DOI: 10.46924/jihk.v8i1.496

Reconstructing Legal Protection for Deepfake Victims in Indonesia

Fathah Oscar[1*], Femmy Silaswaty[2], & Hanuring Ayu Ardhani Putri[3]

[1,2,3]Universitas Islam Batik Surakarta, Indonesia

Correspondence

Fathah Oscar, Universitas Islam Batik Surakarta, Indonesia, Jl. Agus Salim No.10, Sondakan, Kec. Laweyan, Kota Surakarta, Jawa Tengah 57147, *e*-mail: oscar.fathah@gmail.com

How to cite

Oscar, Fathah., Silaswaty, Femmy., & Putri, Hanuring Ayu Ardhani. 2026. Reconstructing Legal Protection for Deepfake Victims in Indonesia. *Jurnal Ilmu Hukum Kyadiren* 8(1), 746-766. https://doi.org/10.46924/jihk.v8i1.496

Original Article

Abstract

The rapid advancement of artificial intelligence (AI), particularly deepfake video technology, presents significant challenges to the protection of privacy, digital identity, and legal certainty. These challenges are exacerbated by the absence of a comprehensive legal framework governing deepfakes under Indonesian law. This study aims to analyze the regulation of deepfake technology under the Electronic Information and Transactions (ITE) Law, the Personal Data Protection Law, and the Indonesian Criminal Code; evaluate the effectiveness of existing legal protection for deepfake victims; and formulate a cyber law–based legal protection model. This research employs a normative legal methodology using qualitative analysis through statutory, conceptual, case, and comparative approaches. The findings indicate that the current legal framework remains fragmented and fails to provide a clear legal definition of deepfakes, standardized digital forensic procedures, an effective takedown-and-staydown mechanism, or an integrated system of victim protection. In response to these shortcomings, this study proposes a Legal Protection Model for Deepfake Video Victims Based on the Deepfake Life Cycle, integrating preventive, repressive, and restorative legal approaches. The proposed model is intended to strengthen legal certainty, safeguard digital identity, enhance the effectiveness of cyber law enforcement, and ensure comprehensive protection and recovery for victims of deepfake-related offenses.

Keywords: *Artificial Intelligence, Cyber Law, Deepfake Videos, Victim Protection*

Abstrak

Perkembangan teknologi artificial intelligence, khususnya video deepfake, menimbulkan tantangan serius terhadap perlindungan privasi, identitas digital, dan kepastian hukum karena hukum positif Indonesia belum mengatur teknologi tersebut secara komprehensif. Kajian ini bertujuan menganalisis pengaturan hukum deepfake dalam UU ITE, UU Pelindungan Data Pribadi, dan KUHP, mengevaluasi efektivitas perlindungan hukum bagi korban, serta merumuskan model perlindungan hukum berbasis cyber law. Penelitian menggunakan metode hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, kasus, dan komparatif yang dianalisis secara kualitatif. pengaturan yang ada masih terpisah-pisah, belum memiliki definisi hukum deepfake, standar forensik digital, mekanisme takedown-and-staydown, maupun perlindungan korban yang terintegrasi. Kajian ini merumuskan Model Perlindungan Hukum Korban Video Deepfake Berbasis Deepfake Life Cycle yang mengintegrasikan pendekatan preventif, represif, dan restoratif untuk memperkuat kepastian hukum, perlindungan identitas digital, efektivitas penegakan hukum, serta pemulihan korban.

Kata kunci: *Data Pribadi, Deepfake Video, Hukum Siber, Perlindungan Korban*

1. INTRODUCTION

The rapid advancement of artificial intelligence (AI) has fundamentally transformed the digital landscape, including the emergence of deepfake technology, which uses deep learning algorithms to generate highly realistic synthetic images, videos, and audio that replicate an individual's facial features, voice, expressions, and movements. This technology offers substantial benefits across a wide range of sectors, including the creative industries, education, entertainment, and digital media production. Despite these advantages, deepfakes also present significant risks by facilitating new forms of abuse that threaten privacy, personal data protection, digital identity, and public confidence in digital information.

Unlike traditional forms of digital manipulation, deepfakes are capable of producing audiovisual content that is virtually indistinguishable from authentic recordings, thereby undermining the reliability and authenticity of digital evidence. The widespread use of social media platforms and other digital communication channels has accelerated the dissemination of deepfake content, amplifying its societal impact and making its removal increasingly difficult. Consequently, the rapid evolution of AI technology has given rise to an emerging category of cybercrime that demands a comprehensive and adaptive legal response.

The harmful consequences of malicious deepfake content extend far beyond the dissemination of misinformation. Deepfakes have been used to facilitate invasions of privacy, identity theft, defamation, fraud, extortion, technology-enabled sexual exploitation, and other forms of digital abuse. For victims, the resulting harm is multidimensional, encompassing economic loss, psychological trauma, social stigmatization, and reputational damage. Unlike conventional offenses, the harm caused by deepfakes may persist indefinitely because the content can be copied, modified, redistributed, and archived across multiple digital platforms without the victim's knowledge or consent.

Accordingly, effective legal protection should extend beyond imposing criminal sanctions on perpetrators. A comprehensive legal framework must also provide mechanisms to halt the dissemination of harmful content, remove or disable access to deepfake materials, erase digital traces where feasible, safeguard personal data, restore victims' reputations, and facilitate psychological and legal recovery. Moreover, the adjudication of deepfake-related offenses increasingly depends on sophisticated digital forensic techniques and reliable electronic evidence capable of verifying the authenticity and integrity of digital content. These developments require judicial institutions and law enforcement agencies to adapt their evidentiary standards and investigative practices to the evolving capabilities of AI technology.

In Indonesia, legal provisions relevant to deepfake-related offenses are dispersed across several statutory instruments, including Law No. 1 of 2024 concerning

Electronic Information and Transactions (ITE Law), Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), and the Indonesian Criminal Code. Although these legal instruments regulate electronic information, personal data protection, and criminal offenses committed through digital media, none specifically addresses the unique characteristics of deepfake technology. Existing legislation also lacks clear provisions concerning the legal definition of deepfakes, standards for authenticating AI-generated electronic evidence, the liability of digital platform providers, and comprehensive mechanisms for victim protection and redress.

This fragmented regulatory framework creates substantial legal uncertainty and underscores the need for a more integrated legal approach. Against this background, this study seeks to analyze Indonesia's existing legal framework governing deepfake videos, evaluate the effectiveness of current legal protections available to victims, and develop a cyber law–based legal protection model that integrates preventive, repressive, and restorative dimensions. The proposed model is intended to strengthen legal certainty, enhance the protection of digital rights, improve institutional responses to AI-enabled cybercrime, and provide comprehensive remedies for victims of deepfake-related offenses.

The issue of legal protection for deepfake victims has attracted growing attention in both international and domestic legal scholarship. A seminal study by Chesney and Citron identified deepfakes as a multidimensional threat to individual rights, democratic institutions, national security, and the integrity of the digital information ecosystem. The authors argue that advances in machine learning have enabled the creation of highly convincing synthetic audiovisual content and propose a range of regulatory responses, including AI detection technologies, criminal sanctions, civil liability, administrative regulation, and digital authentication mechanisms.[1] Similarly, Kietzmann et al. examine how synthetic media erodes public trust in audiovisual evidence and increases the risk of digital identity misuse.[2] Nevertheless, these studies primarily emphasize technology governance and public policy, while offering comparatively limited analysis of comprehensive legal protection and remedies for victims of deepfake-related harms.

From a technical perspective, Diel et al., Farid , and Mirsky and Lee examine scientific approaches to deepfake detection.[3] Mirsky and Lee identify Generative Adversarial Networks (GANs) as the principal technology underlying the creation of

---

1 Robert Chesney and Danielle K. Citron, "Deep Fakes: A Looming Challenge for Priv Es: A Looming Challenge for Privacy, Democr , Democracy, and National Security," *California Law Review* 107 (2019): 1753–820.

2 Jan Kietzmann et al., "Deepfakes: Trick or Treat?," *Business Horizons* 63, no. 2 (2020): 135–46, https://doi.org/10.1016/j.bushor.2019.11.006.

3 Alexander Diel et al., "Human Performance in Detecting Deepfakes: A Systematic Review and Meta-Analysis of 56 Papers," *Computers in Human Behavior Reports* 16 (December 2024): 100538, https://doi.org/10.1016/j.chbr.2024.100538; Hany Farid, "Creating, Using, Misusing, and Detecting Deep Fakes," *Journal of Online Trust and Safety* 1, no. 4 (2022): 1–33, https://doi.org/10.54501/jots.v1i4.56; Yisroel Mirsky and Wenke Lee, "The Creation and Detection of Deepfakes: A Survey," *ACM Computing Surveys* 54, no. 1 (2022): 1–41, https://doi.org/10.1145/3425780.

deepfakes,[4] whereas Farid emphasizes the importance of digital forensic techniques, including metadata analysis, lighting inconsistencies, audio–video synchronization, and visual artifact detection, for authenticating digital content.[5] Diel et al. further demonstrate that individuals generally exhibit limited ability to distinguish authentic videos from manipulated ones, highlighting the necessity of advanced forensic technologies. Although these studies significantly contribute to the development of electronic evidence verification, they do not sufficiently examine the relationship between technical detection methods, legal standards of admissibility, and mechanisms for protecting victims within the judicial process.[6]

Scholarly attention has increasingly shifted toward the protection of victims. Lazard et al. characterize malicious deepfakes as a form of online violence against women (OVAW) and demonstrate that such abuse inflicts long-term psychological, social, and reputational harm.[7] Within the Indonesian context, Palindria et al. emphasize the vulnerability of biometric data under Law No. 27 of 2022 on Personal Data Protection,[8] while Arvitto identifies a regulatory gap resulting from the absence of explicit provisions governing deepfakes in both the Electronic Information and Transactions (ITE) Law and the Personal Data Protection (PDP) Law.[9] Likewise, Noerman and Ibrahim, Kusnadi and Putri, Karo et al., Haida and Nuriyatman (2024), and Meisyah conclude that Indonesia's legal framework provides only fragmented protection and continues to rely heavily on broad judicial interpretation of existing statutory provisions.[10]

Existing scholarship has primarily focused on the regulatory gap surrounding deepfakes, privacy protection, biometric data security, and incremental reforms to criminal law. However, no prior study has comprehensively integrated the ITE Law,

---

4 Mirsky and Lee, "The Creation and Detection of Deepfakes."

5 Farid, "Creating, Using, Misusing, and Detecting Deep Fakes."

6 Diel et al., "Human Performance in Detecting Deepfakes."

7 Lisa Lazard et al., "Deepfake Technology and Gender-Based Violence: A Scoping Review," *Trauma, Violence, & Abuse*, 2025, 15248380251384271, https://doi.org/10.1177/15248380251384271.

8 Arvi Erawan Palindria et al., "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia," *Spektrum Hukum* 21, no. 2 (2024): 110, https://doi.org/10.56444/sh.v21i2.5319.

9 Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP," *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 4, no. 2 (2025): 73–82, https://doi.org/10.35912/jihham.v4i2.3937.

10 Chiquita Thefirstly Noerman and Aji Lukman Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara," *Jurnal Usm Law Review* 7, no. 2 (2024): 603–21, https://doi.org/10.26623/julr.v7i2.8995; Sekaring Ayumeida Kusnadi and Dina Wanda Setiawan Putri, "Perlindungan Hak Privasi Dalam Penyalahgunaan Teknologi Deepfake Di Indonesia," *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 195–210, https://doi.org/10.33331/rechtsvinding.v14i2.2135; Rizky Karo Karo et al., "Analisis Dalam Kasus Penyalahgunaan Deepfake Dari Segi Perlindungan Data Pribadi Dalam UU ITE Dan UU PDP Di Indonesia," *Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial, Dan Hukum* 1, no. 1 (2026): 1–8, https://journal.unj.ac.id/unj/index.php/senpishum/article/view/62862; Rendi Syaputra Nur Haida and Eko Nuriyatman, "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia," *Jurnal Hukum Respublica* 24, no. 1 (2024): 1–13, https://doi.org/10.31849/respublica.v24i01.23327; Meisyah Meisyah, "Perlindungan Hukum Pidana Bagi Pemilik Wajah Yang Digunakan Online Sebagai Hasil Kecerdasan Buatan (Artificial Intelligence)," *Edu Yustisia: Jurnal Edukasi Hukum* 4, no. 2 (2025): 19–24.

the Personal Data Protection Law, the Indonesian Criminal Code, the legal framework governing electronic evidence, the liability of digital platform providers, and victim recovery mechanisms into a unified legal protection framework. The principal contribution of this study lies in the development of a cyber law–based legal protection model for deepfake victims that integrates preventive, repressive, and restorative approaches. Unlike previous studies, the proposed model positions victims as the central subjects of legal protection while systematically incorporating personal data protection, digital evidence, content removal mechanisms, platform accountability, and reputational restoration into a coherent legal framework.

Accordingly, this study aims to analyze the legal regulation of deepfake videos within the Indonesian legal system, evaluate the effectiveness of legal protection available to victims under the Electronic Information and Transactions (ITE) Law, the Personal Data Protection Law, and the Indonesian Criminal Code, and identify regulatory deficiencies relating to electronic evidence, personal data protection, and the liability of digital platform providers. Furthermore, this study proposes a cyber law–based legal protection model that integrates preventive, repressive, and restorative legal measures to strengthen legal certainty, improve institutional responses to AI-enabled cybercrime, and ensure comprehensive protection and effective recovery for victims of deepfake-related offenses.

2. RESEARCH METHODOLOGY

This study employs a normative legal research methodology with a prescriptive-analytical orientation to examine the adequacy of Indonesia's legal framework in protecting victims of deepfake videos from a cyber law perspective. The research is grounded in the *das sollen* approach, which focuses on analyzing statutory provisions, legal principles, doctrines, and scholarly literature to identify normative gaps and inconsistencies and to formulate a more comprehensive model of legal protection.

To achieve these objectives, the study adopts four complementary research approaches. First, the statutory approach examines relevant legal instruments, including the 1945 Constitution of the Republic of Indonesia, the Electronic Information and Transactions (ITE) Law, the Personal Data Protection Law, the Indonesian Criminal Code, and other related legislation. Second, the conceptual approach analyzes the legal concepts of deepfakes, digital identity, personal data protection, electronic evidence, and the liability of digital platform providers. Third, the case approach evaluates the application of existing legal norms in selected cases involving the misuse of deepfake technology. Finally, a limited comparative approach is employed to examine regulatory developments in selected foreign jurisdictions and to identify comparative legal principles relevant to the Indonesian context.

The research relies on primary, secondary, and tertiary legal materials, all of which were collected through an extensive review of legal literature and documentary sources. These materials are analyzed qualitatively using grammatical, systematic, teleological, and prospective interpretative methods to evaluate the coherence and effectiveness of the existing legal framework. The analysis culminates in a doctrinal synthesis that proposes a cyber law–based legal protection model for victims of deepfake-related offenses, integrating preventive, repressive, and restorative legal measures to strengthen legal certainty, enhance the protection of digital rights, and provide comprehensive remedies for victims.

3. RESEARCH RESULT AND DISCUSSION

3.1. Legal Regulation of Deepfake Videos Under Indonesia's Positive Legal System

Indonesia's positive legal system contains several statutory provisions that may be applied to the misuse of deepfake technology. However, these provisions remain sectoral and fragmented and do not constitute a comprehensive legal framework specifically addressing the unique characteristics of deepfake technology. Consequently, the principal legal challenge is not merely the absence of regulation but rather normative fragmentation, which creates uncertainty in the interpretation and application of existing legal norms.

The Electronic Information and Transactions (ITE) Law is the principal statutory instrument governing activities involving deepfake technology because the creation, manipulation, storage, and dissemination of deepfake videos occur entirely within the electronic environment. Article 5 of the ITE Law, which recognizes Electronic Information and/or Electronic Documents as legally admissible evidence, provides the normative basis for victims to establish claims arising from deepfake-related misconduct through digital videos, metadata, screenshots, upload histories, user account information, and the results of digital forensic examinations.

Nevertheless, the legal recognition of electronic evidence has not been accompanied by specific standards governing the authentication of AI-generated audiovisual content. The defining characteristic of deepfake technology is its ability to produce highly convincing synthetic videos that appear authentic despite being generated through algorithmic manipulation.[11] Consequently, proving a deepfake-related offense requires more than establishing the existence of a digital video; it also requires demonstrating that the content has been artificially manipulated through reliable digital forensic methods. At present, however, Indonesian law provides no

[11] Mubarak Alrashoud, "Deepfake Video Detection Methods, Approaches, and Challenges," *Alexandria Engineering Journal* 125 (2025): 265–77, https://doi.org/10.1016/j.aej.2025.04.007.

specific evidentiary standards for authenticating AI-generated audiovisual evidence in judicial proceedings.

Accordingly, Article 5 of the ITE Law functions primarily as a provision recognizing the admissibility of electronic evidence rather than as a regulatory framework governing the authenticity of synthetic media. This finding extends the technical analyses of Diel et al. and Farid, both of whom emphasize the importance of digital forensic technologies in detecting deepfakes.[12] However, the authentication of AI-generated content is not solely a technical issue; it is equally a normative legal issue because Indonesia's positive legal system has yet to establish legal standards for determining the authenticity and evidentiary value of AI-generated audiovisual content before the courts.

Articles 27(1), 27A, 35, and 40 of the ITE Law provide potential legal bases for addressing various forms of deepfake-related misconduct. Article 27(1) may be applied where a deepfake contains content that violates public morality, particularly in cases involving non-consensual sexually explicit deepfakes. Article 27A may be invoked when manipulated audiovisual content is used to attack an individual's honor or reputation through the dissemination of electronic information falsely portraying the victim as having engaged in conduct that demeans their dignity.

The significance of Constitutional Court Decision No. 105/PUU-XXII/2024 lies in its clarification that the offense of defamation under Article 27A must be interpreted as conduct that objectively undermines an individual's honor or reputation. Accordingly, in deepfake-related cases, the legal inquiry should not focus exclusively on the factual accuracy of the audiovisual content. Rather, the decisive issue is whether the manipulated content objectively creates the false impression that the victim engaged in conduct capable of damaging the victim's honor, dignity, or reputation.

These findings differ from much of the existing literature, which primarily characterizes deepfakes as existing within a regulatory vacuum. Arvitto, Kusnadi and Putri, and Noerman and Ibrahim conclude that Indonesia lacks legislation specifically regulating deepfake technology.[13] While the present study agrees that no dedicated deepfake legislation currently exists, it offers a broader doctrinal interpretation by demonstrating that several provisions of the ITE Law already provide normative entry points for addressing deepfake-related misconduct. Accordingly, the central legal problem is not the complete absence of applicable legal norms but rather the lack of an integrated regulatory framework that expressly recognizes synthetic media as a distinct

---

[12] Diel et al., "Human Performance in Detecting Deepfakes"; Farid, "Creating, Using, Misusing, and Detecting Deep Fakes."

[13] Arvitto, "Implikasi Hukum Deepfake"; Kusnadi and Putri, "Perlindungan Hak Privasi Dalam Penyalahgunaan Teknologi Deepfake Di Indonesia"; Kusnadi and Putri, "Perlindungan Hak Privasi Dalam Penyalahgunaan Teknologi Deepfake Di Indonesia"; Noerman and Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara."

subject of legal regulation and establishes legal standards tailored to its unique technological characteristics.

Article 35 of the Electronic Information and Transactions (ITE) Law criminalizes the manipulation, creation, alteration, deletion, or destruction of electronic information with the intent of making it appear authentic. Among the provisions of the ITE Law, this article most closely corresponds to the defining characteristics of deepfake technology, which generates synthetic digital content designed to appear genuine despite being produced through artificial intelligence. Nevertheless, Article 35 continues to rely on the general concept of electronic information manipulation and therefore does not adequately accommodate emerging technologies such as synthetic media, digital replicas, voice cloning, or AI-generated audiovisual content. Accordingly, although Article 35 may serve as a legal basis for prosecuting deepfake-related offenses, it does not provide sufficient legal certainty regarding the increasingly sophisticated forms of AI-enabled digital manipulation.

The Personal Data Protection (PDP) Law is equally significant because the misuse of deepfake technology fundamentally involves the unauthorized use of an individual's facial image, voice, and other biometric characteristics as personal data. This study finds that Articles 1 and 4 of the PDP Law recognize biometric data as a category of specific personal data entitled to enhanced legal protection. Consequently, the use of an individual's facial image or voice to train artificial intelligence systems or to generate deepfake content without valid consent may constitute a violation of the fundamental principles governing personal data processing.

These findings reinforce the conclusions of Palindria et al., who argue that Indonesia's legal framework does not yet provide adequate protection for biometric data.[14] They also extend the analysis of Karo et al., who characterize deepfakes primarily as violations of privacy rights.[15] The present study demonstrates that the legal implications of deepfake technology extend beyond conventional privacy concerns to encompass violations of the data subject's right to control the use and representation of their digital identity.

Despite these protections, the PDP Law continues to exhibit significant normative limitations. The statute does not expressly regulate the use of biometric data for AI model training, the creation of digital replicas, or voice cloning technologies. Furthermore, although data subjects are granted rights to object to data processing, withdraw consent, request data deletion, and seek compensation, these rights are not supported by effective mechanisms for the rapid removal of deepfake content that has been disseminated across multiple digital platforms and jurisdictions. Consequently, the

---

[14] Palindria et al., "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia."

[15] Karo et al., "Analisis Dalam Kasus Penyalahgunaan Deepfake Dari Segi Perlindungan Data Pribadi Dalam UU ITE Dan UU PDP Di Indonesia."

existing framework for personal data protection remains largely confined to the legal relationship between the data controller and the data subject, whereas the transnational and viral nature of deepfake dissemination requires a far more responsive takedown-and-staydown mechanism.

Substantive criminal law likewise plays an important role in addressing the legal consequences of deepfake-related misconduct. Articles 433 (defamation), 434 (false accusation), 438 (false reporting), and 492 (fraud) of the Indonesian Criminal Code may be applied where the constituent elements of the respective offenses are satisfied. For example, a perpetrator may employ a deepfake video that falsely reproduces another person's face or voice to deceive victims into transferring funds or engaging in fraudulent financial transactions. Nevertheless, this study finds that the Criminal Code primarily regulates the criminal consequences arising from the misuse of deepfake technology rather than the technological characteristics of deepfakes themselves. It contains no provisions governing content removal, cooperation with electronic system providers, preservation of digital evidence, or the restoration of victims' digital identities and online reputations.

Accordingly, legal protection for victims of deepfake-related offenses under Indonesia's positive legal system is inherently multilayered. The Personal Data Protection Law provides safeguards for biometric and personal data; the ITE Law regulates the creation, dissemination, authentication, and removal of electronic content; and the Indonesian Criminal Code establishes criminal liability for offenses committed through the misuse of deepfake technology. However, these three legal regimes remain insufficiently integrated, resulting in significant normative deficiencies. These include the absence of a statutory definition of deepfakes, the lack of evidentiary standards for authenticating AI-generated audiovisual content, the absence of victim-centered takedown-and-staydown procedures, the lack of specialized digital forensic standards for deepfake investigations, and the failure to establish clear legal responsibilities for digital platform providers regarding the continued dissemination of synthetic media.

Given these shortcomings, the legal regulation of deepfakes can no longer rely on isolated statutory provisions or a sector-specific regulatory approach. The misuse of deepfake technology presents a multidimensional legal challenge involving personal data protection, electronic communications law, digital evidence, privacy rights, intermediary liability, and criminal law simultaneously. Therefore, the ITE Law, the Personal Data Protection Law, and the Indonesian Criminal Code should be interpreted and applied through an integrated cyber law framework capable of providing legal certainty, strengthening institutional responses to AI-enabled cybercrime, ensuring effective law enforcement, and delivering comprehensive protection and meaningful remedies for victims of deepfake-related harms.

3.2. Effectiveness of Legal Protection for Victims of Deepfake Videos and the Normative and Practical Weaknesses of Indonesia's Positive Legal System

Although Indonesia has several legal instruments that may be applied to combat the misuse of deepfake technology, the effectiveness of legal protection for victims remains limited. The existing legal framework is primarily designed to criminalize unlawful conduct rather than to provide comprehensive protection for victims. Consequently, the principal deficiency lies not only in the absence of legal norms specifically addressing deepfakes but also in the lack of an integrated victim protection framework encompassing prevention, content removal, evidentiary procedures, and post-violation remedies.

The most fundamental weakness is the absence of a statutory definition of deepfake technology within Indonesia's legal system. Neither the Electronic Information and Transactions (ITE) Law, the Personal Data Protection (PDP) Law, nor the Indonesian Criminal Code expressly recognizes concepts such as deepfake videos, synthetic media, digital replicas, or AI-generated voice cloning. As a result, law enforcement authorities must rely on analogical reasoning and broad interpretations of general provisions governing electronic information, personal data, and conventional criminal offenses. This situation makes it difficult to distinguish legitimate applications of artificial intelligence—such as those used in education, scientific research, filmmaking, satire, or artistic expression—from malicious uses that infringe individual rights. Accordingly, this study demonstrates that establishing a legal definition of deepfakes is not merely a matter of terminology; rather, it constitutes a foundational normative requirement for defining the scope of criminal liability, ensuring effective victim protection, and promoting legal certainty.

These findings reinforce the conclusions of Arvitto and Haida and Nuriyatman, who argue that Indonesia has yet to adopt legislation specifically regulating deepfake technology.[16] However, the absence of a statutory definition also has broader legal implications, directly affecting evidentiary requirements, the determination of the constituent elements of criminal offenses, the scope of law enforcement authority, and the legal responsibilities of electronic system providers. In this respect, a legal definition functions as the cornerstone for integrating the broader legal framework governing AI-enabled misconduct.

The effectiveness of legal protection is further undermined by the fragmented relationship among the ITE Law, the PDP Law, and the Indonesian Criminal Code. A single deepfake incident may involve multiple stages of unlawful conduct, including the unauthorized collection of photographs from social media, the processing of biometric

[16] Arvitto, "Implikasi Hukum Deepfake"; Haida and Nuriyatman, "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia."

data, the creation of synthetic audiovisual content, dissemination through digital platforms, reputational attacks, and the acquisition of financial benefits through fraud or extortion. Each of these activities is governed by different statutory regimes, meaning that the legal response depends largely on the provisions selected by investigators and prosecutors. The absence of integrated enforcement guidelines has resulted in inconsistent protection for victims. Factually similar cases may be prosecuted under different statutes, producing divergent legal outcomes and undermining the principles of consistency, equality before the law, and legal certainty.

These findings indicate that a sector-specific regulatory approach is no longer adequate to address AI-enabled cybercrime. Unlike conventional criminal offenses, which generally involve a single protected legal interest, deepfake-related misconduct simultaneously affects personal data protection, digital identity, electronic communications, individual reputation, and the integrity of electronic transactions. Consequently, effective legal protection can be achieved only through the coordinated implementation of the ITE Law, the PDP Law, and the Indonesian Criminal Code within an integrated cyber law framework that places victims at the center of legal protection.

A third significant weakness concerns the absence of specialized digital forensic standards and evidentiary rules for deepfake-related cases. Although Article 5 of the ITE Law recognizes electronic information and electronic documents as legally admissible evidence, Indonesian law does not establish procedures for authenticating AI-generated synthetic media. The investigation and adjudication of deepfake offenses require sophisticated forensic techniques, including metadata analysis, cryptographic hash verification, digital provenance analysis, audiovisual integrity assessment, source attribution, preservation of system logs, and maintenance of an unbroken chain of custody for digital evidence. This study finds that these essential evidentiary requirements remain largely unregulated, leaving their implementation heavily dependent on the technical expertise of investigators and the capabilities of digital forensic laboratories rather than on clear and consistent legal standards.

These findings are consistent with those of Farid, who emphasizes that the detection of deepfakes requires sophisticated digital forensic techniques, and Marsilindo et al., who argue that the evidentiary value of electronic evidence depends upon reliable authentication, data integrity, and an unbroken chain of custody.[17] However, the evidentiary challenges posed by deepfakes extend beyond technological considerations and raise fundamental issues of procedural law. Effective adjudication of deepfake-related offenses requires nationally recognized standards governing AI-assisted forensic examinations and the authentication of AI-generated audiovisual evidence. Moreover,

[17] Farid, "Creating, Using, Misusing, and Detecting Deep Fakes"; Marsilindo Marsilindo et al., "Penggunaan Alat Bukti Digital Dalam Pembuktiian Tindak Pidana Siber Di Pengadilan Indonesia," *Judge: Jurnal Hukum* 6, no. 8 (2026): 1527–38, https://doi.org/10.54209/judge.v6i08.2213.

the handling of deepfake cases presents an inherent tension between the need to remove harmful content promptly to minimize ongoing harm to victims and the obligation to preserve electronic evidence for criminal investigations and judicial proceedings. Indonesia's current legal framework does not adequately reconcile these competing interests.

Another significant weakness is the absence of a victim-centered takedown-and-staydown mechanism. Although Article 40 of the Electronic Information and Transactions (ITE) Law authorizes the government to restrict access to unlawful electronic content, it does not establish specific procedures enabling victims of deepfake abuse to obtain expedited content removal. Nor does it impose mandatory response deadlines on electronic system providers or require digital platforms to prevent the repeated uploading of identical or substantially similar content. Consequently, victims are frequently compelled to submit multiple removal requests because deleted deepfake content is subsequently reposted through different user accounts or across multiple digital platforms.

This finding extends the analysis of Rohmawati et al., who emphasize the importance of regulating deepfakes as part of a broader legal strategy for protecting victims of technology-facilitated gender-based violence.[18] The present study argues that removing unlawful content without a corresponding staydown obligation is insufficient to prevent continuing harm. The injury suffered by victims does not cease upon the conviction of the perpetrator; rather, it persists for as long as the manipulated content remains searchable, downloadable, reproducible, or capable of further dissemination. Accordingly, the effectiveness of legal protection should not be assessed solely by the successful prosecution of offenders but also by the legal system's capacity to prevent the continuing circulation of harmful content and to mitigate its ongoing impact on victims.

A further weakness is that the restoration of victims' rights has not been treated as a central objective of Indonesia's existing legal framework. The ITE Law, the Personal Data Protection (PDP) Law, and the Indonesian Criminal Code continue to emphasize prohibited conduct and criminal sanctions rather than comprehensive mechanisms for victim redress. Yet victims of deepfake-related offenses require substantially broader legal protection, including the right to public correction or clarification, rehabilitation of their reputation, permanent removal of harmful digital content, protection of their digital identity, access to psychological assistance, and compensation for demonstrable material and non-material harm. This study demonstrates that the imposition of criminal sanctions alone neither restores a victim's

[18] Indah Rohmawati et al., "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)," *Innovative: Journal of Social Science Research* 4, no. 6 (2024): 1779–94, https://doi.org/10.31004/innovative.v4i6.16559.

reputation nor eliminates the enduring digital footprint created by widely disseminated deepfake content.

These findings reinforce the conclusions of Lazard et al., who demonstrate that deepfake abuse causes long-term psychological, social, relational, and reputational harm.[19] Similarly, Rohmawati et al. place victims at the center of legal protection in the context of technology-facilitated gender-based violence.[20] Building upon these studies, the present research argues that legal protection for deepfake victims should be understood as a continuous and integrated process that begins with preventing the unlawful collection and processing of personal data, continues through the rapid removal of harmful content and effective law enforcement, and culminates in the restoration of victims' dignity, digital identity, and legal rights.

The effectiveness of legal protection for victims of deepfake-related offenses in Indonesia remains constrained by five principal deficiencies: (1) the absence of a statutory definition of deepfakes; (2) fragmentation across multiple legal regimes; (3) the lack of specialized digital forensic and evidentiary standards for AI-generated content; (4) the absence of victim-centered takedown-and-staydown mechanisms; and (5) the limited emphasis on restoring victims' rights within the existing legal framework. Accordingly, legal reform in Indonesia should extend beyond the introduction of additional criminal provisions. Instead, it should establish an integrated cyber law framework capable of responding to the evolving challenges posed by artificial intelligence while consistently recognizing victims as the primary subjects of legal protection. Such reform requires a fundamental shift from a predominantly punitive legal paradigm toward a comprehensive model that integrates preventive, repressive, and restorative measures to promote legal certainty, strengthen institutional responses, and ensure the effective restoration of victims' rights.

3.3. A Cyber Law–Based Legal Protection Model for Victims of Deepfake Videos

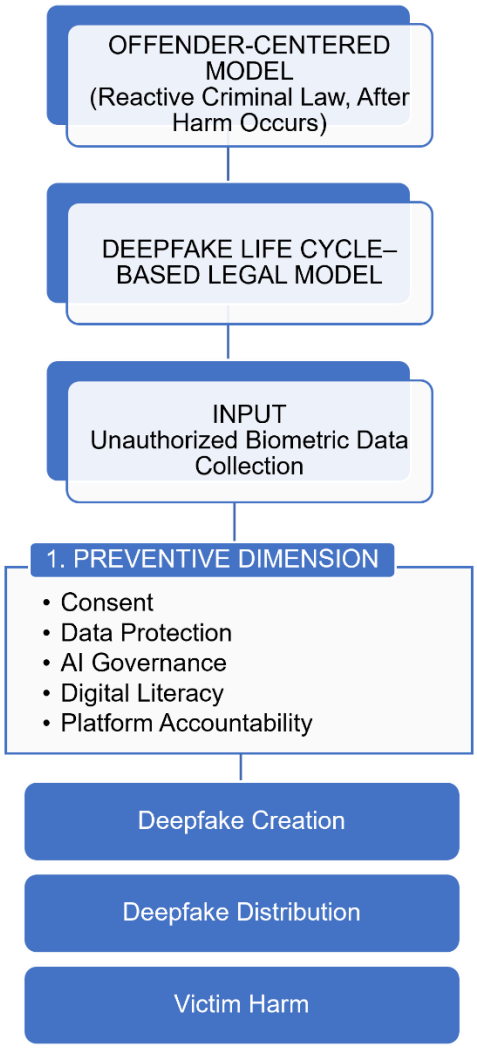
The principal weakness of Indonesia's legal framework lies not only in the absence of legal provisions specifically regulating deepfakes but also in its prevailing protection paradigm, which remains predominantly offender-oriented. Existing legal mechanisms primarily emphasize the punishment of perpetrators rather than the comprehensive protection of victims. However, because deepfakes constitute AI-enabled cyber offenses capable of causing continuous digital harm, an effective legal framework must adopt a victim-centered cyber law approach that places victims at the core of legal protection.

---

[19] Lazard et al., "Deepfake Technology and Gender-Based Violence."

[20] Rohmawati et al., "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)."

An effective legal protection model cannot be structured solely around the stages of criminal proceedings. Instead, it should correspond to the deepfake life cycle, recognizing that legal risks arise long before harmful content is publicly disseminated. This life cycle encompasses the unlawful acquisition of personal data, the processing of biometric information, the generation of synthetic media, the dissemination and use of manipulated content, detection, reporting, content removal, criminal investigation, judicial proceedings, and the restoration of victims' rights. By adopting a deepfake life cycle framework, this study proposes a fundamental shift in legal reasoning. Legal protection should begin not after a deepfake has been widely distributed and caused harm, but at the earliest stage of unauthorized collection or use of an individual's facial image, voice, or biometric data. Within this framework, the law functions as an instrument of digital risk governance, emphasizing prevention and early intervention rather than serving merely as a mechanism for imposing sanctions after harm has occurred.



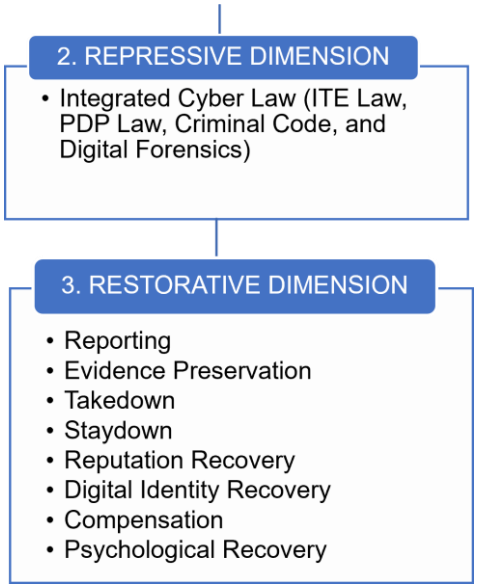


Figure. Deepfake Life Cycle–Based Legal Protection Model for Victim-Centered Cyber Law

The proposed model reflects a paradigm shift from a conventional criminal law approach toward a preventive and adaptive cyber law framework capable of responding to the evolving challenges of artificial intelligence. Unlike the influential analysis of Chesney and Citron, which primarily conceptualizes deepfakes as threats to democracy, national security, and the integrity of public information,[21] the present study positions victims as the primary subjects of legal protection. Accordingly, the focus of legal regulation shifts from safeguarding state interests to protecting individual rights, including the rights to privacy, digital identity, informational autonomy, and human dignity.

Under this model, legal protection must begin before a deepfake is created. Analysis of the Personal Data Protection (PDP) Law demonstrates that facial images, voice recordings, and other biometric characteristics constitute specific personal data that may be processed only on a valid legal basis. Accordingly, this study proposes that the use of photographs, videos, voice recordings, or other biometric information for AI model training or the creation of synthetic media should be subject to three fundamental requirements: explicit and informed consent, purpose limitation, and data minimization. These principles establish the legal foundation for preventing unauthorized exploitation of biometric data by artificial intelligence systems.

The mere availability of an individual's personal data on social media platforms or other publicly accessible sources should not be interpreted as implied consent for its use in generating deepfake content. This finding extends the analysis of Kusnadi and Putri, who characterize privacy as an individual's right to control personal information.[22] The

[21] Robert Chesney and Danielle K. Citron, "Deep Fakes: A Looming Challenge for Priv Es: A Looming Challenge for Privacy, Democr , Democracy, and National Security."

[22] Kusnadi and Putri, "Perlindungan Hak Privasi Dalam Penyalahgunaan Teknologi Deepfake Di Indonesia."

present study advances this perspective by introducing the concept of control over digital self-representation, defined as the right of every individual to determine how their digital identity is collected, reproduced, modified, or manipulated through artificial intelligence technologies. This concept provides a broader normative foundation for protecting personal autonomy in the era of generative AI.

Beyond strengthening personal data protection, a preventive legal framework should incorporate mandatory digital literacy initiatives, enhanced public education concerning artificial intelligence, and more robust governance obligations for electronic system providers. Digital platforms and other electronic system operators should be required to implement internal policies for the early detection of deepfake content, ensure transparency regarding the deployment of AI technologies, and establish effective verification mechanisms for synthetic media that may pose risks to individuals or the public. Consequently, legal protection should not be viewed solely as a function of state authority but rather as an integral component of digital governance, requiring coordinated responsibilities among government institutions, electronic system providers, AI developers, civil society, and individual users.

Effective law enforcement against deepfake-related offenses can be achieved only through the integrated application of the Electronic Information and Transactions (ITE) Law, the Personal Data Protection (PDP) Law, and the Indonesian Criminal Code. In practice, law enforcement authorities have tended to rely on individual statutory regimes in isolation, resulting in only certain aspects of an offender's conduct being addressed. To overcome this limitation, the present study proposes an integrated normative framework under which Article 35 of the ITE Law is applied to the manipulation of electronic information; Articles 27(1) and 27A of the ITE Law are applied to deepfakes involving sexually explicit content or defamation; Articles 65–69 of the PDP Law govern the unlawful processing of personal and biometric data; and the Indonesian Criminal Code is applied to offenses such as defamation, false accusation, fraud, extortion, and other crimes committed through the use of deepfake technology. This integrated approach establishes a multilayered enforcement framework that more accurately reflects the complex and multifaceted nature of AI-enabled misconduct.

These findings extend the work of Haida and Nuriyatman, who emphasize the importance of protecting victims within the framework of Indonesian criminal law.[23] The present study argues that effective victim protection cannot be achieved through criminal law reform alone but instead requires the harmonization of all legal regimes governing digital environments. Within this framework, cyber law should not be understood as an autonomous branch of law but rather as an integrative legal framework

[23] Haida and Nuriyatman, "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia."

that coordinates criminal law, administrative law, personal data protection law, and the law governing electronic evidence into a coherent system of legal protection.

The effectiveness of the proposed repressive framework depends substantially on the establishment of robust standards for electronic evidence and digital forensics. Accordingly, this study proposes the adoption of national standards governing the authentication of deepfakes, metadata examination, audiovisual integrity analysis, cryptographic hash verification, digital provenance analysis, preservation of system logs, and maintenance of an unbroken chain of custody for electronic evidence. These standards are essential to ensure that electronic evidence is not only formally admissible under Article 5 of the ITE Law but also satisfies substantive requirements of authenticity, integrity, reliability, and evidentiary credibility. This proposal is consistent with the findings of Marsilindo et al., who emphasize the importance of authentication, data integrity, and chain-of-custody procedures.[24] However, the present study advances this scholarship by proposing the development of specialized forensic standards for AI-generated synthetic media as an integral component of reforming cybercrime procedural law.

Among the three dimensions of legal protection, the restorative dimension remains the least developed within Indonesia's current legal framework. Existing legislation generally treats victim recovery as an incidental consequence of the offender's conviction. In deepfake-related cases, however, the harm suffered by victims frequently persists long after judicial proceedings have concluded because the manipulated content may continue to be accessed, reproduced, archived, and redistributed indefinitely. Consequently, the legal protection model proposed in this study identifies victim recovery as the primary objective of legal protection, rather than as a secondary consequence of criminal prosecution.

A comprehensive restorative framework should include accessible mechanisms for reporting deepfake-related abuse, preliminary verification based on minimum evidentiary thresholds, temporary restrictions on access to disputed content, preservation of electronic evidence by digital platforms, prompt content removal, takedown-and-staydown obligations, public clarification where appropriate, rehabilitation of the victim's reputation, protection of digital identity, access to psychological support services, and compensation for demonstrable material and non-material harm. In cases involving non-consensual sexually explicit deepfakes, these measures should receive particular priority because the resulting harm extends beyond legal injury to encompass violations of personal dignity, physical and psychological security, mental well-being, and social relationships.

---

[24] Marsilindo et al., "Penggunaan Alat Bukti Digital Dalam Pembuktiian Tindak Pidana Siber Di Pengadilan Indonesia."

These findings reinforce the framework proposed by Meisyah, who conceptualizes legal protection as comprising preventive, repressive, and restorative dimensions.[25] However, the present study advances this framework by developing a Deepfake Life Cycle–Based Legal Protection Model, which integrates each stage of legal protection into a single, continuous, and coordinated system. Within this model, restoration is understood not merely as financial compensation but as the comprehensive process of restoring victims' control over their digital identity, personal autonomy, and digital self-representation.

Digital platforms should bear clearly defined legal responsibilities within the ecosystem of legal protection for victims of deepfake-related offenses. Electronic system providers should be required not only to establish accessible reporting mechanisms but also to implement dedicated procedures for reporting deepfake content, respond to complaints within prescribed timeframes, preserve electronic evidence before removing disputed content, cooperate with law enforcement authorities in accordance with applicable legal procedures, and, where technologically feasible, prevent the re-uploading of identical or substantially similar content through takedown-and-staydown measures. These obligations should be implemented in accordance with the principles of accountability, transparency, due process, and freedom of expression, thereby ensuring effective victim protection while minimizing the risk of disproportionate content moderation and overblocking.

The legal protection model proposed in this study represents a reconstruction of the prevailing cyber law paradigm that differs substantially from existing scholarship. Whereas previous studies have primarily emphasized the introduction of new criminal provisions or the partial protection of privacy rights, the present research develops a Deepfake Life Cycle–Based Legal Protection Model that integrates three complementary dimensions of legal protection. The first dimension consists of preventive measures, including strengthened personal data protection and governance of AI systems. The second comprises repressive measures, achieved through the harmonized application of the Electronic Information and Transactions (ITE) Law, the Personal Data Protection (PDP) Law, and the Indonesian Criminal Code, supported by comprehensive standards governing electronic evidence and digital forensics. The third encompasses restorative measures, including takedown-and-staydown procedures, rehabilitation of victims' reputations, restoration of digital identity, and compensation for demonstrable harm.

Accordingly, legal protection for victims of deepfake-related offenses should no longer be understood merely as a mechanism for imposing criminal liability upon offenders. Rather, it should function as a comprehensive system of digital legal risk

---

[25] Meisyah, "Perlindungan Hukum Pidana Bagi Pemilik Wajah Yang Digunakan Online Sebagai Hasil Kecerdasan Buatan (Artificial Intelligence)."

governance that seeks to prevent the unlawful use of personal data, strengthen the effectiveness of law enforcement, safeguard digital identity, halt the continued dissemination of harmful synthetic content, and restore the dignity, autonomy, and legal rights of victims. The model proposed in this study therefore offers a more adaptive framework for legal reform in response to the rapid evolution of artificial intelligence technologies. It also provides a normative foundation for the development of comprehensive legislation specifically regulating deepfakes in Indonesia, with the overarching objectives of promoting legal certainty, justice, and the protection of human rights.

4. CONCLUSION

The Electronic Information and Transactions (ITE) Law, the Personal Data Protection (PDP) Law, and the Indonesian Criminal Code provide a normative foundation for addressing the misuse of deepfake technology. Nevertheless, the existing legal framework remains fragmented, lacking a statutory definition of deepfakes, standardized procedures for the authentication and forensic examination of AI-generated content, a comprehensive framework governing the responsibilities of digital platform providers, and effective mechanisms for victim recovery. In response to these shortcomings, this study proposes a Deepfake Life Cycle–Based Legal Protection Model that integrates preventive, repressive, and restorative measures throughout the entire continuum of deepfake-related harm—from the unlawful collection and processing of personal data, through coordinated law enforcement, to the restoration of victims' digital identity, dignity, and reputation.

The proposed model contributes to the advancement of cyber law scholarship by providing a coherent conceptual framework for the development of comprehensive legislation governing deepfake technology in Indonesia. Nevertheless, this study is subject to certain limitations. As a normative legal study, it does not empirically evaluate the practical implementation or effectiveness of the proposed model, nor does it undertake a comprehensive comparative analysis across jurisdictions. Accordingly, the Indonesian government should prioritize the development of dedicated legislation regulating deepfakes, establish national standards for digital forensic examination and AI-generated evidence, adopt integrated law enforcement guidelines, and implement a victim-centered takedown-and-staydown framework. Future research should focus on empirically assessing the effectiveness of the proposed model in judicial practice, digital platform governance, and cross-border legal cooperation in addressing AI-enabled deepfake-related offenses.

REFERENCES

Journals

Alrashoud, Mubarak. "Deepfake Video Detection Methods, Approaches, and Challenges." *Alexandria Engineering Journal* 125 (2025): 265–77. https://doi.org/10.1016/j.aej.2025.04.007.

Arvitto, Rafi Satrya. "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP." *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 4, no. 2 (2025): 73–82. https://doi.org/10.35912/jihham.v4i2.3937.

Diel, Alexander, Tania Lalgi, Isabel Carolin Schröter, Karl F. MacDorman, Martin Teufel, and Alexander Bäuerle. "Human Performance in Detecting Deepfakes: A Systematic Review and Meta-Analysis of 56 Papers." *Computers in Human Behavior Reports* 16 (December 2024): 100538. https://doi.org/10.1016/j.chbr.2024.100538.

Farid, Hany. "Creating, Using, Misusing, and Detecting Deep Fakes." *Journal of Online Trust and Safety* 1, no. 4 (2022): 1–33. https://doi.org/10.54501/jots.v1i4.56.

Haida, Rendi Syaputra Nur, and Eko Nuriyatman. "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia." *Jurnal Hukum Respublica* 24, no. 1 (2024): 1–13. https://doi.org/10.31849/respublica.v24i01.23327.

https://journal.unj.ac.id/unj/index.php/senpishum/article/view/62862.

Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or Treat?" *Business Horizons* 63, no. 2 (2020): 135–46. https://doi.org/10.1016/j.bushor.2019.11.006.

Kusnadi, Sekaring Ayumeida, and Dina Wanda Setiawan Putri. "Perlindungan Hak Privasi Dalam Penyalahgunaan Teknologi Deepfake Di Indonesia." *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 195–210. https://doi.org/10.33331/rechtsvinding.v14i2.2135.

Lazard, Lisa, Rose Capdevila, Emma L. Turley, Kathryn Gilfoyle, and Nelli Stavropoulou. "Deepfake Technology and Gender-Based Violence: A Scoping Review." *Trauma, Violence, & Abuse*, 2025, 15248380251384271. https://doi.org/10.1177/15248380251384271.

Marsilindo, Marsilindo, Rizky Pratama Putra Karo-Karo, and Bambang Widarto. "Penggunaan Alat Bukti Digital Dalam Pembuktiian Tindak Pidana Siber Di Pengadilan Indonesia." *Judge: Jurnal Hukum* 6, no. 8 (2026): 1527–38. https://doi.org/10.54209/judge.v6i08.2213.

Meisyah, Meisyah. "Perlindungan Hukum Pidana Bagi Pemilik Wajah Yang Digunakan Online Sebagai Hasil Kecerdasan Buatan (Artificial Intelligence)." *Edu Yustisia: Jurnal Edukasi Hukum* 4, no. 2 (2025): 19–24.

Mirsky, Yisroel, and Wenke Lee. "The Creation and Detection of Deepfakes: A Survey." *ACM Computing Surveys* 54, no. 1 (2022): 1–41. https://doi.org/10.1145/3425780.

Noerman, Chiquita Thefirstly, and Aji Lukman Ibrahim. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara." *Jurnal Usm Law Review* 7, no. 2 (2024): 603–21. https://doi.org/10.26623/julr.v7i2.8995.

Palindria, Arvi Erawan, Muhammad Sulthan Thufail, and Muhammad Rieval Febrian. "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data

Biometrik Di Indonesia." *Spektrum Hukum* 21, no. 2 (2024): 110. https://doi.org/10.56444/sh.v21i2.5319.

Robert Chesney and Danielle K. Citron. "Deep Fakes: A Looming Challenge for Priv Es: A Looming Challenge for Privacy, Democr , Democracy, and National Security." *California Law Review* 107 (2019): 1753–820.

Rohmawati, Indah, Amir Junaidi, and Ariy Khaerudin. "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)." *Innovative: Journal of Social Science Research* 4, no. 6 (2024): 1779–94. https://doi.org/10.31004/innovative.v4i6.16559.

Prosidings

Karo, Rizky Karo, Zein Jiddan, and Hanan Atanto Buono. "Analisis Dalam Kasus Penyalahgunaan Deepfake Dari Segi Perlindungan Data Pribadi Dalam UU ITE Dan UU PDP Di Indonesia." *Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial, Dan Hukum* 1, no. 1 (2026): 1–8.