold the content privately. Similarly, the Pornography Law of 2008 focuses only on the production and circulation of "conventional" material and has never been revised to accommodate the dynamics of generative AI technology.[22]

Meanwhile, the proposed revision of the second ITE Law and the Pornography Law in Indonesia is still wallowing in the meetings of the special committee of the House of Representatives, without a single draft

[22] Haida Fadhilah and Dedy Nuriyatman, "The Norm Gap for the Production of Deepfake Pornography in Indonesia: A Review of the ITE Law and the Pornography Law," Journal of Law and Criminology 9, no. 1 (2024): 101–117, doi:10.31849/respublica.v24i01.23327.

containing an explicit article on AI crimes until mid-2025.[23] This legislative delay has serious implications for victim protection, as the room for takedown and restoration of victims' civil rights is practically closed by a loophole. Legal academics and policy think tanks highlight this stagnation as evidence of "lost momentum" that confirms that without an AI-based digital crime article, Indonesia will be left behind in prevention efforts and strict sanctions against deepfake pornography perpetrators. Failure to impose sanctions on deepfake manufacturers and a slow legislative response created a regulatory deficit that not only weakened law enforcement, but also left victims without effective access to seek justice.

3. Social Constraints

In the context of deepfake pornography, social stigma traps victims in a dilemma between seeking justice and maintaining a good name, so the phenomenon of victim-blaming—in which victims are blamed as if their actions provoked a crime—further exacerbates the reluctance to report. Sabillah's study (2022) shows that the view of society that considers victims responsible for sexual harassment gives rise to the effect of "*family disgrace*" that pressures victims to remain silent.[24] The INFID qualitative survey found that up to 93% of victims of sexual violence are reluctant to report because of stigma and concerns of being humiliated.[25] In the case of deepfake pornography, the impact of trauma is not only psychological but the victim also experiences social exclusion and loss of confidence – a phenomenon recorded in the research of Aurelita et al. (2024) on the victimization of women in deepfakes.

This condition reflects a large knowledge gap about the risks of deepfakes and reporting procedures, where most victims are unaware that manipulation of their faces is a criminal offence or do not know how to

[23] Angelica Vanessa Audrey Nasution, Suteki Suteki, and Anggita Doramia Lumbanraja, "Prospects for Fulfilling the Right to Be Forgotten for Victims of Deepfake Pornography Due to Artificial Intelligence Abuse in Indonesia," *Diponegoro Law Journal* 13, no. 2 (2024): 150–165.

[24] Wina Sabillah, "Social Stigma of Victims of Sexual Violence and Its Impact on Victim Psychology," *Journal of Social and Humanities* 10, no. 1 (2022): 15–25.

[25] INFID (International NGO Forum on Indonesian Development), Report on Sexual Violence in the Digital Space (Jakarta: INFID, 2023).

access legal aid. In fact, global research reveals that the public in general is not confident in detecting deepfakes and has little understanding of the legal consequences. Thus, social barriers for victims of deepfake pornography lie not only in fear of stigma and victim-blaming, but also in the low digital literacy and laws that hinder access to justice. Without interventions in the form of legal awareness campaigns, digital literacy enhancement, and efforts to remove stigma, victims will continue to be confined in silence and helplessness.

B. Law Enforcement Efforts That Can Be Developed

The initial effort is of course to revise existing regulations by including the Definitions of "*AI Engineered Content*" and "*Deepfake*" in the Pornography Law and the ITE Law. Currently, the Pornography Law and the ITE Law do not contain specific terminology related to AI engineering content or deepfakes, so the authorities often have to use analogous interpretations that are vulnerable to formal and material lawsuits. Therefore, it is necessary to add explicit definitions in both laws, for example: "*Pornographic content includes any form of digital engineering, including the manipulation of photos, videos, or audio using AI (deepfake) technology, created without the subject's consent.*"

Article 27 paragraph (1) of the ITE Law must be expanded to include "*production of illegal AI engineering content*" as a standalone criminal offense—regardless of its spread—so that deepfake creators can be processed from the production stage. Thus, law enforcement officials obtain a stronger normative basis to ensnare perpetrators directly, rather than just focusing on content spreaders.

Indonesia has not ratified the Convention on Cybercrime (Budapest Convention) to date, even though this convention provides a comprehensive digital investigation framework, including a preservation of evidence mechanism (Article 16) and mutual legal assistance between countries.[26] Ratification will allow officials such as the National Police to

[26] Raihani Latifatunnisa and Made Wira Yudha, "The Urgency of Regulatory Reform in Tackling the Misuse of Artificial Intelligence and Deepfake Technology in

quickly request data from foreign service providers and track the digital footprint of perpetrators who use servers or platforms abroad. The Budapest Convention will also encourage cross-border cooperation in the collection of electronic evidence, so that deepfake pornography investigations involving platforms with advanced encryption or servers in different jurisdictions can be more effective—for example through Interpol channels or mutual legal assistance treaties.[27] By combining these principles, Indonesia will strengthen access to critical information from other countries and enhance the technical capacity of the apparatus through joint training and exchange of digital forensic expertise.

Law enforcement officials in Indonesia need a structured and sustainable skill-based learning digital forensic training program to keep pace with the complexity of deepfake pornography crimes. The Study on the Role of the Police in Deepfake Pornography Crime confirms that there is still a shortage of trained human resources and cutting-edge forensic equipment in the National Police's cybercrime unit, making it difficult for investigators to verify the authenticity of AI-engineered content.[28] Udayana University's "Legal Protection for Victims of Deepfake Pornography" report recommends the integration of digital forensic training in the police and prosecutor's education curriculum, in collaboration with technology institutions such as ITB and BSSN for AI detection tools and blockchain tracing software.[29] In comparison, the Singapore Police, through its AI for Safer Children initiative, has conducted regional training involving simulating deepfake cases and

Indonesia: Perspectives on the Protection of Privacy Rights," *Causa: Journal of Law and Citizenship* 11, no. 1 (2025): 21–30, doi:10.3783/causa.v11i1.11617.

[27] Angelica Vanessa Audrey Nasution, Suteki Suteki, and Anggita Doramia Lumbanraja, "Prospects for the Fulfillment of the Right to Be Forgotten for Victims of Deepfake Pornography Due to Artificial Intelligence Abuse in Indonesia," *Diponegoro Law Journal* 13, no. 2 (2024): 150–165.

[28] Thessaloniki Liony Polandos, Wenly R. J. Lolong, and Merry Lenda Kumajas, "Criminal Accountability of Deepfake Porn Perpetrators Using Artificial Intelligence (AI)," *Journal of Rectum: A Juridical Review of Criminal Handling* 7, no. 2 (2025): 217–224, doi:10.46930/jurnalrectum.v7i2.5618.

[29] Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "The Urgency of Regulation of Deepfake Pornography in Indonesia," *Kertha Wicara: Journal of Legal Studies* 13, no. 10 (2024): 530–541, doi:10.24843/KW.2024.v13.i10.p5.

practicing using tools such as Deepware Scanner and Microsoft Video Authenticator to trace traces of video manipulation.[30] The adaptation of this model in Indonesia—for example through the cooperation of UNICRI, BSSN, and technology campuses—will improve the ability of investigators to uncover and document deepfake evidence, as well as speed up the takedown and prosecution process.

Digital literacy about deepfakes in Indonesia is still low, around 32% of the public understands the risks and ways to identify AI-manipulated content. This figure was obtained from the 2024 Kominfo Digital Literacy Index, which also noted that almost 70% of respondents did not recognize the difference between original and deepfake videos.[31] To close the gap, the government needs to launch a national social media-based campaign with the theme of #HapusDeepfake targeting vulnerable groups—adolescents and women—through short video content, infographics, and interactive dialogues. Campaign materials should include practical guidance, such as checking for lighting inconsistencies or lip movement synchronization, as well as highlighting real-life case examples such as the abuse of AI in 37 female students at Udayana University. In addition, educational modules can be developed in collaboration with institutions such as BSSN and universities (UGM, UNUD) for socialization in schools and campuses. Legal measures that must be socialized include reporting procedures to the police and alternative channels through the SAPA 129 hotline under the Ministry of PPPA, which has been proven effective in accommodating reports of violence against women and children.[32] Large platform providers (Meta, Google) can also be involved to deliver campaign materials to their users, so that the scope of education becomes wider.

[30] United Nations Interregional Crime and Justice Research Institute (UNICRI), AI for Safer Children, UNICRI, diakses pada 22 Mei 2025, https://unicri.org/topics/AI-for-Safer-Children.

[31] Ministry of Communication and Information of the Republic of Indonesia, Indonesian Digital Literacy Status 2022, 2022, https://aptika.kominfo.go.id/wp-content/uploads/2023/02/Report_Nasional_2022_FA_3101.pdf.

[32] Ministry of Women's Empowerment and Child Protection of the Republic of Indonesia, "SAPA 129," accessed May 24, 2025, https://www.kemenpppa.go.id/page/view/NDgzNg%3D%3D.

In Indonesia, services are needed that are integrated with the Sexual Violence Reporting and Handling System (SPPK) under the Ministry of PPPA, using hotline number 129 (SAPA 129) and WhatsApp 08111-129-129. This hotline must be equipped with a mobile application to upload digital evidence (video/photo files), as well as a triage system to channel cases to the National Police Criminal Investigation Branch or cybercrime unit at the local Police. In addition to the official route, the National Police's cyber patrol (Directorate of Cyber Crime Bareskrim) needs to open a direct complaint channel on social media platforms and digital community forums, so that victims who are not familiar with formal procedures can still report easily.[33] With the combination of literacy campaigns and responsive hotlines, the community not only became more vigilant, but victims also gained quick access to justice and protection.

C. Recommendations for Profit Policy for Handling Deepfake Pornography in Indonesia

It is necessary to design a "*Digital Sexual Crime Prevention Act*" similar to South Korea, which contains a penalty of 5-12 years in prison for the production of deepfake pornography, without the need for proof of distribution.[34] This law must accommodate the element of intent (*mens rea*) and regulate a mechanism for quick takedown and restitution for victims.

Indonesia must also immediately emulate Chinese regulations with the increasing cases of deepfakes circulating, all AI-based synthetic content must be watermarked or labeled "AI-engineered content" so that users can distinguish which is real or the result of manipulation.[35] This obligation

[33] Directorate of Cyber Crimes of the Criminal Investigation Branch of the National Police, "Cyber Patrol," accessed May 24, 2025, https://patrolisiber.id/contact-us/.

[34] "South Korea to criminalise watching or possessing sexually explicit deepfakes," Reuters, September 26, 2024, https://www.reuters.com/world/asia-pacific/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes-2024-09-26/.

[35] Venkateswarlu Sunkari dan Ayyagari Sri Nagesh "Artificial Intelligence for Deepfake Detection: Systematic Review and Impact Analysis,"*International Journal*

applies to platform providers and individuals, with administrative and criminal sanctions for those who ignore the provisions. Apart from the watermark, it is also necessary to form a special cyber unit under the National Police Criminal Investigation Branch which is specialized in handling deepfake cases, equipped with digital forensic tools such as EnCase, FTK, and Autopsy, as well as a team of programming experts (Python, SQL) to examine the source code and metadata of content.[36] The unit must also have real-time monitoring capacity and integration with a feedback loop system that allows for continuous improvement of detection methods. The existence of this unit is expected to shorten the chain of investigations, improve the accuracy of perpetrator attribution, and strengthen electronic evidence in the judicial process.

Meanwhile, in an effort to establish criminal sanctions commensurate with the psycho-social and reputational impact experienced by victims of deepfake pornography, Indonesia can emulate several jurisdictions that have implemented progressive schemes. For example, Massachusetts in An Act to Prevent Abuse and Exploitation imposes criminal penalties of up to two and a half years in prison and a maximum fine of $10,000 for non-consensual deepfake pornography perpetrators of the first offense, with increased penalties of up to $15,000 and imprisonment of up to ten years for repeated offenses.[37] In California, Assembly Bill No. 602 grants victims the right to civil lawsuits, while Section 647(j)(4)(A) of the California Penal Code threatens fines of up to $1,000 and imprisonment for up to one year as a criminal basis for revenge porn.[38] This policy can be packaged into impact-based criminal sanctions,

*of Artificial Intelligence (IJ-AI)*13, no. 4 (2024): 3786–3792, doi:10.11591/ijai.v13.i4.pp3786-3792

[36] "Exploring Legal Approaches to Regulating Nonconsensual Deepfake Pornography," Tech Policy Press, 2023, https://techpolicy.press/exploring-legal-approaches-to-regulating-nonconsensual-deepfake-pornography.

[37] "Legislature Acts to Prevent Abuse and Exploitation," Senator Mike Moore, Juni 2024, https://www.senatormikemoore.com/new-blog/2024/6/14/legislature-acts-to-prevent-abuse-and-exploitation.

[38] "AB-602 Depiction of individual using digital or electronic technology: sexually explicit material: cause of action," California Legislative Information, 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

where the severity of the punishment increases according to the extent of the content's spread, the victim's vulnerability (for example, if the subject is under 18 years old), and the perpetrator's track record. By adding a "double penalty" provision—for example, a doubling of criminal penalties—if the victim is a minor, this regulation not only has a stronger deterrent effect, but also confirms the value of special protection for children. To ensure the restoration of victims' rights and material compensation, Article 5 of Law Number 12 of 2022 concerning the Crime of Sexual Violence (TPKS) needs to be expanded to include restitution for victims of deepfake pornography—including takedown fees, reputational restoration, and psychosocial support. An empirical study on India's Cyber Crime Reporting Portal shows the effectiveness of rapid restitution in reducing victim trauma and increasing trust in the justice system.[39] In addition, Government Regulation Number 35 of 2020 concerning the Provision of Compensation, Restitution, and Assistance to Witnesses and Victims already provides a basic mechanism for restitution, but it needs to be strengthened with specific technical guidelines for digital deepfake cases, including electronic evidence verification procedures and a "fast-track" mechanism for the issuance of immediate takedown orders. Thus, the integration of progressive criminal sanctions and structured material restitution will close the legal loophole, accelerate the justice process, and comprehensively restore the rights of victims of deepfake pornography.

International collaboration is a key pillar in the fight against deepfake pornography, as these crimes often involve dual jurisdiction and advanced technologies that exceed national capacity. The Convention on Cybercrime (Budapest Convention), which has been ratified by 78 countries as of January 2025, provides a common legal framework—including standards for the definition of cybercrimes, preservation of evidence mechanisms, and mutual legal assistance[40]—as well as capacity building through a network of T-CY experts who actively share best

[39] Restitution for Victims of Nonconsensual Deepfake Pornography," Cyber Crime Reporting Portal India, 2023, diakses 23 Mei 2025, https://www.techpolicy.press/exploring-legal-approaches-to-regulating-nonconsensual-deepfake-pornography/

[40] "About the Convention - Cybercrime," Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

practices in emergency situations. The benefits of being a party to the Convention include the adoption of common standards, follow-up procedures, and capacity building that help protect the rights of individuals online. Until now, Indonesia has still not ratified the agreement, even though the ITE Law and the RKUHP provide a domestic legal basis for cybercrime. Ratification of the Convention will open up official access to the 24/7 Interpol Network, which was formed on the model of the Budapest Convention and serves as an operational point of contact for any request for technical assistance—such as the exchange of electronic evidence, preservation of metadata on foreign servers, and real-time coordination in deepfake investigations in different countries. At the regional level, the ASEAN Cybersecurity Cooperation Strategy (2021–2025) has emphasized the importance of harmonizing cyber regulation with the principles of the Budapest Convention and the digital development of MLAT to accelerate mutual legal assistance. In January 2025, Malaysia proposes the establishment of an ASEAN Cybercrime Task Force—similar to the Interpol structure—to conduct annual cybercrime drills, build Confidence Building Measures, and facilitate the exchange of cyber threat information on a regular basis.[41] In addition, Interpol's platform in dealing with cyber in Southeast Asia demonstrates the effectiveness of global cooperation in joint operations. By leading this initiative, Indonesia is not only closing the juridical and technical gaps in the handling of deepfake pornography, but also strengthening its position as a regional leader that facilitates cross-border coordination and exchange of expertise between ASEAN member states and international partners.

According to Kant, punishment must be based on the principle of retributive—the perpetrator is punished solely for his actions against the law, as a form of respect for human dignity through strict justice.[42] But in the case of deepfake pornography, technical constraints such as digital forensic limitations and end-to-end encryption prevent the accurate

[41] BankInfoSecurity Asia. "Malaysia Proposes Pan-ASEAN Cybercrime Task Force." BankInfoSecurity Asia, January 10, 2025. Retrieved 23 May 2025. https://www.bankinfosecurity.asia/malaysia-proposes-pan-asean-cybercrime-task-force-a-27347.

[42] Immanuel Kant, *The Metaphysics of Morals*, trans. Mary Gregor (Cambridge: Cambridge University Press, 2017), 105–110.

identification of the perpetrator, so the principle of "every offender deserves a fair punishment" cannot be met.[43] Without certainty of identity and evidence, the state fails to enforce just punishment according to Kant's categorical imperative—that criminal acts must always be balanced by proportionate and predictable sanctions for all citizens.

From the point of view of regulatory constraints, the unclear norms in the ITE Law and the Pornography Law create a legal loophole where the production of deepfake content has not been automatically regulated as an independent criminal act. For Kant, the law must be universal and clear (legisprudence as universal law), but the absence of a special article on "AI-based pornography production" confirms that the Indonesian legal system has not actualized the principle of categorical imperative, because perpetrators who engineer content can get away with not being[44] held accountable, even though morality demands equal treatment for equal violations.

Social constraints—stigma, victim-blaming, and low digital literacy—make many victims reluctant to report. Kant views the state as responsible for providing the means for legal subjects to claim their rights (duty-to-protect). Efforts to train digital forensic officers, revise criminal articles, and establish victim-friendly reporting mechanisms are concrete steps to realize the principle of respect for individual dignity within the framework of Kantian; Every victim must be treated as an end, not just a means, so that their right to see the offender punished fairly can be guaranteed.

Conclusion

The development of Artificial Intelligence (AI) technology that gave birth to the phenomenon of deepfake pornography has created new legal challenges in Indonesia. Positive legal regulations such as the Pornography Law, ITE Law, and TPKS Law have not explicitly regulated the production of AI-engineered content, so law enforcement is often not

[43] Kant.

[44] Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "The Urgency of Regulation of Deepfake Pornography in Indonesia," *Kertha Wicara: Journal of Legal Studies* 13, no. 10 (2024): 530–541, doi:10.24843/KW.2024.v13.i10.p5.

optimal. The main obstacles include the absence of a specific legal definition of deepfakes, the limitations of digital evidence, and the weak forensic capacity of the apparatus. In addition, social stigma and low digital literacy exacerbate the vulnerability of victims, who are reluctant to report for fear of being ostracized. A case study of Udayana University students (2025) shows that criminal sanctions are disproportionate to the psychosocial impact of victims, while legal protection has not provided adequate restitution and rehabilitation mechanisms.

To address this, a regulatory reformulation is needed that includes an explicit definition of deepfakes in the Pornography Law and ITE Law, impact-based progressive criminal sanctions, and a mechanism for restitution and removal of illegal content (right to be forgotten). National digital literacy education needs to be strengthened to increase public awareness, supported by integrated services such as the Cyber Victim Support Center. Ratification of the Budapest Convention and international cooperation are also key to expanding the capacity of cross-border investigations. With a holistic approach that combines preventive, repressive, and curative aspects, the Indonesian legal system is expected to be able to effectively protect victims' rights and respond to the dynamics of digital crime in the AI era.

References

"AB-602 Depiction of individual using digital or electronic technology: sexually explicit material: cause of action," California Legislative Information, 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

"About the Convention - Cybercrime," Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

"Exploring Legal Approaches to Regulating Nonconsensual Deepfake Pornography," Tech Policy Press, 2023, https://techpolicy.press/exploring-legal-approaches-to-regulating-nonconsensual-deepfake-pornography.

"Legislature Acts to Prevent Abuse and Exploitation," Senator Mike

Moore, Juni 2024, https://www.senatormikemoore.com/new-blog/2024/6/14/legislature-acts-to-prevent-abuse-and-exploitation.

"Restitution for Victims of Nonconsensual Deepfake Pornography," Cyber Crime Reporting Portal India, 2023, diakses 23 Mei 2025, Exploring Legal Approaches to Regulating Nonconsensual Deepfake Pornography | TechPolicy.Press

ANTARA News, "Udayana University Investigates Case of Alleged Online Sexual Harassment," Antara News, accessed May 23, 2025, https://www.antaranews.com/berita/4802537/universitas-udayana-investigasi-kasus-dugaan-pelecehan-seksual-daring.

Astuti, Linda, Wiwit Ariyani, and Bayu Aryanto. "Urgency Right to Be Forgotten as a Legal Protection for Deepfake Pornography Victims by Artificial Intelligence Technology in Social Media." *International Journal of Law, Government and Communication* 9, no. 37 (2024): 45–58. doi: 10.35631/IJLGC.937006.

BankInfoSecurity Asia. "Malaysia Proposes Pan-ASEAN Cybercrime Task Force." BankInfoSecurity Asia, January 10, 2025. Retrieved 23 May 2025. https://www.bankinfosecurity.asia/malaysia-proposes-pan-asean-cybercrime-task-force-a-27347.

Directorate of Cyber Crime of the National Police Criminal Investigation Branch, "Cyber Patrol," accessed May 25, 2025, https://patrolisiber.id/contact-us/.

Fadhilah, Haida, and Dedy Nuriyatman. "Norm Void on the Production of Deepfake Pornography in Indonesia: A Review of the ITE Law and the Pornography Law. "*Journal of Law and Criminology* 9, no. 1 (2024): 101–117. doi:10.31849/respublica.v24i01.23327.

Fauzyah, Rizgita Nurul, Putri Hafidati, and Sunarya Sunarya. "Legal Protection for Victims of Artificial Intelligence (AI)-Based Deepfake Porn Videos in Indonesia." *Lex Veritatis* 3, no. 3 (2024): 74–88.

Hoesein, Zainal Arifin. *Metode Penelitian Hukum Normatif dan Empiris.* Prenada Media, 2020.

INFID (International NGO Forum on Indonesian Development). Report on Sexual Violence in the Digital Space. INFID, 2023.

Kant, Immanuel. *The Metaphysics of Morals.* Cambridge University Press, 2017.

KOMPAS. "Udayana University Bali Students Suspected of Creating AI-

Based Fake Porn Content," Kompas.com, April 25, 2025, https://denpasar.kompas.com/read/2025/04/25/131021978/mahasiswa-universitas-udayana-bali-diduga-bikin-konten-porno-palsu-berbasis.

Kumparan, "The Revelation of the Case of Deepfake Pornographic Content of Udayana University Students," Kumparan, accessed on May 19, 2025, https://kumparan.com/kumparannews/terungkapnya-kasus-konten-porno-deepfake-mahasiswi-unud-24xOaAR2Ntv/full.

Latifatunnisa, Raihani, and Made Wira Yudha. "The Urgency of Regulatory Reform in Tackling the Misuse of Artificial Intelligence and Deepfake Technology in Indonesia: A Perspective on the Protection of Privacy Rights." *Causa: Journal of Law and Citizenship* 11, no. 1 (2025): 21–30. doi:10.3783/causa.v11i1.11617.

Lolong, Wenly R. J., and Merry Lenda Kumajas. "Criminal Liability of Deepfake Porn Perpetrators Using Artificial Intelligence (AI)." *Journal of Rectum: A Juridical Review of Criminal Handling* 7, no. 2 (2025): 217–224. doi:10.46930/jurnalrectum.v7i2.5618.

Metro TV, *Udayana University Students Create Deepfake Student Porn Content*, YouTube video, 2:20, April 27, 2025, https://www.youtube.com/watch?v=QIIH3DBgt9U, accessed on May 19, 2025.

Ministry of Communication and Information of the Republic of Indonesia, Indonesian Digital Literacy Status 2022, 2022, https://aptika.kominfo.go.id/wp-content/uploads/2023/02/Report_Nasional_2022_FA_3101.pdf.

Ministry of Women's Empowerment and Child Protection of the Republic of Indonesia, "SAPA 129," accessed on May 25, 2025, https://www.kemenpppa.go.id/page/view/NDgzNg%3D%3D.

Nasution, Angelica Vanessa Audrey, Suteki Suteki, and Anggita Doramia Lumbanraja. "The Prospect of Fulfilling the Right to Be Forgotten for Victims of Deepfake Pornography Due to the Abuse of Artificial Intelligence in Indonesia." *Diponegoro Law Journal* 13, no. 2 (2024): 150–165.

Natalia, Cindy, and I Wayan Bela Siki Layang. "Legal Protection for Victims of Deepfake Pornography in the Context of Indonesian

Law." *Kertha Semaya* 12, no. 5 (2024): 4462–4473.

Novera, Olivia, and Yenny Fitri Z. "Analysis of Criminal Law Arrangements for the Abuse of Image Manipulation Technology (Deepfake) in the Dissemination of Pornographic Content Through Social Media Accounts." *El-Faqih: Journal of Islamic Thought and Law* 10, no. 2 (2024): 460–474. doi:10.58401/faqih.v10i2.1539.

Nurjanah, Siti. "Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia." *International Journal of Multicultural and Multireligious Understanding* 10, no. 1 (2023): 1–13. doi:10.18415/ijmmu.v10i1.4409.

Putra, Komang Bagus Wicaksana, and Gusti Ayu Arya Prima Dewi. "The Urgency of Regulating the Crime of Deepfake Pornography in Indonesia." *Journal of Law* 13, no. 10 (2024): 530–541. doi:10.24843/KW.2024.v13.i10.p5.

Rahardjo, Satjipto. *Ilmu Hukum: Paradigma Baru dan Dinamika Perkembangannya.* Genta, 2020.

Reuters, "South Korea to criminalise watching or possessing sexually explicit deepfakes," Reuters, September 26, 2024, https://www.reuters.com/world/asia-pacific/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes-2024-09-26/.

Sabillah, Vienna. "Social Stigma for Victims of Sexual Violence and Its Impact on Victim Psychology." *Journal of Social and Humanities* 10, no. 1 (2022): 15–25.

United Kingdom, Crime and Policing Bill 2025, HC Bill (2025) 123, Parliament of the United Kingdom, diakses pada 19 Mei 2025, https://bills.parliament.uk/bills/3123.

United Nations Interregional Crime and Justice Research Institute (UNICRI), AI for Safer Children, UNICRI, diakses pada 23 Mei 2025, https://unicri.org/topics/AI-for-Safer-Children.

Venkateswarlu Sunkari dan Ayyagari Sri Nagesh "Artificial Intelligence for Deepfake Detection: Systematic Review and Impact Analysis," *International Journal of Artificial Intelligence* (IJ-AI) 13, no. 4 (2024): 3786–3792, doi:10.11591/ijai.v13.i4.pp3786-3792

***

The advance of technology is based on making it fit in so that you don’t really even notice it, so it’s part of everyday life.”

— *Bill Gates*

DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

None

ACKNOWLEDGMENT

This paper is the result of the research conducted for my undergraduate thesis, and I wish to express my deepest gratitude to those who have supported and guided me throughout this academic endeavor. I would like to extend my sincere thanks to Mr. Ridwan Arifin, SH, LLM, my thesis supervisor, whose expertise, guidance, and unwavering support have been invaluable in shaping this research. His constructive feedback and insightful advice have been essential to the completion of this study. I am also profoundly grateful to the Faculty of Law, Universitas Negeri Semarang, for providing the academic resources and intellectual environment that have facilitated the success of this research. Finally, I would like to acknowledge all those who have contributed in any way to this work. Their support has been greatly appreciated.

HISTORY OF ARTICLE

Submitted	: May 28, 2025
Revised	: August 11, 2025
Accepted	: November 2, 2025
Published	: December 8, 2025

GENERATIVE AI STATEMENT

None