CRIMINALIZATION OF DEEPFAKE PORNOGRAPHY OFFENSES: THE URGENCY OF REGULATION UNDER THE ELECTRONIC INFORMATION AND TRANSACTIONS LAW

Novalinda Nadya Putri[1]*, Muhammad Enaldo Hasbaj[2]
[12]Mahkamah Agung Republik Indonesia, Indonesia
Correspondent Email : 1) novalindanp@mahkamahagung.go.id

Received	:01 November 202	Published	: 13 January 2026
Revised	:15 November 2025	DOI	: https://doi.org/10.54443/ijerlas.v5i6.4944
Accepted	:10 December 2025	Link Publish	: https://radjapublika.com/index.php/IJERLAS

Abstract

Deepfake pornography enables the manipulation of an individual's image or likeness into explicit content without consent, resulting in severe harm to personal dignity, privacy, reputation, and psychological well-being. This study aims to examine the urgency of criminalizing deepfake pornography within Indonesia's legal framework, particularly under the Law on Electronic Information and Transactions (UU ITE), which currently lacks explicit regulation addressing this phenomenon. Employing a normative juridical research method, this study analyzes relevant Indonesian legislation, including the UU ITE, the Pornography Law, and the Criminal Code, alongside fundamental principles of criminal law. A comparative legal approach is also adopted by examining regulatory responses in several jurisdictions, such as the United States, the European Union, and Japan, which have implemented more specific and adaptive legal measures against deepfake-related offenses. The findings reveal significant legal gaps in Indonesian law that hinder effective law enforcement and fail to provide adequate legal protection for victims. Consequently, this study argues that the explicit criminalization of deepfake pornography within the UU ITE is essential to ensure legal certainty, enhance victim protection, and strengthen cybercrime enforcement mechanisms. The study further recommends regulatory reform that integrates criminal sanctions, platform accountability, and victim-oriented remedies as part of a comprehensive legal response to technology-driven sexual exploitation in the digital era.

Keywords: ***Deepfake Pornography, Artificial Intelligence, Cybercrime, Victim Protection***

INTRODUCTION

The rapid advancement of artificial intelligence (AI) technology has profoundly transformed various aspects of human life, encompassing industry, economic systems, education, and digital media. One of the most rapidly evolving innovations in this technological landscape is deepfake technology, which enables the manipulation of visual and audio content with an exceptionally high degree of realism (Kietzmann et al., 2020). Through the application of deep learning algorithms, deepfake technology allows the replacement of an individual's face in video footage or the fabrication of a voice that closely mimics a specific person. Although initially developed for creative and innovative purposes, particularly within the film and entertainment industries, this technology has increasingly been misused, giving rise to serious legal and ethical concerns. One of the most alarming manifestations of such misuse is deepfake pornography, defined as the creation and dissemination of pornographic content that digitally incorporates an individual's likeness without their consent.

The proliferation of deepfake pornography has emerged as a significant threat in an increasingly open and interconnected digital environment. This technology enables perpetrators to falsify personal identities by digitally superimposing faces onto pornographic material, rendering such content difficult to distinguish from authentic recordings. A report published by DeepTrace Technologies in 2019 revealed that more than 15,000 deepfake videos were circulating online, approximately 96% of which consisted of pornographic content. Even more concerning is the disproportionate impact on women as primary victims, while children are also increasingly vulnerable to exploitation through pedophilic deepfake content disseminated across various digital platforms, including Pixiv in Japan (Kumparan, 2023). These findings demonstrate that deepfake pornography is not merely a technological anomaly but a systemic form of digital sexual exploitation. The consequences of deepfake pornography are multifaceted, affecting individual privacy, digital security, and the psychological well-being of victims (Sharma, 2024). Individuals targeted by deepfake pornography often suffer severe reputational damage, particularly when manipulated content spreads rapidly online and becomes virtually impossible to erase. In many cases, victims experience intense social stigmatization, loss of employment opportunities, and exposure to gender-based violence. From a psychological perspective, deepfake

Publish by **Radja Publika**

pornography can inflict profound trauma, anxiety, depression, and social withdrawal due to the circulation of falsified sexual content involving the victim's identity. These harms extend beyond individual victims and pose broader threats to social trust and integrity, as the technology enables virtually anyone to become a target of malicious digital manipulation. In response to these emerging threats, several jurisdictions have begun to acknowledge the dangers posed by deepfake pornography and have attempted to formulate regulatory responses. Nevertheless, there remains no comprehensive international legal framework specifically addressing deepfake-related offenses. In the United States, certain states, such as California and Virginia, have enacted legislation criminalizing the creation and dissemination of harmful deepfake content, particularly when it causes reputational or electoral harm. Within the European Union, the General Data Protection Regulation (GDPR) has been utilized as a legal basis to protect individuals from the misuse of personal data through deepfake technologies (Dremliuga & Korobeev, 2021). Despite these efforts, regulatory approaches remain fragmented and largely reactive (Mania, 2022: 117–129).

In Indonesia, the regulation of deepfake pornography has yet to be explicitly addressed under the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*, hereinafter UU ITE). Although several provisions within the UU ITE govern the dissemination of content violating morality and defamation, these provisions are insufficient to effectively address the unique characteristics of deepfake pornography, particularly when such content is generated and distributed using AI-based technologies. Law No. 44 of 2008 on Pornography may also serve as a legal basis for prosecuting offenders; however, significant normative gaps persist, especially concerning the attribution of criminal liability for AI-generated content and the delineation of responsibility between creators, distributors, and digital platforms. Beyond normative deficiencies, the enforcement of laws against deepfake pornography presents substantial challenges. One of the primary obstacles lies in the difficulty of identifying perpetrators, as deepfake content is often difficult to detect through conventional digital forensic techniques. Many online platforms continue to struggle with effectively identifying and removing deepfake material, despite ongoing developments in detection technologies (Rana, Nobi & Sung, 2022). Moreover, the widespread use of anonymous accounts and Virtual Private Networks (VPNs) further complicates law enforcement efforts to trace and apprehend perpetrators of deepfake-based cybercrimes.

Given the severity and complexity of the harms caused by deepfake pornography, the strengthening of regulatory provisions within the UU ITE is urgently required. This may be achieved through the incorporation of explicit legal definitions and specific criminal provisions addressing deepfake pornography as a distinct form of cybercrime, the enhancement of public digital literacy to improve awareness and identification of deepfake threats, and the promotion of international cooperation. Such cooperation may include the involvement of global institutions such as the United Nations, UN Women, and UNICEF in developing coordinated policies to regulate the misuse of AI technologies. Deepfake pornography constitutes a serious threat to individual security and human rights, underscoring the urgent need for ethically grounded technological development and robust legal frameworks to control the misuse of deepfake technology. Clear criminal regulations and effective enforcement mechanisms are essential to prevent the creation and dissemination of harmful deepfake content and to ensure adequate protection for victims. Accordingly, this study aims to analyze the urgency of criminalizing deepfake pornography under the UU ITE, to identify existing regulatory shortcomings, and to propose normative and policy-based recommendations to strengthen legal protection against the misuse of AI-generated deepfake technology.

LITERATURE REVIEW

Scholarly discussions on deepfake technology increasingly emphasize its dual character as both an innovative digital tool and a source of serious legal and ethical risks. Early studies largely focused on its technological foundations, particularly the use of deep learning models such as Generative Adversarial Networks (GANs) to manipulate visual and audio data with high realism. Kietzmann et al. (2020) conceptualize deepfakes as a "double-edged sword," noting their creative potential while warning of their disruptive impact when misused, especially in the production of misleading and non-consensual content. Subsequent scholarship has shifted attention toward the social and legal harms caused by deepfake pornography. Deepfake pornography characterizes as a dehumanizing practice that violates dignity, autonomy, and consent, framing it as a form of digital sexual violence rather than mere technological abuse (Pascale, 2023). Sharma (2024) similarly highlights its disproportionate impact on women, emphasizing how deepfake pornography undermines digital privacy and exacerbates online gender-based violence. These perspectives position deepfake pornography as both a cybercrime and a human rights issue requiring firm legal intervention. From a comparative legal standpoint, Mania (2022) observes that European legal frameworks on revenge pornography and data protection can partially address deepfake pornography, yet remain inadequate due to the absence of explicit criminal provisions. Romero Moreno (2024) strengthens this argument through a human rights-based approach, asserting that state obligations to protect privacy and personal integrity justify proactive regulation of generative AI and deepfake content. These analyses suggest that traditional legal instruments are insufficient to respond to the unique characteristics of AI-generated sexual content.

Criminal law scholars further highlight enforcement challenges. Dremliuga and Korobeev (2021) underline difficulties in attributing criminal liability for AI-generated content, particularly due to anonymity and the transnational nature of digital platforms. Wahyudi (2025) adds that limited technological capacity and inadequate digital forensics weaken effective prosecution of AI-based crimes. In the Indonesian context, existing studies consistently identify regulatory gaps. Novyanti and Astuti (2021) argue that the Electronic Information and Transactions Law (UU ITE) lacks explicit provisions on deepfake misuse, creating legal uncertainty. Rohmawati et al. (2024) and Darmawan et al. (2025) further stress that this gap disproportionately harms victims of gender-based violence and child exploitation. Despite this growing literature, comprehensive normative analysis on the urgency of explicitly criminalizing deepfake pornography within Indonesia's criminal law framework remains limited. This study addresses that gap by examining deepfake pornography as a distinct cybercrime and proposing legal reforms grounded in comparative and human rights perspectives.

METHOD

This study employs a normative juridical research method, which focuses on the systematic analysis of legal norms, principles, and doctrines within the framework of positive law. The normative approach is utilized to examine the urgency of criminalizing deepfake pornography within the Indonesian legal system, particularly in relation to the adequacy and coherence of existing cybercrime regulations. The research primarily adopts a statutory approach by analyzing relevant legislation, including the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*/UU ITE), Law No. 44 of 2008 on Pornography, and the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana*/KUHP). In addition, the study examines fundamental principles of criminal law, such as legality, culpability, and criminal liability, in order to assess whether the current legal framework sufficiently addresses the distinctive characteristics of AI-generated deepfake pornography.

Furthermore, this research incorporates a comparative legal approach by examining regulatory responses to deepfake pornography in selected jurisdictions, including the United States, the United Kingdom, and Japan. These jurisdictions are selected due to their relatively advanced legal and policy responses to digital sexual exploitation and technology-driven cybercrime. The comparative analysis aims to identify best practices and regulatory models that may inform the formulation of a more effective and context-sensitive criminal policy framework in Indonesia. The legal materials analyzed in this study consist of primary legal materials, including statutory instruments and official legal documents; secondary legal materials, such as scholarly articles, legal commentaries, and academic journals related to cybercrime, artificial intelligence, and digital sexual exploitation; and tertiary legal materials, including legal dictionaries and encyclopedias. The collected legal materials are analyzed using qualitative juridical analysis to construct normative arguments concerning the necessity and scope of criminalization of deepfake pornography under Indonesian law.

RESULTS AND DISCUSSION

Regulation of Deepfake Pornography as a Cybercrime under Indonesian Law

The advancement of artificial intelligence (AI) technology has generated profound impacts across multiple dimensions of human life, including communication, entertainment, and digital media. One of the most prominent AI-driven technological developments is deepfake technology, which relies on deep learning algorithms to manipulate visual and audio content with a high degree of realism (Riadi, Prayogi & Setyawati, 2024). Deepfake technology employs sophisticated computational models capable of learning facial features, vocal patterns, and bodily movements from extensive datasets, enabling the creation of digital content that appears authentic despite being entirely computer-generated (Pascale, 2023).

Initially, deepfake technology was developed for legitimate and creative purposes, particularly within the film and entertainment industries, where it was used to enhance visual effects and improve production quality. However, as access to deepfake software has become increasingly widespread and user-friendly, the technology has gradually been misused for harmful purposes. One of the most concerning forms of misuse is deepfake pornography, which has emerged as a new and complex category of cybercrime. Deepfake pornography refers to the use of deepfake technology to produce pornographic content that digitally inserts the face of an individual into sexually explicit material without their consent. In many cases, the faces of individuals, predominantly women (CNN, 2019), are superimposed onto the bodies of actors in pornographic videos, creating the false impression that the depicted individuals are directly involved in the fabricated sexual acts. This phenomenon is particularly alarming due to the speed at which such content can be disseminated through digital platforms and the difficulty of removing it once it has circulated online. As a result, deepfake pornography poses severe threats to victims' privacy, reputation, and psychological well-being.

A report published by Deeptrace Technologies in 2019 indicated that out of more than 15,000 deepfake videos circulating online, approximately 96 percent consisted of pornographic content, with women constituting the vast majority of victims. Even more troubling is the growing use of deepfake pornography to exploit children, including the circulation of manipulated pedophilic content across various digital platforms in several countries, including Japan. To fully understand the legal challenges posed by deepfake pornography, it is essential to examine the technological mechanisms underlying deepfake production. Deepfake technology primarily utilizes deep learning algorithms, particularly Generative Adversarial Networks (GANs), which consist of two competing models: a generator and a discriminator. The generator is responsible for creating synthetic images or videos based on previously learned data patterns, while the discriminator evaluates the authenticity of the generated content. Through continuous iterative processes, the generator improves its output until the manipulated content becomes increasingly indistinguishable from genuine recordings.

In the context of deepfake pornography, this technology enables the creation of highly convincing videos portraying individuals in situations in which they were never involved. Facial images of victims are often extracted from publicly available photos or videos online and then processed using deepfake algorithms to be embedded into pornographic material. The resulting content can appear highly realistic (Satriawan, Imran & Erniwati, 2023), making it difficult for viewers, and even law enforcement authorities, to immediately identify it as fabricated. Although deepfake pornography falls within the broader category of cybercrime, it differs fundamentally from other forms of digital sexual offenses, such as revenge pornography, digital sexual extortion, or online defamation. Revenge pornography typically involves the non-consensual distribution of authentic sexual content, often by former intimate partners, motivated by revenge or coercion (Salsabila, 2024). In contrast, deepfake pornography involves fabricated content created without any direct participation by the victim, yet it can cause equally severe, if not greater, harm to the victim's reputation and dignity. Moreover, deepfake pornography presents greater evidentiary and investigative challenges, as perpetrators often operate anonymously and exploit easily accessible software tools.

The consequences of deepfake pornography are extensive and affect social, psychological, and legal dimensions. Socially, victims frequently experience stigmatization, discrimination, and social exclusion, particularly when manipulated content spreads widely online. Many victims face intense societal pressure, loss of employment, or damage to professional credibility due to false assumptions regarding their involvement in pornographic activities. From a psychological perspective, the impact of deepfake pornography can be devastating. Victims often suffer from anxiety, depression, and severe emotional distress as a result of the circulation of falsified sexual content involving their identity. Feelings of helplessness and loss of control over one's personal image may lead to prolonged social withdrawal and isolation (Respati et al., 2024). In extreme cases, such psychological trauma has been linked to self-harm and suicidal ideation (Rohmawati, Junaidi & Khaerudin, 2024). From a legal standpoint, deepfake pornography poses significant challenges to law enforcement in many jurisdictions, including Indonesia (Darmawan, Junaidi & Khaerudin, 2025). One of the primary issues is the absence of specific legal provisions that directly regulate the creation and dissemination of deepfake pornography. Although certain provisions within Indonesia's Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*/UU ITE) and the Pornography Law may be invoked to prosecute offenders, these legal instruments contain substantial normative gaps. A key difficulty lies in determining criminal liability for deepfake pornography, particularly when content is produced anonymously or generated outside Indonesian jurisdiction. Furthermore, evidentiary challenges arise due to the highly realistic nature of deepfake content, which complicates efforts to distinguish manipulated material from authentic recordings.

Within Indonesia's cyber law framework, digital crimes are primarily regulated under Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, as well as Law No. 44 of 2008 on Pornography. However, neither statute explicitly addresses deepfake pornography, despite its serious implications for privacy rights, reputation, and human dignity. Consequently, an analysis of existing legal provisions is necessary to assess the extent to which Indonesia's cyber law regime can respond to deepfake pornography and to identify regulatory deficiencies requiring reform. One provision frequently cited in prosecuting deepfake pornography cases is Article 27 paragraph (1) of the UU ITE, which prohibits the intentional distribution, transmission, or making accessible of electronic information containing content that violates public morality. In theory, the dissemination of deepfake pornographic material may fall within this prohibition. However, the principal issue concerns the interpretation of deepfake content as "electronic information containing immoral content." This provision has traditionally been applied to cases involving the dissemination of genuine pornographic material, such as revenge pornography. In contrast, deepfake pornography involves AI-generated content that does not reflect actual conduct by the victim, thereby creating ambiguity regarding the applicability of this provision. Similarly, Article 27 paragraph (3) of the UU ITE, which governs defamation, is often associated with deepfake pornography cases. This provision criminalizes the intentional and unauthorized dissemination of electronic information containing defamatory material. Deepfake pornography can severely damage a victim's reputation by falsely depicting them in explicit sexual acts. However, defamation law typically focuses on verbal or written statements that insult or degrade an individual, rather than on AI-generated visual manipulation, which raises further interpretative challenges. Law No. 44 of 2008 on Pornography represents another potential legal basis for prosecuting deepfake pornography. Article 4 paragraph (1) prohibits the production, creation, duplication, distribution, broadcasting, importation, exportation, offering, sale, rental, or provision of pornographic content. The definition of pornography under Article 1 paragraph (1) encompasses images, sketches, illustrations, photographs, audio, animated visuals, cartoons, and other forms of communication containing sexual exploitation or obscenity. Based on this definition, deepfake pornographic videos may fall within the scope of prohibited content, despite being digitally fabricated.

Nevertheless, a major challenge in applying the Pornography Law to deepfake pornography lies in establishing the requisite element of intent. Article 4 paragraph (1) implies conscious intent to produce or disseminate pornographic content. In deepfake cases, perpetrators often operate through anonymous accounts or foreign-based platforms, making it difficult to identify the individual responsible. Moreover, since deepfake pornography does not involve physical exploitation of the victim, legal debates frequently arise regarding whether such content constitutes sexual exploitation within the meaning of the statute. Regulatory weaknesses in addressing deepfake pornography in Indonesia extend beyond substantive legal norms to encompass limitations in enforcement mechanisms and digital content oversight (Yudha, 2024). One of the principal obstacles is the lack of effective legal instruments enabling law enforcement agencies to trace the origin of deepfake production. Deepfake pornography is often created and disseminated via overseas digital platforms, complicating cross-border investigations. Additionally, perpetrators frequently utilize Virtual Private Networks (VPNs) and dark web technologies to conceal their identities, further hindering enforcement efforts (Ariyadi et al., 2024).

Another significant challenge is the limited technical understanding of deepfake technology among law enforcement officials. Investigators often encounter difficulties distinguishing deepfake content from authentic videos, particularly given the rapid evolution of AI-generated media. Although various detection tools and forensic algorithms have been developed, the implementation of advanced digital forensic technologies in Indonesia remains limited. Consequently, many deepfake pornography cases cannot be effectively prosecuted due to insufficient or unreliable evidence. Several cases in Indonesia illustrate the misuse of deepfake pornography as a tool for defamation and digital extortion (Novyanti & Astuti, 2021). One widely publicized case involved the circulation of a deepfake pornographic video resembling a public official, which sparked public controversy and caused significant reputational harm. Notably, a female prosecutor named Tasya became a victim of deepfake pornography, alongside other prosecutors, civil servants, and medical professionals. These cases demonstrate the growing prevalence of AI-based digital crimes in Indonesia (Telisik.id, 2024).

However, law enforcement authorities have faced considerable difficulties in prosecuting perpetrators due to the absence of specific regulations governing deepfake pornography. As a result, cases are often addressed through defamation or morality-based offenses, which fail to fully capture the technological complexity and distinct nature of deepfake pornography as a cybercrime. Based on the foregoing analysis, Indonesia must urgently reform its cyber law framework to address the challenges posed by deepfake technology (Wahyudi, 2025). One critical step is revising the UU ITE to include explicit definitions and sanctions related to deepfake pornography. In addition, collaboration between government institutions, technology companies, and civil society is essential to enhance deepfake detection systems and strengthen victim reporting mechanisms. Beyond regulatory reform, digital literacy plays a crucial role in preventing and mitigating deepfake pornography. Public education initiatives aimed at increasing awareness of deepfake risks, digital ethics, privacy, and personal data protection can help reduce the misuse of AI technology in the future. In conclusion, although the UU ITE and the Pornography Law provide a legal basis for addressing deepfake pornography, existing regulations remain inadequate in terms of legal definitions, enforcement capacity, and victim protection mechanisms. Therefore, comprehensive legal reform and a multidisciplinary approach are necessary to effectively combat deepfake pornography and ensure meaningful protection for victims within Indonesia's digital legal landscape.

The Urgency of Criminalizing Deepfake Pornography under the Electronic Information and Transactions Law

The phenomenon of deepfake pornography has evolved into an increasingly tangible threat in the digital era, particularly in light of rapid advancements in artificial intelligence (AI) that enable highly accurate manipulation of images and videos. The harms generated by deepfake pornography extend beyond individual victims and carry the potential to undermine broader social stability, as such technological abuse is becoming increasingly difficult to detect and address through existing legal mechanisms. In Indonesia, the absence of explicit legal provisions criminalizing the creation and dissemination of deepfake-based content designed to harm individuals constitutes a significant regulatory gap. Within the context of cyber law, existing regulations—most notably the Electronic Information and Transactions Law (Undang-Undang Informasi dan Transaksi Elektronik/UU ITE) and the Pornography Law—remain insufficient to effectively prosecute perpetrators of deepfake pornography. Accordingly, the explicit criminalization of deepfake pornography within the UU ITE has become an urgent necessity to ensure legal certainty and adequate protection for victims. The legal vacuum in addressing the dissemination of deepfake pornography primarily stems from the absence of provisions that explicitly prohibit or regulate the creation and distribution of AI-generated manipulated content. Current Indonesian regulations focus predominantly on immoral content and defamation, which are inadequate for addressing the unique characteristics of deepfake-based offenses (Syahirah & Prasetyo, 2025). In many cases, victims of deepfake pornography encounter significant barriers in pursuing legal remedies due to the ambiguous legal status of deepfake content. This ambiguity is exacerbated by the fact that deepfake material is often generated by artificial intelligence systems rather than directly produced by identifiable individuals. As a result, law enforcement authorities face substantial difficulties in determining criminal responsibility, particularly when perpetrators distribute content through foreign-based platforms or employ anonymity techniques to evade detection.

In developing an effective regulatory framework to address deepfake pornography, Indonesia may draw valuable lessons from jurisdictions that have already taken steps to criminalize such practices. In the United States, several states, including California and Virginia, have enacted legislation specifically targeting deepfake pornography as a form of unlawful conduct (ASI Online, 2021). California, for example, has adopted Assembly Bill 730, which restricts the use of deepfake technology in political contexts, as well as Assembly Bill 602, which grants victims the right to pursue civil actions against individuals who create and disseminate non-consensual deepfake pornography (Daily Journal, 2020). Virginia, meanwhile, became the first state to explicitly categorize deepfake pornography as a form of revenge pornography, thereby enabling victims to seek legal remedies for defamation and the unlawful distribution of sexual content. These regulatory developments demonstrate that targeted legal provisions addressing deepfake technology can significantly enhance victim protection and provide law enforcement agencies with clearer legal foundations for prosecution.

In the European Union, regulatory responses to deepfake pornography emphasize the protection of personal data and individual privacy rights. The General Data Protection Regulation (GDPR) affords individuals the right to request the removal of harmful content, including deepfake pornography created without consent (Romero Moreno, 2024). In addition, the recently enacted Digital Services Act (DSA) imposes proactive obligations on digital platforms to detect, report, and remove harmful content, including deepfake material (European Commission, 2024). This regulatory approach underscores that effective protection against deepfake pornography requires not only criminalization but also platform accountability in preventing and mitigating the dissemination of illegal content. Japan adopts a distinct regulatory approach by focusing on pornography regulation and gender-based violence prevention. The Japanese government has tightened regulations concerning digitally mediated sexual exploitation, including stricter oversight of the adult entertainment industry to prevent the misuse of deepfake technology (Japan Today, 2023). Moreover, Japan has invested in advanced digital forensic technologies that facilitate the identification of deepfake content, thereby enhancing law enforcement capacity in cases involving digital manipulation. When compared to these jurisdictions, Indonesia remains significantly behind in explicitly regulating deepfake pornography. The lack of clear legal provisions has contributed to the increasing prevalence of deepfake pornography cases that are difficult to address through existing legal frameworks. One of the most immediate consequences of regulatory inadequacy is the difficulty faced by victims in obtaining justice, as perpetrators frequently evade liability under existing legal provisions. Furthermore, the absence of firm legal sanctions may embolden offenders to disseminate deepfake pornography with minimal fear of legal repercussions.

The threat posed by deepfake pornography in Indonesia is exacerbated by the widespread accessibility of deepfake technology and the low level of public awareness regarding the dangers of digital manipulation. The proliferation of AI-based applications capable of generating deepfake content using only a few facial images has significantly increased the risk of victimization. Many individuals remain unaware of how to legally protect themselves, while law enforcement agencies lack sufficient legal instruments to effectively process deepfake pornography cases. For these reasons, the explicit criminalization of deepfake pornography within the UU ITE is imperative to ensure legal certainty and to close existing regulatory gaps (Putri 2024). One concrete step would be the introduction of specific provisions within the UU ITE that prohibit the creation, dissemination, and use of deepfake technology for harmful purposes. Such provisions should be accompanied by proportionate criminal sanctions that reflect the severity of the harm caused. In addition, legal mechanisms must be established to enable victims to seek remedies, including the right to request the removal of harmful deepfake content and to pursue compensation for damages suffered (Algamar dan Ampri 2022). Beyond criminalization, the UU ITE should be strengthened by imposing clearer obligations on digital platforms to actively address deepfake pornography. Social media platforms and internet service providers should be required to implement effective deepfake detection systems and to establish accessible reporting mechanisms for victims seeking content removal. This approach has been successfully implemented in jurisdictions such as the European Union through the Digital Services Act, which mandates proactive platform responsibility. The urgency of criminalizing deepfake pornography must also be accompanied by efforts to enhance law enforcement capacity. This includes specialized training for investigators and prosecutors in detecting and handling cases involving deepfake technology. Collaboration among government agencies, academic institutions, and technology companies is essential to develop advanced AI-based detection systems capable of identifying manipulated content with greater accuracy. The rapid advancement of AI technology has significantly increased the complexity of cyber law enforcement. Highly realistic deepfake content often makes it difficult for victims to prove that videos or images are digitally manipulated rather than authentic recordings (Sulianta 2025). The absence of clear digital traces identifying the creators of deepfake pornography further complicates enforcement efforts. Key challenges faced by law enforcement authorities include difficulties in identifying and apprehending perpetrators, technical barriers in detecting deepfake content, limited platform accountability, and insufficient public digital literacy (Juhandi et al. 2023).

One of the most significant obstacles in prosecuting deepfake pornography is the anonymity of perpetrators. Unlike conventional crimes, deepfake pornography is often produced and disseminated anonymously through VPNs, proxy services, or the dark web. The availability of user-friendly AI-based deepfake generators further enables individuals without advanced technical expertise to create and distribute manipulated content, complicating efforts to identify those responsible (Mahendra et al. 2024). Technical challenges in detecting deepfake content also present serious obstacles. As detection technologies improve, deepfake generation techniques evolve to evade identification. Many deepfake videos undergo encryption or recompression, making them difficult to distinguish from authentic recordings using conventional forensic methods. Although various AI-based detection tools have been developed, their effectiveness remains limited, particularly against deepfake content generated using advanced models capable of dynamically adjusting facial expressions, lighting, and skin textures.

Digital platforms play a crucial role in both the dissemination and prevention of deepfake pornography. While major platforms such as Facebook, Instagram, X (formerly Twitter), and TikTok have adopted policies prohibiting harmful deepfake content, moderation processes often rely on user reports and may be slow. The sheer volume of content uploaded every second renders manual moderation ineffective, while automated detection systems continue to suffer from high error rates (Sulianta 2025). Moreover, in Indonesia, digital platforms are not subject to explicit legal obligations to promptly remove deepfake pornography. Unlike the European Union, where regulations such as the Digital Services Act impose proactive responsibilities on platforms (Rojszczak 2023), Indonesia lacks a specific regulatory framework governing platform accountability for deepfake content. Consequently, harmful content often remains accessible for extended periods, even after being reported by victims.

Low levels of digital literacy among the public further exacerbate the spread of deepfake pornography. Many individuals lack awareness of how deepfake technology operates and how easily personal images shared online can be misused. This lack of understanding contributes to the unintentional dissemination of deepfake content and prevents victims from effectively seeking legal protection. In several international cases, deepfake pornography has been created using facial images taken directly from victims’ social media accounts, highlighting the vulnerability created by inadequate digital awareness (Shobirin, Rosyadi, dan Sari 2025). Addressing these challenges requires a comprehensive approach encompassing regulatory reform, enhanced law enforcement capacity, and cooperation with digital platforms. Law enforcement agencies must be equipped with advanced digital forensic tools capable of tracing deepfake creators despite anonymity measures. Governments should collaborate with technology companies to integrate AI-based detection systems directly into digital platforms to prevent the dissemination of deepfake pornography at an early stage. In addition, digital platforms should be required to increase transparency regarding their handling of deepfake content, including publishing periodic reports on removed content and explaining the operation of their detection algorithms. Technology companies should also be encouraged to develop digital verification tools that enable users to identify whether content has been manipulated, thereby empowering the public to distinguish authentic media from AI-generated fabrications.

The rapid development of AI technology has undeniably facilitated the production of deepfake pornography (Putra et al. 2024), presenting significant challenges for legal regulation in Indonesia. Existing legal frameworks remain insufficient to address this phenomenon effectively. Accordingly, concrete measures are required to strengthen regulatory responses, including the adoption of more specific legal provisions, enhanced intersectoral cooperation, public education initiatives, and international advocacy through global organizations. A key recommendation in addressing deepfake pornography is the formulation of more explicit legal policies within the UU ITE. Currently, the UU ITE regulates immoral content and defamation without explicitly recognizing deepfake pornography as a distinct cybercrime. Legal reform is therefore necessary to introduce clear definitions, constituent elements of the offense, and sanctions applicable to deepfake pornography. Such clarity is essential to avoid ambiguity in law enforcement and to ensure effective prosecution. Sanctions for deepfake pornography offenses should be designed to produce a strong deterrent effect, particularly for perpetrators who intentionally exploit deepfake technology for purposes of sexual exploitation or reputational harm. Proposed penalties may include imprisonment and proportionate fines, as well as victim-centered remedies such as the right to request content removal and compensation for damages. Legal harmonization with existing statutes, including the Pornography Law and the Criminal Code, is also essential to prevent regulatory overlap. As a follow-up to the urgent need for firm legal enforcement, explicit legal norms prohibiting and sanctioning deepfake pornography must be formulated. Adaptive and technologically responsive legal provisions are crucial to ensuring legal certainty and enabling effective prosecution of emerging cybercrimes involving AI-generated pornographic content. One proposed provision may be formulated as follows: "Any person who intentionally and without lawful authority produces, creates, duplicates, reproduces, distributes, broadcasts, imports, exports, offers, sells, rents, or provides pornographic electronic content created using artificial intelligence technology shall be punished with imprisonment of up to six (6) years and/or a fine of up to IDR 1,000,000,000 (one billion rupiah)." Overall, the establishment of clear legal regulations concerning deepfake pornography within the UU ITE would provide stronger protection for society and reinforce Indonesia's legal system in responding to the challenges posed by digital technological advancement. Through explicit criminalization, victims would gain clearer legal pathways to justice, while law enforcement authorities would possess firmer legal grounds for addressing deepfake pornography cases effectively. Ultimately, such measures would strengthen the protection of individual privacy and reputation and contribute to the development of a safer and more ethical digital ecosystem in Indonesia.

CONCLUSION

Deepfake pornography represents a rapidly evolving form of technology-enabled cybercrime that poses serious challenges to criminal law in the digital era. The misuse of artificial intelligence to manipulate an individual's image or voice and embed it into pornographic content without consent results in severe social, psychological, and legal harm, including violations of dignity, privacy, and reputation. This study demonstrates that the existing Indonesian legal framework, particularly the Electronic Information and Transactions Law (UU ITE), has not yet explicitly regulated deepfake pornography. Although certain provisions may be applied indirectly, their general and fragmented nature has proven inadequate to provide legal certainty, effective enforcement, and meaningful protection for victims.

From a normative and comparative perspective, the absence of specific legal provisions governing deepfake pornography has created significant legal loopholes that complicate law enforcement efforts and allow perpetrators to evade accountability. Comparative experiences from jurisdictions such as the United States, the European Union, and Japan indicate that explicit criminalization, combined with platform accountability and victim-centered remedies, is essential to address the unique characteristics of deepfake-based sexual exploitation. Accordingly, this study recommends the reformulation of the UU ITE through the introduction of clear definitions, constituent elements of the offense, and proportionate criminal sanctions targeting the creation, distribution, and use of deepfake pornography. Such reform should be harmonized with existing legislation, including the Pornography Law and the Criminal Code, to avoid regulatory overlap and ensure coherent enforcement.

In addition to legal reform, an effective response to deepfake pornography requires a comprehensive and multidisciplinary approach. This includes strengthening law enforcement capacity through specialized training and advanced digital forensic tools, imposing clearer obligations on digital platforms to detect and remove deepfake content proactively, and enhancing public digital literacy to reduce vulnerability to technological abuse. Furthermore, international cooperation with global organizations and cross-border regulatory frameworks is essential to address the transnational nature of deepfake-related crimes. Through integrated legal reform, institutional capacity building, platform responsibility, and societal awareness, Indonesia can develop a more adaptive, just, and rights-based legal framework capable of responding effectively to the challenges posed by deepfake pornography in the digital age.

REFERENCES

Algamar, Muhammad Deckri, and Aliya Ilysia Irfana Ampri. (2022). "Hak untuk Dilupakan: Penghapusan Jejak Digital sebagai Perlindungan Selebriti Anak dari Bahaya Deepfake." Jurnal Yustika: Media Hukum dan Keadilan 25 (1): 25–39.

Ariyadi, Mohamad Noor Fajar Al Arif, and Dadang Herli. (2024). "Penegakan Hukum Pidana terhadap Pelaku Ujaran Kebencian di Media Sosial Menggunakan Akun Palsu." Journal of Innovation Research and Knowledge 4 (6): 3463–3480.

Darmawan, Muh. Taufik, Amir Junaidi, and Ariy Khaerudin. (2025). "Penegakan Hukum terhadap Penyalahgunaan Deepfake pada Pornografi Anak di Era Artificial Intelligence di Indonesia." Jurnal Penelitian Serambi Hukum 18 (1): 42–54.

Juhandi, April Laksana, Faturohman, Ina Khodijah, Achmad Nashrudin Priatna, Riska Ferdiana, and Santia. (2023). "Literasi Digital: Sinergitas TNI, Polri, dan Akademisi dalam Kajian Pengabdian kepada Masyarakat dari Perspektif Remaja Milenial sebagai Pengguna Media Sosial dalam Pandangan Hukum di SMA 1 Mancak Kabupaten Serang." In Prosiding Seminar Umum Pengabdian kepada Masyarakat, Vol. 1, No. 1, 136–145.

Kietzmann, Jan H., Linda W. Lee, Ian Paul McCarthy, and Tim C. Kietzmann. (2020). "Deepfakes: Trick or Treat?" Business Horizons.

Mahendra, Gede Surya, Daniel Adolf Ohyver, Najirah Umar, Loso Judijanto, Ayuliamita Abadi, Budi Harto, and I. Gede Adi Sudi Anggara et al. (2024). Tren Teknologi AI: Pengantar, Teori, dan Contoh Penerapan Artificial Intelligence di Berbagai Bidang. Jakarta: PT Sonpedia Publishing Indonesia.

Mania, Karolina. (2022). "Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings from a Comparative Legal Study." Trauma, Violence, & Abuse 25: 117–129.

Novyanti, Heny, and Pudji Astuti. (2021). "Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau dari Hukum Pidana." Novum: Jurnal Hukum: 31–40.

Pascale, Emily. (2023). "Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse." Syracuse Law Review 73: 335–370.

Putra, Muhammad Alvin Maulidana Firdaus, Deborah Kurniawati, Pulut Suryati, and Sumiyatun. (2024). "Integrasi Kecerdasan Buatan dalam Berbagai Sektor: Dampak, Peluang, dan Tantangan." Jurnal Cakrawala Ilmiah 3 (12): 3831–3838.

Putri, Nadea Aulia. (2024). Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana Kekerasan Seksual Berbasis Elektronik Artificial Intelligence (Deepfake Porn). Undergraduate Thesis, UPN "Veteran" Jawa Timur.

R. Dremliuga, and A. Korobeev. (2021). "A Fight Against the Dissemination of Deepfakes in Other Countries: Criminal and Criminological Aspects." Russian Journal of Criminology.

Rana, M., B. Murali Nobi, and A. Sung. (2022). "Deepfake Detection: A Systematic Literature Review." IEEE Access 10: 25494–25513.

Respati, Adnasohn Aqilla, Astri Dewi Setyarini, Dodi Parlagutan, Muhammad Rafli, Rayhan Syahbana Mahendra, and Andriyanto Adhi Nugroho. (2024). "Analisis Hukum terhadap Pencegahan Kasus Deepfake serta Perlindungan Hukum terhadap Korban." Media Hukum Indonesia 2 (2).

Riadi, Bambang, Rahmat Prayogi, and Christina Natalia Setyawati. (2024). Media Animasi Berbasis Artificial Intelligence: Teori dan Praktik. Jakarta: Selat Media.

Rohmawati, Indah, Amir Junaidi, and Ariy Khaerudin. (2024). "Urgensi Regulasi Penyalahgunaan Deepfake sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)." Innovative: Journal of Social Science Research 4 (6): 1779–1794.

Rojszczak, Marcin. (2023). "The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content." Institutiones Administrationis – Journal of Administrative Sciences 3 (2): 44–59.

Romero Moreno, Felipe. (2024). "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content." International Review of Law, Computers & Technology 38 (3): 297–326. https://doi.org/10.1080/13600869.2024.2324540

Salsabila, Neydelin Tiara. (2024). "Perlindungan Hukum terhadap Perempuan Korban Pornografi Balas Dendam (Revenge Porn): Studi Kasus Putusan Nomor 147/Pid.B/2023/PN Tlk." Lex Progressium: Jurnal Kajian Hukum dan Perkembangan Hukum 1 (1): 65–79.

Satriawan, Andre, Bahtiar Imran, and Surni Erniwati. (2023). "Identifikasi Kemiripan Foto Asli dan Sketsa Menggunakan Model Generatif Adversarial Network (GANs)." Jurnal Kecerdasan Buatan dan Teknologi Informasi 2 (3): 122–127.

Sharma, Muskan. (2024). "Deepfake Pornography: Examining the Impact on Women's Digital Privacy and Consent." International Journal for Multidisciplinary Research.

Shobirin, Ma'as, Ratih Nurillah Rosyadi, and Elok Fariha Sari. (2025). Tantangan dan Problematika Masyarakat Modern. Bandung: Cahya Ghani Recovery.

Sulianta, Feri. (2025). Masyarakat Digital: Tren, Tantangan, dan Perubahan di Era Teknologi. Bandung: Feri Sulianta.

Syahirah, Sabrina Nur, and Bayu Prasetyo. (2025). "Tinjauan Yuridis terhadap Penggunaan Teknologi Deepfake untuk Pornografi melalui Artificial Intelligence (AI) di Indonesia." Jurnal Inovasi Hukum dan Kebijakan 6 (1).

Wahyudi, B. R. (2025). "Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI." Innovative: Journal of Social Science Research 5 (1): 3436–3450.

Yudha, Musfala. (2024). "Perlindungan Hukum terhadap Data Pribadi Korban Pornografi dengan Penggunaan Deepfake."

Japan Today. "Deepfake Porn: Why We Need to Make It a Crime to Create It, Not Just Share It." retrieved from https://japantoday.com/category/features/opinions/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it

Telisik.id. "Pengakuan Jaksa Tasya: Pertama Kali Wajahnya Dipakai dalam Video Syur Viral." retrieved from https://telisik.id/news/pengakuan-jaksa-tasya-pertama-kali-wajahnya-dipakai-link-video-syur-viral

European Commission. "Digital Services Act: Impact on Online Platforms." retrieved from https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

Kumparan. "Bahaya Deepfake Pornography: Ancaman Serius Teknologi AI di Asia Pasifik." retrieved from https://kumparan.com/bagas-zesi-eka-prasetya/bahaya-deepfake-pornography-ancaman-serius-teknologi-ai-di-asia-pasifik-21TjrS4XDZ8/full

ASIS Online. "U.S. Laws Address Deepfakes." retrieved from https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2021/january/U-S-Laws-Address-Deepfakes/

CNN. "Deepfake Videos Are Increasing." retrieved from https://www.cnn.com/2019/10/07/tech/deepfake-videos-increase/index.html

Daily Journal. "AB-602 and AB-730: Curbing Deepfakes in Pornography and Elections.", retrieved from https://www.dailyjournal.com/articles/355794-ab-602-and-ab-730-curbing-deepfakes-in-pornography-and-elections