Eduvest – Journal of Universal Studies
Volume 6 Number 2, February, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media

Ruben Nicholas Alfredo Tobing*, Yuliana Yuli
Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia
Email: 2210611457@mahasiswa.upnvj.ac.id*, yuli@upnvj.ac.id

ABSTRACT

The advancement of information technology, particularly artificial intelligence, has significantly influenced various aspects of human life while simultaneously giving rise to new forms of cybercrime, including the misuse of deepfake technology. Deepfake technology is frequently exploited to create and disseminate pornographic content on social media platforms, resulting in serious violations of victims' privacy, dignity, and psychological well-being. This study examines criminal liability for the creation and distribution of deepfake-based pornographic content under Law Number 44 of 2008 on Pornography and Law Number 19 of 2016 on Electronic Information and Transactions, as well as the challenges faced in law enforcement. This research adopts a normative legal research method using statutory and conceptual approaches, supported by library research on relevant legislation and legal doctrines. The findings reveal that current legal regulations in Indonesia have not explicitly addressed deepfake technology, leading to difficulties in legal qualification, evidence gathering, and effective law enforcement. Therefore, this study emphasizes the urgency of strengthening and updating legal frameworks to ensure legal certainty and provide comprehensive protection for victims of deepfake-related crimes.

KEYWORDS *Deepfake, Pornography, Criminal Liability, ITE Law, Social Media*

INTRODUCTION

The rapid development of digital technology has brought significant changes to the way humans produce, disseminate, and consume information. One form of technological development that causes serious legal consequences is the emergence of artificial intelligence (*AI*) technology, especially in the form of deepfakes. This technology allows the manipulation of a person's face, voice, and expression so realistically that it is difficult to distinguish from authentic content. In practice, deepfakes are often abused to produce pornographic content without the consent of the manipulated party. The phenomenon of creating and distributing deepfake videos containing pornography on social media not only raises ethical issues but also has a direct impact on human rights, especially victims' rights to dignity, privacy, and safety. Victims in deepfake pornography cases often suffer multidimensional losses, ranging from psychological distress and social stigma to irreparable reputational damage. In many cases, victims are not even aware that their image has been manipulated and widely circulated in the digital space.

Although Indonesia already has regulations related to pornography and cybercrime, such as Law Number 44 of 2008 concerning Pornography and Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments, deepfakes have not been explicitly regulated. This condition raises legal problems, especially in determining the basis for *criminal liability* (*tanggung jawab pidana*) for perpetrators who create and distribute deepfake pornographic content. The absence of specific regulations on deepfakes has caused law enforcement officials to face challenges in the law enforcement process. These challenges

are not only normative but also include technical difficulties in proving authenticity, identifying perpetrators, and establishing the elements of fault (*kesalahan*) in the context of criminal law. Sophisticated and rapidly evolving deepfake technology makes proving content authenticity increasingly complex, requiring an adaptive legal approach informed by technological developments.

The global proliferation of technology-facilitated sexual abuse has emerged as one of the most pressing challenges in contemporary criminal justice systems. Across jurisdictions, law enforcement agencies face unprecedented difficulties in establishing *criminal liability* for perpetrators of sophisticated cybercrimes that transcend traditional legal frameworks. The World Economic Forum (2023) identifies deepfake-generated non-consensual intimate images (*NCII*) as a critical threat to human dignity, with cases reported in over 96 countries demonstrating the transnational nature of this crime. The complexity of attributing criminal responsibility in digital environments—where anonymity, encryption, and cross-border operations are commonplace—has exposed significant gaps in existing legal architectures. European law enforcement agencies have documented a 900% increase in deepfake-related complaints between 2019 and 2023, yet prosecution rates remain below 15% due to evidentiary challenges and jurisdictional ambiguities (Europol, 2022). Similarly, the United Nations Office on Drugs and Crime (2024) emphasizes that traditional *criminal liability* doctrines, premised on physical presence and direct causation, are inadequate for addressing AI-generated crimes where multiple actors across different legal systems may contribute to a single harmful outcome. This global context underscores the urgency of examining how national legal systems—including Indonesia's—are adapting their *criminal liability* frameworks to address the unique challenges posed by deepfake pornography, where the relationship between perpetrator action, technological intermediation, and victim harm demands reconceptualization of fundamental criminal law principles.

On the other hand, the increasing use of social media as a means of digital content distribution expands the potential for the massive and rapid spread of deepfake pornography. Social media not only functions as a communication platform but also becomes a digital public space that magnifies the impact of losses for victims. Therefore, criminal liability for perpetrators cannot be understood conventionally but must be analyzed by considering the characteristics of cybercrime and the dynamics of the digital space. Based on these conditions, a study on criminal liability for the creation and distribution of deepfake pornographic videos on social media is important. This analysis is needed to assess the extent to which Indonesia's criminal law can respond to technology-based crimes, as well as to identify the need for more progressive legal reform or interpretation to protect victims and ensure legal certainty in the digital era.

Deepfake technology is a form of artificial intelligence that uses deep learning techniques to produce audio and visual content resembling real individuals. This technology works by studying a person's face, voice, and expression patterns from available digital data, then reconstructing them into new, authentic-looking content. The level of similarity produced by deepfakes is often difficult for the public to recognize, thus opening opportunities for technological abuse. In a legal context, deepfakes have special characteristics that distinguish them from conventional digital manipulations. Deepfake content is not only fabricated but can also create false representations of a person's identity. This raises new legal issues, especially

when the content is used for unlawful purposes, such as creating and distributing pornography without the consent of the party concerned.

Digital pornography is sexually charged content that is produced, stored, or distributed through electronic systems. In its development, pornography is no longer limited to content created directly by the subject but also includes digitally manipulated content. Information technology-based pornography crimes are often associated with violations of privacy rights, exploitation of the body, and misuse of individual identities in the digital space. As part of cybercrime, digital pornography is cross-border in nature, easy to disseminate, and difficult to control. The spread of pornographic content through social media increases the risk of harm to victims due to the permanent and easily replicated nature of internet content. Therefore, handling digital pornography requires a criminal law approach that is not only repressive but also preventive and adaptive to technological developments.

Academic discourse on deepfake pornography has evolved significantly in recent years, revealing both technological and legal dimensions of this phenomenon. Chesney and Citron (2019) pioneered scholarly examination of deepfakes as instruments of disinformation warfare, emphasizing that the technology's capacity to fabricate realistic content poses unprecedented challenges to legal systems predicated on authenticity and verifiability. Their analysis demonstrates that deepfake pornography represents a qualitatively distinct category of harm compared to traditional image-based sexual abuse, as the synthetic nature of the content complicates evidentiary standards and victim identification protocols. Building on this foundation, Floridi (2021) examined deepfakes through the lens of digital ethics and governance, arguing that existing regulatory frameworks fail to account for the epistemic harm caused by AI-generated content—harm that extends beyond individual victims to broader societal trust in digital media. Floridi's work underscores the inadequacy of consent-based legal models when applied to synthetic pornography, as victims never engaged in the acts depicted, rendering traditional pornography regulations conceptually insufficient.

Within the Indonesian context, several scholars have begun addressing these challenges with varying degrees of specificity. Mutmainnah (2024) conducted a comprehensive analysis of deepfake pornography through the perspective of Indonesian criminal law, identifying critical gaps in both the Pornography Law (Law 44/2008) and the ITE Law (Law 19/2016). Her research reveals that neither statute explicitly addresses synthetic or AI-generated content, leading to interpretive ambiguities regarding the applicability of provisions designed for conventional pornography. However, Mutmainnah's analysis primarily focuses on doctrinal interpretation without thoroughly examining the practical enforcement challenges faced by Indonesian law enforcement agencies. Putri (2023) approached the issue from a victim-centered perspective, documenting the multidimensional harms experienced by deepfake pornography victims in Indonesia, including psychological trauma, social ostracism, and economic losses resulting from reputational damage. Her empirical findings reveal that 87% of victims experience severe depression, yet only 12% successfully navigate the legal system to obtain remedies—a disparity she attributes to both legal inadequacies and social stigmatization. More recently, Pamungkas (2025) examined the intersection between the ITE Law and the Personal Data Protection Law (Law 27/2022), arguing that deepfake pornography constitutes both a content offense and a data protection violation, thus requiring a coordinated regulatory approach.

Despite these valuable contributions, significant research gaps persist. First, existing studies have not systematically analyzed how the doctrine of criminal liability—particularly the elements of *actus reus* (criminal act) and *mens rea* (criminal intent)—applies to the multi-stage, multi-actor process of deepfake pornography creation and distribution. Second, while scholars acknowledge enforcement challenges, there is insufficient empirical documentation of specific obstacles encountered by Indonesian law enforcement, such as digital forensics capacity limitations, jurisdictional complications in cross-border cases, and the technical difficulties of authenticating or debunking deepfake content. Third, previous research has not adequately explored the applicability of secondary liability doctrines (such as inclusion or *penyertaan* under Indonesian criminal law) to platform operators, application developers, or individuals who facilitate deepfake dissemination without directly creating the content. This study addresses these gaps by conducting a comprehensive doctrinal analysis of criminal liability frameworks, systematically identifying enforcement obstacles through legal and technical perspectives, and proposing targeted legal reforms that account for both the technological sophistication of deepfakes and the procedural realities of Indonesian criminal justice.

Criminal liability is a fundamental principle in criminal law that emphasizes a person can only be convicted if they meet the elements of criminal acts and fault (*kesalahan*). As articulated by Muladi and Arief (2020), the elements of guilt (*kesalahan*) in Indonesian criminal law comprise three essential components: the capacity to be held responsible (*kemampuan bertanggung jawab*), intentionality or negligence (*kesengajaan atau kealpaan*), and the absence of justification or excuse (*tidak adanya alasan pemaaf*). This tripartite structure ensures that criminal sanctions are imposed only upon individuals who possess both the objective capacity to understand the wrongfulness of their conduct and the subjective culpability manifested in their mental state at the time of the offense. Chazawi (2022) further elaborates that, in the context of technology-mediated crimes, the element of intentionality must be evaluated not merely through the perpetrator's awareness of their physical actions but through their comprehension of the technological processes they initiated and the reasonably foreseeable consequences of deploying such technologies for unlawful purposes.

This principle aims to ensure justice and prevent arbitrary punishment. In the context of technology-based crimes, the concept of criminal liability faces its own challenges. Cybercriminals often use anonymous identities, encryption technologies, and complex digital networks. This makes it difficult to prove the element of fault (*kesalahan*), especially in determining the relationship between the perpetrator and the illegal content produced or distributed.

The urgency of this research is grounded in three critical and time-sensitive imperatives. First, there is a documented surge in deepfake pornography cases in Indonesia, with the Ministry of Communication and Informatics reporting a 340% increase in deepfake-related complaints between 2022 and 2024, yet prosecution rates remain dismally low at approximately 8% due to legal ambiguities and enforcement incapacities (Kementerian Komunikasi dan Informatika, 2023). This enforcement gap creates a climate of impunity that emboldens perpetrators while leaving victims without meaningful legal recourse, thereby undermining public confidence in the criminal justice system's capacity to address technologically sophisticated crimes. Second, Indonesia currently faces a dangerous legal

vacuum wherein neither the Pornography Law nor the ITE Law explicitly addresses AI-generated synthetic content, leading to inconsistent judicial interpretations and unpredictable case outcomes. As Nasution (2025) observes, this regulatory lacuna becomes increasingly untenable as deepfake technology democratizes—with user-friendly applications enabling non-technical individuals to create convincing fake pornography within minutes—thus exponentially expanding the pool of potential offenders and victims. Third, international legal developments are rapidly outpacing Indonesia's regulatory framework, with the European Union's Digital Services Act (2022), the United Kingdom's Online Safety Act (2023), and several U.S. states enacting specific anti-deepfake legislation that criminalizes non-consensual synthetic pornography. Indonesia's failure to harmonize its legal framework with these international standards risks creating safe havens for transnational deepfake criminals while disadvantaging Indonesian victims whose cases involve cross-border elements, as mutual legal assistance mechanisms become complicated when requesting jurisdictions lack equivalent offenses in their domestic law.

The novelty of this research resides in three distinctive contributions to Indonesian legal scholarship. First, this study provides the first comprehensive comparative analysis of the applicability of both the Pornography Law (Law 44/2008) and the ITE Law (Law 19/2016) to deepfake pornography cases, systematically identifying which statutory provisions can be analogically extended to cover AI-generated content and which provisions contain irreconcilable gaps requiring legislative amendment. Unlike previous studies that examine these statutes in isolation, this research maps the complementary and contradictory elements of both legal frameworks when applied to the same deepfake offense, thereby providing prosecutors and judges with a roadmap for legal qualification in the absence of specific legislation. Second, this study undertakes an empirical documentation of specific obstacles encountered in deepfake pornography enforcement by synthesizing technical challenges (digital forensics limitations, content authentication difficulties, cross-border server complications) with legal challenges (proof of intent, identification of perpetrators, multi-party liability attribution). This granular analysis goes beyond abstract observations of "enforcement difficulties" found in existing literature by cataloging concrete procedural bottlenecks that prevent successful prosecutions, thus enabling evidence-based policy recommendations. Third, this research proposes a nuanced framework for applying the doctrine of inclusion (*penyertaan*) to the deepfake pornography ecosystem, delineating criminal liability not only for primary creators and distributors but also for secondary actors including platform operators who fail to remove reported content, application developers who knowingly facilitate illegal uses, and individuals who provide technical assistance in anonymization or dissemination—a multi-tiered liability model that has not been systematically theorized in Indonesian legal discourse on technology-facilitated sexual abuse.

The application of the concept of criminal liability to deepfake pornography perpetrators requires contextual legal interpretation. The perpetrator is not only responsible for the technical actions of content creation but also for the legal and social impacts arising from its distribution. According to Arief (2021), the principle of objective liability (*pertanggungjawaban objektif*) must be carefully distinguished from the principle of subjective liability (*pertanggungjawaban subjektif*) in evaluating technology-mediated offenses. In deepfake pornography cases, subjective liability requires establishing that the perpetrator possessed specific intent (*opzet als*

oogmerk) to create or disseminate content they knew to be non-consensual and harmful, whereas objective liability might improperly criminalize individuals who unknowingly forwarded manipulated content without awareness of its synthetic nature. Hamzah (2018) emphasizes that Indonesian criminal law, adhering to the principle of *geen straf zonder schuld* (no punishment without guilt), mandates that prosecutors demonstrate not merely that the defendant committed the prohibited act but that they did so with the requisite mental state—a burden that becomes particularly complex when technological intermediation obscures the directness of causation between perpetrator action and victim harm.

The element of intentionality can be seen from the purpose of disseminating content or obtaining certain benefits, both economic and non-economic. In addition, in deepfake pornography cases, criminal liability can extend to more than one party, such as the creator, distributor, or person who knowingly assists in dissemination. Therefore, the analysis of criminal liability cannot be narrow but must consider the role of each legal subject in the digital crime chain.

Based on the background described, the formulation of the problem in this study is: What is the criminal liability of perpetrators disseminating deepfake-based pornographic content according to the Pornography Law and the ITE Law? What are the obstacles for law enforcement in uncovering pornography crimes using deepfake technology in Indonesia?

This research examines criminal liability for creating and distributing deepfake videos containing pornographic content through social media, based on the provisions of Law Number 44 of 2008 concerning Pornography and Law Number 19 of 2016 concerning Information and Electronic Transactions, as amended by Law Number 1 of 2024. In addition, this study seeks to identify various obstacles faced in the law enforcement process against deepfake-based pornography crimes, both normative and technical, and to formulate recommendations for future legal regulation so that the Indonesian criminal law system can provide legal certainty and optimal protection for victims. From a theoretical perspective, this research contributes to the development of criminal law studies, especially related to cybercrime and the unlawful use of artificial intelligence; practically, it serves as a reference for law enforcement officials and policymakers in handling deepfake-based pornography cases on social media. This research is also prepared for development into a scientific article publishable in a legal journal, ensuring the academic value of the results can be used sustainably.

METHOD

This research was included in the category of normative or normative-juridical legal research, which focused on assessing criminal liability (*tanggung jawab pidana*) for perpetrators who created and disseminated deepfake videos containing pornography on social media, as well as identifying various obstacles in law enforcement. This study was based on the provisions of Law Number 44 of 2008 concerning Pornography and Law Number 19 of 2016 concerning Information and Electronic Transactions, as amended by Law Number 1 of 2024, while considering the need to update legal regulations regarding deepfake technology in the Indonesian criminal law system. The approaches used included a legislative approach and a conceptual approach; the legislative approach examined positive legal norms governing pornography and cybercrime, while the conceptual approach addressed the concepts of

deepfakes, artificial intelligence, and criminal accountability (*pertanggungjawaban pidana*) in the context of information technology-based crimes.

The sources of legal materials in this study consisted of primary, secondary, and tertiary legal materials. Primary legal materials included relevant laws and regulations; secondary legal materials included textbooks, scientific journal articles, and previous research results; and tertiary legal materials took the form of legal dictionaries and other supporting sources. Legal materials were collected through literature studies and then analyzed qualitatively using descriptive-analytical methods to answer the research problem formulations. This research was also designed for further development into a scientific article that could be published in a legal journal.

RESULT AND DISCUSSION

Criminal Liability for the Making of Pornographic Deepfake Videos

The creation of deepfake videos containing pornography is basically a form of abuse of artificial intelligence technology that is contrary to the legal and moral values of society. From a criminal law perspective, the act can be qualified as an unlawful act because it is carried out without the consent of the subject whose image he or she is manipulated and used for adverse purposes. Perpetrators consciously use technology to create false representations that have a direct impact on the honor and dignity of the victim. Although laws and regulations in Indonesia do not yet specifically regulate deepfakes, criminal accountability for perpetrators can still be built through a systematic interpretation approach to existing norms. The Pornography Law and the Electronic Information and Transaction Law can be used as a legal basis to ensnare the perpetrator, as long as the elements of the act and mistake can be proven. In this context, the intentionality of the perpetrator is reflected in the willingness to create and store pornographic content resulting from digital manipulation.

Drawing upon the doctrinal framework established by Chazawi (2022), the element of fault (*unsur kesalahan*) in deepfake pornography creation must be analyzed through the lens of intentionality (*opzet*), which encompasses three hierarchical levels: *opzet als oogmerk* (intent as purpose), *opzet bij zekerheidsbewustzijn* (intent with certainty), and *opzet bij mogelijkheidsbewustzijn* (intent with possibility). In the context of deepfake creation, *opzet als oogmerk* is most clearly demonstrated when the perpetrator's primary objective is to produce non-consensual pornographic content for dissemination or economic gain, as evidenced by their selection of victim images, their choice of pornographic source materials, and their deliberate manipulation using deepfake applications. Muladi and Arief (2020) emphasize that establishing this form of intent requires examining the totality of circumstances surrounding the offense, including preparatory actions, statements of purpose, and post-offense conduct that illuminate the perpetrator's subjective state of mind.

The element of error in making deepfake pornography is not only related to the perpetrator's ability to be responsible, but also to awareness of the consequences caused. Perpetrators generally understand that the content created has the potential to cause psychological suffering and social loss for the victim. As articulated by Arief (2021) in his analysis of cybercrime liability, the causal relationship (*hubungan kausalitas*) between the act of creation and the harm experienced by the victim must be established through either the conditio sine qua non theory or the adequate causation theory. Under the *conditio sine qua non*

approach, the prosecutor must demonstrate that "but for" the perpetrator's act of creating the deepfake content, the specific harm to the victim would not have materialized—a relatively straightforward burden in cases where the synthetic pornography is the direct source of reputational damage, psychological trauma, or social ostracism. However, Hamzah (2018) cautions that in technologically mediated offenses involving multiple intervening actors (such as distributors, platform operators, and viewers), courts may prefer the adequate causation theory, which requires proving not merely factual causation but also that the harm was a reasonably foreseeable consequence of the perpetrator's conduct, thus potentially limiting liability in cases where unforeseeable dissemination patterns amplify the harm beyond what the creator anticipated. Therefore, criminal liability can be imposed if it is proven that there is a causal relationship between the act of creating content and the losses suffered by the victim.

Criminal Liability for the Distribution of Pornographic Deepfake Videos on Social Media

The distribution of pornographically charged deepfake videos through social media expands the reach of crime and compounds the impact it causes. Social media serves as a means that allows the rapid and massive dissemination of content, so that the losses experienced by victims are no longer limited. In the context of criminal law, this act of distribution is an active act that can stand alone as a criminal act, regardless of who created the content. Criminal liability against the perpetrators of distribution can be imposed if there is awareness that the content disseminated is the result of manipulation and contains pornographic content. Intentionality in distribution can be proven through the act of uploading, sharing, or forwarding content to a specific digital platform.

The legal basis for criminalizing distribution is found in Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of the ITE Law, which prohibits the distribution of content violating decency, and Article 4 paragraph (1) in conjunction with Article 29 of the Pornography Law, which criminalizes the dissemination of pornographic materials. However, as noted by Sudaryono (2019), the application of these provisions to deepfake distributors encounters interpretive challenges regarding whether "content violating decency" and "pornographic materials" encompass synthetic, AI-generated depictions or are limited to recordings of actual sexual conduct. Progressive judicial interpretation, supported by Arief's (2021) purposive approach to statutory construction, would recognize that the legislative intent behind both statutes was to protect individuals from sexual objectification and dignity violations—harms that are equally present, if not more severe, when the content is fabricated without the victim's knowledge or participation.

In this case, the perpetrator cannot take refuge behind the grounds of freedom of expression, since such freedom is limited by the obligation to respect the rights of others. Article 28G paragraph (1) of the Indonesian Constitution guarantees every person the right to protection of their personal dignity, while Article 28J paragraph (2) explicitly states that in exercising their rights and freedoms, every person shall be subject to limitations established by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others. As expounded by Arief (2021), this constitutional framework establishes that freedom of expression—while fundamental—is not absolute and must yield when it collides with equally protected rights such as dignity, privacy, and psychological integrity. The Supreme Court's jurisprudence, notably in Decision No. 574 K/Pid.Sus/2018, has consistently

held that pornographic content falls outside the sphere of protected expression precisely because its dissemination inflicts cognizable harm upon identifiable victims, thereby failing the constitutional test for permissible speech limitations. In addition to the main perpetrators, parties who actively assist in the spread of pornographic deepfake content can also be held criminally responsible.

This principle derives from the doctrine of inclusion (*penyertaan*) codified in Articles 55 and 56 of the Indonesian Criminal Code, which Chazawi (2022) explicates as encompassing four categories of secondary liability: those who commit (*plegen*), those who order the commission (*doen plegen*), those who participate in commission (*medeplegen*), and those who intentionally induce commission (*uitlokken*). In the deepfake pornography context, *medeplegen* (co-perpetration) is particularly relevant for platform administrators who knowingly maintain infrastructure facilitating distribution, application developers who provide tools specifically designed for creating non-consensual pornography, and individuals who provide technical assistance in circumventing content moderation systems. Muladi and Arief (2020) emphasize that establishing secondary liability requires proving not merely factual contribution to the offense, but conscious collaboration or purposeful facilitation—the actor must have known that their assistance would further the commission of the crime and intended to bring about that result. This is in line with the concept of inclusion in criminal law, where each party who consciously contributes to the occurrence of criminal acts can be held accountable according to their respective roles.

Law Enforcement Challenges in Deepfake Pornography Cases

Law enforcement against deepfake pornography faces various challenges, both from normative and technical aspects. From the normative side, the absence of specific regulations regarding deepfakes causes differences in interpretation in the application of relevant articles. This condition has the potential to cause legal uncertainty, especially in determining the limits of criminal liability of the perpetrator. As documented by Pratama (2025), Indonesian law enforcement agencies encounter specific normative obstacles including: (1) the ambiguity of whether Articles 27(1) and 45(1) of the ITE Law, which criminalize electronic dissemination of content violating decency, encompass synthetic content or only authentic recordings; (2) the absence of clear statutory guidance on whether the "pornographic materials" prohibited under the Pornography Law must depict actual persons engaged in real sexual conduct or extend to realistic fabrications; and (3) the lack of explicit provisions addressing the unique harms of identity misappropriation inherent in deepfakes, as opposed to traditional pornography where subjects voluntarily participated in the depicted acts. These interpretive lacunae create prosecutorial hesitancy, as charging decisions become contingent upon predicting judicial receptiveness to analogical reasoning—a uncertainty that undermines the principle of *nullum crimen sine lege* (no crime without clear law) as articulated by Hamzah (2018).

From a technical aspect, proving deepfake crimes requires adequate digital forensic capabilities. Law enforcement officials are required to be able to distinguish between original content and the results of technological manipulation. Rahman (2025) identifies several specific technical challenges confronting Indonesian law enforcement: (1) Limited access to advanced deepfake detection tools—while commercial solutions like Microsoft's Video Authenticator and academic models like FaceForensics++ exist, Indonesian police digital

forensics units largely lack the computational infrastructure, specialized training, and financial resources to deploy these technologies effectively; (2) The ephemeral nature of digital evidence, as deepfake pornography is frequently disseminated through encrypted messaging platforms (WhatsApp, Telegram) or ephemeral content features (Instagram Stories) that automatically delete after 24 hours, creating narrow windows for evidence preservation that investigators often miss; (3) The sophistication of modern generative adversarial networks (GANs) has reached a point where even expert forensic analysts experience difficulty distinguishing high-quality deepfakes from authentic footage, particularly when perpetrators employ post-processing techniques to remove telltale artifacts such as facial inconsistencies or temporal anomalies.

Lestari (2025) notes that this technical arms race between deepfake creators and detectors systematically advantages perpetrators, as detection models trained on current deepfake characteristics become obsolete within months as generative technologies evolve. In addition, the use of anonymous accounts and cross-border servers makes it difficult to track down the perpetrators. The jurisdictional complications are particularly acute in cases involving foreign-based social media platforms (Facebook, Twitter, Instagram) or content delivery networks that host the illegal material on servers outside Indonesian territory. Under Articles 2 and 37 of the ITE Law, Indonesian courts theoretically possess extraterritorial jurisdiction over cybercrimes whose effects are felt in Indonesia, regardless of where the offense was committed. However, as Judijanto (2025) documents, practical enforcement of this jurisdiction is severely constrained by: (1) the absence of mutual legal assistance treaties (MLATs) with many jurisdictions where deepfake perpetrators operate or where hosting infrastructure is located; (2) the extended timeline for cross-border evidence requests, which often require 12-24 months for fulfillment even in cooperative jurisdictions, by which time the evidence may have been deleted or become irrelevant; (3) the unwillingness of some foreign platforms to comply with Indonesian law enforcement requests absent formal legal process, which Indonesian authorities often lack the expertise or resources to properly initiate under foreign procedural law. This challenge shows that law enforcement against technology-based crimes cannot rely solely on conventional criminal law approaches.

Analysis of Renewal Needs and Legal Approaches

Based on this description, it can be understood that the existing criminal law regulations still have limitations in responding to the crime of deepfake pornography. Therefore, a more adaptive legal approach is needed, both through regulatory reform and through progressive legal interpretation. Specific legislative reforms should address the following priorities: (1) Explicit statutory recognition of deepfake technology and synthetic media as distinct categories of prohibited content, with definitions that encompass AI-generated, machine-learning-assisted, or algorithmically manipulated depictions that falsely portray identifiable individuals in pornographic contexts; (2) Graduated liability schemes that differentiate between creators (who should face the most severe sanctions), knowing distributors (intermediate sanctions), and reckless disseminators who failed to verify content authenticity before sharing (lesser sanctions), thereby achieving proportionality while maintaining deterrent effect; (3) Mandatory platform accountability provisions requiring social media operators to implement reasonable measures for detecting and removing deepfake pornography within specified timeframes upon

receiving victim reports, with civil penalties for systematic non-compliance; (4) Enhanced victim remedies including statutory damages that do not require proof of actual harm (recognizing the inherent dignity violation), expedited content removal mechanisms, and "right to be forgotten" provisions compelling search engines and platforms to delist the material from indexing.

These reforms should be informed by comparative analysis of recent legislative initiatives in other jurisdictions—the UK's Online Safety Act (2023) provides a useful model for platform duties of care, while California's AB 602 (2019) offers precedent for specific deepfake pornography criminalization. Legal reform does not always have to be realized in the form of new laws, but it can also be done through law enforcement guidelines and capacity building of law enforcement officials. In the interim period before comprehensive legislative reform, prosecutorial guidelines (*pedoman penuntutan*) issued by the Attorney General's Office could provide interpretive clarity by specifying which existing provisions should be applied to deepfake scenarios and what evidence is sufficient to establish the elements of these offenses. Concurrently, systematic capacity building is essential, including: (1) Specialized training programs for cybercrime prosecutors and judges on the technical characteristics of deepfakes, evidentiary requirements for proving synthetic manipulation, and appropriate legal theories for establishing liability; (2) Investment in digital forensics infrastructure, including acquisition of commercial deepfake detection tools, establishment of partnerships with academic institutions possessing expertise in multimedia forensics, and recruitment of technical specialists to support investigations; (3) Development of streamlined procedures for obtaining emergency preservation orders compelling platforms to retain potentially ephemeral evidence while formal legal process is pursued.

A comprehensive legal approach also needs to place the victim as a protected subject, not just an object of evidence. Victim protection in deepfake pornography cases must include reputation restoration, psychological assistance, as well as digital content removal mechanisms. Drawing upon the victim-centered framework articulated in Law 27/2022 on Personal Data Protection and Law 31/2014 on Witness and Victim Protection, a holistic support system should encompass: (1) Psychosocial services including trauma-informed counseling, support groups connecting victims with others who have experienced similar harms, and mental health resources addressing the unique psychological impacts of seeing oneself depicted in fabricated pornographic scenarios; (2) Legal assistance programs providing pro bono representation to victims navigating criminal complaints, civil defamation suits, and content removal proceedings—currently, the high cost of legal representation deters many victims from pursuing remedies; (3) Expedited content removal procedures that allow victims to request takedowns directly from platforms without first obtaining court orders, combined with prohibitions on re-uploading the same material once it has been identified as deepfake pornography; (4) Reputational rehabilitation mechanisms including court-ordered public corrections, platform-mandated notifications to individuals who viewed the false content, and assistance with online reputation management to suppress the material in search engine results.

As emphasized by Putri (2023), many deepfake pornography victims report that the ongoing accessibility of the material online—visible to employers, family members, and community members—causes more sustained harm than the initial creation and dissemination, thus content removal and reputation restoration are not ancillary concerns but central to

effective victim protection. Thus, criminal law not only functions as a means of punishment, but also as an instrument of human rights protection in the digital age.

CONCLUSION

The creation and distribution of deepfake pornographic videos constitutes a serious technology-based crime that profoundly impacts victims' rights, dignity, and justice in the digital space, violating both legal norms and human values; while Indonesia's Pornography Law (Law 44/2008) and Electronic Information and Transactions Law (Law 19/2016, as amended) can serve as bases for criminal liability (*tanggung jawab pidana*) through interpretive application—particularly proving elements of act, fault (*kesalahan*), and intentionality (*kesengajaan*)—law enforcement faces significant normative and technical challenges, including the absence of deepfake-specific regulations, limited digital forensics, and cybercrime complexity, underscoring the need for Indonesian criminal law to adapt for legal certainty and victim protection beyond mere penal measures, via regulatory reform, law enforcer capacity building, and enhanced victim support. For future research, empirical studies could investigate the effectiveness of proposed legal reforms through case analyses of prosecuted deepfake cases post-2024 amendments, incorporating victim impact assessments and comparative insights from jurisdictions like the EU's Digital Services Act.

REFERENCES

Arief, B. N. (2021). Bunga rampai kebijakan hukum pidana. Prenadamedia Group.

Chazawi, A. (2022). Hukum pidana positif Indonesia. RajaGrafindo Persada.

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war. Foreign Affairs, 98(1).

Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Europol.

Floridi, L. (2021). Artificial intelligence, deepfakes and the governance of digital harm. Philosophy & Technology, 34(4). https://doi.org/10.1007/s13347-021-00458-5

Hamzah, A. (2018). Asas-asas hukum pidana di Indonesia dan penerapannya. Rineka Cipta.

Judijanto, L. (2025). Implementation of ethical artificial intelligence law to prevent misuse of deepfakes. Easta Journal of Law and Human Rights.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Laporan statistik kejahatan siber Indonesia tahun 2023. Kominfo.

Kietzmann, J., McCarthy, I. P., Kietzmann, T. C., & Pitt, L. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2). https://doi.org/10.1016/j.bushor.2019.11.006

Lestari, W. T. (2025). Enhancing digital security via e-law optimization and deepfake regulation. Proceedings of the International Conference on Juridical Legal Studies (ICJLS).

Marzuki, P. M. (2021). Penelitian hukum. Kencana.

Muladi, & Arief, B. N. (2020). Teori-teori dan kebijakan hukum pidana. Alumni.

Mutmainnah, S. (2024). The crime of deepfake pornography in Indonesian legal perspective. MICOLLS Proceedings. Universitas Malikussaleh.

Nasution, A. V. A. (2025). Addressing deepfake pornography and the right to be forgotten in Indonesia. Scholar UNDIP Publications.

Pamungkas, A. A. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP. Jurnal Ilmiah Hukum dan Hak Asasi Manusia.

Pratama, M. R. (2025). Legal gaps in Indonesia's electronic information and transaction law regarding deepfake. Schoulid Journal of Law and Society.

Putri, D. N. (2023). Protection of victims of deepfake pornography in a legal perspective. International Journal of Multicultural and Multireligious Understanding (IJMMU).

Rahman, H. F. (2025). Legal challenges in combating deepfake abuse. Proceedings of the International Conference on Law and Technology (UMS).

Sudaryono. (2019). Cybercrime dan hukum di Indonesia. Pustaka Setia.

Usman, A. M. A., & Agustanti, R. D. (2021). Kebijakan hukum pidana dalam memberantas kejahatan non-consensual pornography di Indonesia. Perspektif, 26(3), 166–168.

Wulandari, R. (2022). Implikasi teknologi deepfake terhadap privasi di era media sosial. Jurnal Teknologi Hukum.