Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 3 Number 6, 2025
DOI: https://doi.org/10.61104/alz.v3i5.2714

Regulatory Gaps and Legal Enforcement Challenges on Deepfake Pornography as a Form of Digital Sexual Violence in Indonesia

Theodora Kristina Boleng[1], Adi Nur Rohman[2]
Faculty of Law, Bhayangkara Jakarta Raya University, Indonesia[1-2]
Email Korespondensi: theodoraboleng11@gmail.com

Article received: 15 September 2025, Review process: 25 September 2025
Article Accepted: 10 Oktober 2025, Article published: 09 Desember 2025

ABSTRACT
The emergence of deepfake pornography, a development closely linked to artificial intelligence, has transformed the landscape of digital sexual assault. Perpetrators may employ machine learning algorithms to falsely portray a victim as being pornographically engaged without their consent or awareness. This research aims to examine the effective legislative frameworks addressing deepfake pornography in Indonesia, considering digital evidence and cross-border jurisdictions, and to evaluate the challenges encountered by law enforcement. This study utilises a normative juridical framework alongside qualitative analytical methods to analyse case studies, including incidents at Udayana and Semarang Universities in 2025, as well as pertinent legal sources such as the ITE Law, TPKS Law, and PDP Law. The study's findings indicate that the lack of standards and inadequacies in rule coordination persist as issues within Indonesia's legal system. TPKS and PDP have yet to tackle digital manipulation through artificial intelligence, whereas ITE has concentrated on the dissemination of ethical content. Moreover, law enforcement's efficacy is hindered by the absence of a national AI laboratory, limitations on digital forensic capabilities, and challenges in international coordination. Legal reform is essential to tackle these concerns; it must include new regulations concerning synthetic media offences, enhance digital forensics capabilities, and adopt victim-centered justice concepts to protect and restore victims' rights in the digital domain.
Keywords: *Artificial Intelligence, Deepfake Pornography, Digital Sexual Violence, Digital Proof, Legal Reconstruction.*

ABSTRAK
Fenomena deepfake pornography merupakan bentuk baru dari kekerasan seksual digital yang muncul seiring dengan perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI). Dengan memanfaatkan algoritma pembelajaran mesin, pelaku mampu memanipulasi wajah dan suara seseorang sehingga tampak seolah-olah terlibat dalam aktivitas pornografi tanpa persetujuan. Penelitian ini bertujuan untuk mengkaji pengaturan hukum positif Indonesia terhadap deepfake pornography dan menganalisis tantangan penegakan hukumnya dari aspek pembuktian digital serta yurisdiksi lintas negara. Penelitian menggunakan pendekatan yuridis normatif dengan metode analisis kualitatif terhadap bahan hukum primer (UU ITE, UU TPKS, dan UU PDP), serta studi kasus aktual seperti peristiwa Universitas Udayana dan Semarang tahun 2025. Hasil penelitian menunjukkan bahwa sistem hukum Indonesia masih menghadapi kekosongan norma dan kelemahan koordinasi antaraturan. UU ITE berfokus pada penyebaran konten kesusilaan, sementara UU TPKS dan UU PDP belum menjangkau manipulasi digital berbasis AI. Selain itu, keterbatasan

kemampuan forensik digital, belum adanya laboratorium AI nasional, serta kendala kerja sama internasional menghambat efektivitas penegakan hukum. Untuk menjawab tantangan tersebut, diperlukan rekonstruksi hukum yang mencakup pengaturan khusus mengenai kejahatan synthetic media, peningkatan kapasitas forensik digital, serta penerapan prinsip victim-centered justice guna memastikan perlindungan dan pemulihan hak korban secara menyeluruh di ruang digital.
Kata kunci: *kecerdasan buatan, deepfake pornography, kekerasan seksual digital, pembuktian digital, rekonstruksi hukum.*

INTRODUCTION

Contemporary technical advancements in the Fourth Industrial Revolution have significantly transformed our daily activities, encompassing work, leisure, and internet communication. A crucial element of this transformation is artificial intelligence (AI), which can emulate human cognitive processes and generate automated outcomes through complex computing methods (Fonna, 2019). This transition exemplifies the "technological disruption era," marked by swift, significant, and systematic changes that replace the former paradigm with one solely reliant on digital data. From this junction sprang a multitude of oddities and cybercrimes, including cybersexual assault (Ramadhan & Muttaqin, 2023).

The application of machine learning algorithms to authentically modify an individual's speech, facial expressions, and body language has resulted in one of the most intriguing and alarming innovations: deepfake technology (Nopiansyah, 2025). Deepfake pornography refers to the application of machine learning algorithms to generate synthetic pornographic content utilising an individual's likeness and voice without their consent or awareness, representing a particularly alarming form of digital sexual exploitation (Darmawan et al., 2025). Historically, when the prevalence of sextortion and revenge porn online, the dissemination of fresh content was crucial. In the era of artificial intelligence, a mere photograph of the victim's face sufficed to create a plausible film (F. A. Wibowo & Permana, 2025). This technology significantly increases the threat to privacy by facilitating sexual exploitation without the need for personal data access.

Deepfake pornography has garnered significant attention in Indonesia since 2023 and is anticipated to increase in prevalence until 2025. The predominant technique is covertly capturing an individual's visage superimposed onto another's physique in a sexually graphic video (CNN Indonesia, 2025). The victim endures mental, social, and ethical damage due to this novel form of non-physical sexual assault, which concurrently infringes upon their right to privacy. The anonymity of cross-border internet platforms utilised for disseminating such information complicates law enforcement intervention. Deepfake pornography illustrates how technically neutral tools may be exploitative and demeaning to human dignity.

An instance of this risk is the event that transpired in 2025 at Udayana University. The victims experienced psychological hardship, peer pressure, and shame due to the digital alteration of their appearance and their superimposition into pornographic films (KumparanNews, 2025). This instance demonstrates that the misuse of AI has become a significant humanitarian and legal issue that necessitates

a robust governmental response, rather than merely a technological one. The May 2025 issue of Tempo reported a notable rise of sexually explicit deepfake films circulating on social media in Southeast Asia, particularly in Indonesia. Inadequate digital surveillance and insufficient legal safeguards resulted in the predominance of young women among the victims, many of whom were unaware that their identities had been exploited without their consent.

Global statistics indicate that women constitute the predominant demographic of sexual assault victims in online environments, accounting for 71% (Sugiyanto, 2021). This case underscores the necessity for legal analysis grounded in feminist legal theory that considers gender inequality. Victims of sexual assault endure dual challenges of social stigma and gender-insensitive legal processes, as posited by Sarah Gamble, due to patriarchal societal and legal frameworks that frequently subordinate women (Nasution et al., 2025).

Currently, there is no statute or legal structure that categorises deepfake pornography as a specific criminal offence inside the nation's legal system. Digital manipulation, central to the deepfake dilemma, is unregulated by Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), which just outlaws the dissemination of immoral content in Article 27, paragraph (1). Although Law Number 12 of 2022 about the Crime of Sexual Violence (TPKS Law) recognises sexual violence committed using electronic means, it does not address offences executed utilising synthetic media. The application of biometrics, such as facial or vocal recognition, in synthetic content currently falls outside the scope of Law Number 27 of 2022 about Personal Data Protection (PDP Law), which mainly focusses on the misuse of personal data in administrative contexts. When a crime is perpetrated across borders utilising untraceable technology, authorities face considerable difficulties in establishing the perpetrator's actus reus (unlawful behaviour) and mens rea (malicious intent) due to this normative gap.

To yet, initiatives to address deepfake pornography have been reactive and fragmented. The act serves as a preventative measure that anticipates potential technical problems, but it only becomes applicable when a case provokes public outcry (Cahyono et al., 2025). The legal system's emphasis on conventional offences complicates law enforcement's ability to apprehend hackers utilising fraudulent identities to perpetrate their activities. Law enforcement's preoccupation with facts frequently eclipses victims' rights to safety and rehabilitation (Butarbutar, 2025). Victims of sexual assault, particularly those subjected to online incidents, shall get compassionate care and psychological rehabilitation as stipulated in the restorative justice framework of the TPKS Law.

The Right to be Forgotten (RtBF), as an element of digital privacy rights, has been enacted in numerous nations globally. The General Data Protection Regulation (GDPR) 2016/679 of the European Union was the inaugural legislation to formalise this concept; it confers upon individuals the right to have their personal data expunged from digital repositories (Zaltina & Nurtjahyo, 2024). Although Indonesia lacks rules analogous to the Right to Be Forgotten (RtBF), victims of sexual assault conducted through electronic means has the right to have any sexually explicit material removed from their cases in accordance with Article 70 paragraph (2) letter

l of the TPKS Law. Nonetheless, substantial barriers exist regarding its implementation in relation to public comprehension and the legal environment.

The significant societal impact of this problem is evidenced by several occurrences highlighted in the media. A woman from Semarang was depicted in a synthetic pornographic film, as reported by a Kompas story dated October 24, 2025. His social status deteriorated, and he suffered psychological distress (Media, 2025). Kumparan (2025) elucidates a similar phenomenon at Udayana University, when numerous student images were manipulated with AI software to produce pornographic films (KumparanNews, 2025). Simultaneously, as indicated by Tempo's study, there is an insufficiency of legislative measures to mitigate the ongoing proliferation of such information (Tempo, 2025). The legal protections are insufficient, and the government is ill-equipped to address new forms of cybersexual assault, as demonstrated by these three cases.

Given these circumstances, the necessity for prompt legislative reform is evident. The objectives of this research are to (1) identify conceptual and normative deficiencies in existing legislation and (2) provide a framework for legal reform that may meet the challenges posed by deepfake pornography in Indonesia. Enhancing law enforcement's digital forensic capabilities, establishing a framework for international collaboration in prosecuting criminals, and including synthetic media offences into the ITE Law or the TPKS Law are essential measures for advancing a more equitable legal system. Furthermore, sufferers ought to possess the entitlement to psychological rehabilitation, digital data deletion, and restoration of reputation as assured by national legislation. The Indonesian legal system aims to uphold human dignity in the face of the unbounded advancement of artificial intelligence technology through a flexible methodology and substantive justice.

Formulation Problem : (1) How does the law in Indonesia address the issue of deepfake pornography, which is a kind of online sexual abuse, and what are the gaps in the current legislation that make it difficult to catch those responsible? (2) In Indonesia, how are digital proof and cross-border jurisdiction posing problems to law enforcement in their fight against deepfake pornography? How can victims be protected by legal reconstruction efforts?

METHODS

This research employs a normative juridical method to examine the norms, regulations, and legal concepts governing online sexual assault, specifically focussing on deepfake pornography. Our objective in employing this method is to ascertain the efficacy of Indonesia's positive legal standards in addressing the emerging legal challenges posed by AI. This study adopts a normative perspective, asserting that the law constitutes a framework of criteria that must be assessed to guarantee the safety of online communities.

Primary, secondary, and tertiary sources of legal knowledge are utilised to aggregate the study data. Primary legal materials include relevant statutes and regulations, such as Law Number 12 of 2022 on the Crime of Sexual Violence, Law Number 27 of 2022 on Personal Data Protection, Law Number 11 of 2008 on Information and Electronic Transactions and its amendments, along with various

judicial rulings and associated implementing regulations. Institutional reports, scientific literature, academic research findings, journal articles, and secondary legal sources pertaining to cybercrime and the misuse of artificial intelligence are utilised. Tertiary legal resources, including legal dictionaries, encyclopaedias, and official online sources, facilitate the understanding of terms and provide research context.

The meticulous collection of data involves reading, investigating, and assessing various legal sources (Marzuki, 2017). To do qualitative-descriptive data analysis, one must first comprehend the significance of norms, subsequently compare them to actual field practices, and finally employ deductive reasoning to draw conclusions. This technique may reveal the connection between the absence of norms, inadequate law enforcement, and the necessity to reform rules to better align with technological improvements (Qamar et al., 2017). This study is anticipated to establish a foundational legal framework that more effectively addresses victims' demands, promotes equity, and enhances victim protection in the contemporary digital era.

RESULTS AND DISCUSSION

Legal Regulation of Deepfake Pornography in the Indonesian Legal System and Its Weaknesses

The advancement of AI has introduced further challenges to the modern criminal justice system. Deepfake pornography, the utilisation of artificial intelligence to replicate sexual interactions without the subject's consent or awareness, constitutes a profoundly troubling kind of abuse. Despite its noble goals, this technology is frequently employed for unethical purposes that undermine human dignity, regardless of its beginnings in the creative sectors, such as cinema or visual education.

Victims of deepfake pornography encounter a wide range of repercussions. Alongside being a victim of cybersexual assault, she endures societal stigma, emotional distress, and financial difficulties due to the persistent threat of extortion. Online Gender-Based Violence (GBV) is characterised by the Association for Progressive Communications (APC) as violent acts inflicted upon persons due to their gender or sexual orientation, facilitated by digital technology. Victims frequently experience feelings of societal abandonment, scepticism towards online institutions, and a lack of faith in emerging technologies (Kasita, 2022).

In Indonesia, deepfake pornography and artificial intelligence remain unregulated under the law. Notwithstanding their bias and sector-specific emphasis, several existing laws may provide a basis for the apprehension of criminals (Ardiyani, 2024).

The principal legislative foundation for addressing cybercrime is Law No. 11 of 2008, which pertains to information and electronic transactions. The dissemination or availability of ethically disputed electronic content is subject to a penalty of up to six years of imprisonment and a fine of one billion rupiah, as stipulated in Article 45, paragraph (1) of the criminal code. This regulation fails to address the digital manipulation process that underlies deepfake pornography; it solely pertains to the distribution of content.

In terms of nomenclature, artificial intelligence (AI) parallels the concept of a "electronic agent" as delineated in Article 1, number 8 of the ITE Law: a constituent of an electronic system that autonomously processes data. Despite conducting its own operations, the individuals in authority remain legally accountable for all occurrences. Consequently, the ITE Law's principle of personal accountability permits the prosecution of those who employ AI to create or distribute synthetic pornographic content (Putra & Haq, 2024).

Moreover, as articulated in Article 15, paragraphs (1) and (2) of the ITE Law, developers of deepfake platforms or applications are required to uphold the reliability and security of the system as Electronic System Operators (PSE). However, due to the lack of AI-specific rules, service providers occasionally impose certain responsibilities on users through privacy agreements, thereby rendering system providers legally unaccountable.

Any medium that facilitates sexual exploitation or contravenes moral standards is classified as pornographic by law. The creation, duplication, distribution, or provision of pornographic content is expressly forbidden in Article 4, paragraph (1), with offenders subject to a criminal punishment ranging from six months to twelve years and/or a fine between IDR 250 million and IDR 6 billion, as specified in Article 29.

While the phrase "deepfake pornography" remains unutilised, its legal implications can be applied to AI-manipulated content that exhibits characteristics of decency. Both charges entail sexual exploitation that undermines the victim's dignity, resulting in comparable criminal consequences to traditional pornography (Novera, 2024).

The definition of sexual assault has been expanded to encompass KSBE by Law No. 12 of 2022. Creating and distributing sexually explicit material without the victim's consent is unlawful (Article 14). Nevertheless, synthetic content generated by AI lacks definitive control. Although the non-physical sexual assault elements in deepfake pornography are evident, prosecuting offenders directly under the TPKS Law poses significant challenges.

According to Article 70, paragraph (2), letter l of the TPKS Law, victims possess the right to have explicit material removed from the digital realm. This principle is referred to as the Right to be Forgotten (RtBF). Although this notion is crucial for safeguarding victims' identities and restoring their reputations, its implementation is obstructed by inter-agency collaboration and jurisdictional constraints.

The unlawful act of utilising another individual's personal information for personal benefit or harm is prohibited under Law No. 27 of 2022 (Articles 66 and 68), with a maximum penalty of six billion rupiah and/or six years of imprisonment. Deepfake pornography's alteration of voice and facial images involves the unauthorised exploitation of an individual's visual identity, thereby fabricating personal data. The PDP Law is inadequate in addressing internet sexual offences due to its predominantly administrative emphasis.

The new Criminal Code imposes a criminal punishment of six months to ten years for the production and distribution of pornographic material. This regulation

will be implemented in 2026 pursuant to Article 407. Although it does not directly touch AI, this norm may provide a basis for the legal protection of synthetic content creators producing explicit material.

The notion of responsibility in criminal law hinges on the premise that individuals possess awareness of and are driven to violate the law. Van Hamel asserts that accountability for criminal actions rests only with individuals who possess self-awareness and the capacity to regulate their own conduct (Oratmangun, 2016). Therefore, the individual who directs or employs AI for unlawful purposes remains legally accountable, even when AI operates autonomously.

The existing legal framework is inadequate to prevent deepfake pornography because to significant deficiencies in its conceptual and normative foundations. Due to its components being difficult to obtain from traditional sources, deepfake pornography presents a unique challenge for criminal law.

1. Firstly, demonstrating the element of actus reus (illegal actions) is challenging, as cybercriminals sometimes employ automated systems, operate through cross-border servers, or maintain anonymity.
2. Secondly, it is not always straightforward to ascertain if an individual possesses mens rea, or malicious intent, in interactions with AI. This is due to the existence of mechanisms that might render users oblivious to the utilisation of AI, exemplified as auto-generator applications or deepfake technologies.
3. Thirdly, the Indonesian legal system has not yet designated deepfake pornography as a separate criminal offence. Individuals often perceive this as an infringement of privacy or ethical standards rather than a digital sexual offence that undermines the victim's dignity.
4. Fourth, a criminal model predicated on an algorithmic system that operates autonomously and anonymously has not been addressed by the legal framework, which remains focused on direct human agents.

Nevertheless, the pertinent regulatory framework exhibits multiple normative deficiencies:

1. Initially, the responsibilities of content hosts and digital platform providers are not delineated in any legislation. Platforms that function beyond jurisdictional boundaries predominantly facilitate the circulation of deepfake pornography.
2. Secondly, the core of the deepfake phenomenon—the digital development and engineering phase—remains unaddressed by the penalties under the ITE Law, which focus on the dissemination of moral content.
3. Thirdly, although biometric data (including facial, vocal, and physical attributes) is classified as sensitive personal information safeguarded by legislation, the PDP Law does not explicitly address violations of this data in relation to deepfake creation.
4. Fourth, law enforcement officers are hindered in effectively apprehending offenders due to jurisdictional overlap and a deficiency in legal coherence.

These deficiencies have incapacitated Indonesia's law enforcement agencies in their battle against deepfake pornography. The complexity of crime classification

results in several instances remaining unresolved during the investigative phase, leaving victims frequently without adequate reparation. The existing legal framework in Indonesia evidently prioritises reactive measures over proactive adaptation to the transformative impact of digital technology.

Consequently, amending the legislation is of paramount importance. Platform providers must be mandated to eliminate content that depicts digital sexual assault, and rules should delineate the elements of sensitivity, affirm the criminal accountability of perpetrators, and specifically regulate crimes involving synthetic media. The legal system must prioritise victim-centered justice to fulfil its dual objectives of punishing perpetrators and restoring victims' dignity while safeguarding their online privacy.

Law Enforcement Challenges against Deepfake Pornography in Indonesia and the Direction of Legal Reconstruction for Victim Protection

a. Aspects of Digital Evidence in Law Enforcement

Law enforcement against deepfake pornography encounters significant challenges regarding evidence. Law enforcement organisations face considerable hurdles in prosecuting cases involving deepfake pornography due to the intricacy and manipulability of the digital evidence generated. Deepfakes differ from conventional digital content since they are produced by AI-generated synthetic media, encompassing visual and aural manipulation. Consequently, their detection and authentication require advanced technical analysis. The synthesised video file constitutes the principal evidence in this case. To demonstrate that the content is an algorithmic modification rather than the original recording, we must employ hashing techniques, metadata analysis, and AI traceability.

In practical application, Indonesia's digital forensic capabilities are significantly deficient. The technical procedures of contemporary digital evidence are beyond the understanding of numerous law enforcement officials, especially those engaged in investigations. Consequently, several reports were suspended during their investigative phases due to the failure to identify the origin of material production. Officials frequently rely on overseas testing methodologies that are not universally recognised for their validity in the legal evidence process, as there is no national AI forensic laboratory capable of detecting AI fingerprints. This exacerbates the situation (A. Wibowo et al., 2023).

Moreover, the crux of the deepfake pornography dilemma is in Indonesia's evidential framework, which prioritises actus reus, namely the dissemination of material, over actus creationis, pertaining to the phase of synthetic content generation. Digital tampering inherently meets the standards for privacy violations and obscenity. This distribution-centric evidence framework enables the primary perpetrators, namely those who produce deepfakes, to avoid criminal punishment.

b. Jurisdictional Challenges and Cross-Border Cooperation

The jurisdictional aspect constitutes the subsequent challenge. Nearly all servers and platforms hosting deepfake pornography are situated outside of Indonesia. To evade domestic legal consequences, numerous offenders utilise

offshore platforms or virtual private networks (VPNs). This complicates the Indonesian police's ability to monitor and enforce effectively (Naili, 2025).

International cooperation is essential in circumstances such as these. Data access across nations, monitoring of offshore servers, and extradition requests should be predominantly managed through the Mutual Legal Assistance (MLA) system. Regrettably, the coordination process is occasionally ineffective and protracted, as Indonesia lacks comprehensive bilateral agreements with other countries that provide digital platforms. Crimes involving artificial intelligence transcend national borders, leading to deficiencies in the enforcement of cyber laws due to the limitations of international legal frameworks.

c. Psychological Obstacles of Victims and Reporting Barriers

Evaluating the victim's psychological condition is an essential factor. Fear, shame, and apprehensions regarding recovery deter numerous victims of deepfake pornography from disclosing their experiences. Despite the evident digital alteration of this film, in a patriarchal society, the female victims are frequently held accountable and perceived as having "contributed" to its production.

The existing legal system has a bias favouring technical evidence over the healing of victims. The TPKS Law is founded on the principle of victim-centered justice, which is contradicted by this. Victims possess the right to psychological safeguarding, rehabilitation, and the removal of materials that undermine their dignity, alongside the right to formal justice. Regrettably, the absence of collaboration among victim support organisations, internet service providers, and law enforcement agencies results in this precaution not operating at optimal efficiency (Ruslinia et al., 2023).

d. Challenges of Proof and Limited Forensic Capacity

In many cases, the technological elements of the evidence process concerning deepfake pornography exceed the proficiency of Indonesian law enforcement. Verifying the authenticity of videos is arduous without AI forensic tools, given deepfake technology's capacity to produce nearly indistinguishable images and sounds.

The issue of the legal validity of the evidence emerges from the dependence on foreign institutions in the absence of a national laboratory specialising in AI-based forensics. A further concern is the inconsistency in the proving process across instances, as there are no technological standards governing the management of digital evidence in synthetic media contexts. This results in the dismissal of several cases when digital evidence is considered inadmissible in court.

The legal system prioritises distribution purpose over manufacturing intent. Deepfake pornography encompasses behaviours that infringe upon both privacy and ethical principles. The law frequently overlooks significant contributors, such as creators of synthetic information, due to the distribution-centric structure of evidence (Maimun & Thomas, 2025).

The Indonesian cyber law enforcement framework requires a comprehensive legal overhaul to address these challenges. The restoration is founded on three pillars: legal culture, substance, and structure.

When amending the ITE legislation or formulating new legislation on AI, it is crucial to establish a definitive norm that regulates synthetic media offences from a legal perspective. The guideline should explicitly mandate that the creation or distribution of deepfake pornography is prohibited for digital platform providers. From a structural perspective, law enforcement and judicial systems must augment their digital forensics competencies. The government should establish a national AI forensic laboratory to legally analyse metadata, hash values, and AI fingerprinting. To overcome jurisdiction-specific difficulties, it is essential to enhance international collaboration through mutual legal assistance and bilateral agreements.

The judicial system must transform its culture to prioritise victims. The TPKS Law mandates the uniform implementation of victim-centered justice, encompassing victims' entitlement to the right to be forgotten and an expedited removal order process. Adopting this approach will ensure that perpetrators of deepfake pornography encounter legal repercussions, while simultaneously providing victims with assistance in restoring their mental health, social connections, and reputations.

CONCLUSION

Deepfake pornography, characterised by the unlawful alteration of an individual's image into sexually explicit content, represents a novel kind of digital sexual assault that has arisen alongside advancements in AI technology. Currently, there is no legal instrument inside Indonesian law that regulates this scenario. The ITE Law, TPKS Law, and PDP Law each independently address offences related to synthetic media. This results in inadequate protection for victims and a legal loophole that complicates the pursuit of justice against the perpetrators. The inadequacy of national legislation in addressing anonymous, global cybercrimes is evidenced by the 2025 occurrences at Udayana University and Semarang City. Conversely, there are intricate technological challenges that law enforcement procedures must surmount. Precise forensic methods are essential for verifying digitally manipulated videos to ascertain their authenticity and legitimacy. Regrettably, numerous law enforcement organisations and investigators are deficient in the expertise and resources required to identify evidence dependent on artificial intelligence. Furthermore, actors utilising overseas servers have significant difficulties due to the absence of an international coordinating structure. In the absence of legal clarity or victim-centered therapeutic approaches, victims frequently endure psychological, social, and reputational challenges linked to these circumstances.

This underscores the necessity of implementing progressive and flexible strategies in the reconstruction of the law. To remain current, the state's criminal code must incorporate new sections targeting synthetic media and deepfake offences, enhance the capabilities of digital forensic institutions, and fortify international collaboration among cyber law enforcement organisations. Furthermore, criminal law should shift its emphasis from repression to the protection of victims and the restoration of their dignity. A comprehensive revision of Indonesian legislation is

essential to uphold the integrity and fairness of the digital domain, enabling them to tackle ethical and technical issues.

LIST OF REFERENCES

Ardiyani, N. K. D. I. (2024). Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif. *Jurnal Kajian Hukum Dan Kebijakan Publik | E-ISSN : 3031-8882*, *2*(1), 603–608. https://doi.org/10.62379/cs863250

Butarbutar, J. M. (2025). Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi. *Media Hukum Indonesia (MHI)*, *3*(2). https://doi.org/10.5281/zenodo.15493512

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 1–23. https://doi.org/10.64344/djl.v1i1.6

CNN Indonesia. (2025). *Marak Kejahatan Deepfake, Komdigi Andalkan UU ITE dan Pornografi*. teknologi. https://www.cnnindonesia.com/teknologi/20250509163207-185-1227813/marak-kejahatan-deepfake-komdigi-andalkan-uu-ite-dan-pornografi

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence di Indonesia. *JURNAL PENELITIAN SERAMBI HUKUM*, *18*(01), 42–54. https://doi.org/10.59582/sh.v18i01.1257

Fonna, N. (2019). *Pengembangan Revolusi Industri 4.0 dalam Berbagai Bidang*. GUEPEDIA.

Kasita, I. D. (2022). Deepfake pornografi: Tren kekerasan gender berbasis online (KGBO) di era pandemi COVID-19. *Jurnal Wanita Dan Keluarga*, *3*(1), 16–26. https://doi.org/10.22146/jwk.5202

KumparanNews. (2025). *Terungkapnya Kasus Konten Porno Deepfake Mahasiswi Unud*. kumparan. https://kumparan.com/kumparannews/terungkapnya-kasus-konten-porno-deepfake-mahasiswi-unud-24xOaAR2Ntv

Maimun, A., & Thomas, D. Y. (2025). Penggunaan Ai Dalam Proses Pemeriksaan Tersangka Dalam Penyidikan Di Kepolisian. *National Multidisciplinary Sciences*, *4*(3), 33–40. https://doi.org/10.32528/nms.v4i3.744

Marzuki, P. D. M. (2017). *Penelitian Hukum: Edisi Revisi*. Prenada Media.

Media, K. C. (2025, October 24). *Kisah Korban Konten Video Deepfake AI Porno di Semarang Alami Syok Berat: Langsung Nangis dan Gemetaran*. KOMPAS.com. https://www.kompas.com/jawa-tengah/read/2025/10/24/153520688/kisah-korban-konten-video-deepfake-ai-porno-di-semarang-alami-syok

Naili, Y. T. (2025). Optimalisasi Penegakan Hukum terhadap Kejahatan Siber Berbasis AI terhadap Perempuan: Kajian Hukum Pidana dan Kebijakan

Digital: Optimizing Law Enforcement against AI-Based Cybercrimes against Women: A Study of Criminal Law and Digital Policy. *Jurnal Media Hukum*, *13*(2), 207–219. https://doi.org/10.59414/jmh.v13i2.1030

Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2025). Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, *38*(7), 2489–2517. https://doi.org/10.1007/s11196-025-10265-0

Nopiansyah, R. (2025). *HUKUM DAN KECERDASAN BUATAN: Menyongsong era baru dunia hukum*. Penerbit Kbm Indonesia.

Novera, O. (2024). Analisis pengaturan hukum pidana terhadap penyalahgunaan teknologi manipulasi gambar (deepfake) dalam penyebaran konten pornografi melalui akun media sosial. *El-Faqih: Jurnal Pemikiran Dan Hukum Islam*, *10*(2), 460–474. https://doi.org/10.58401/faqih.v10i2.1539

Oratmangun, A. Y. (2016). Kajian Hukum Terhadap Kemampuan Bertanggung Jawab Menurut Pasal 44 KUHP. *Lex et Societatis*, *4*(5). https://doi.org/10.35796/les.v4i5.11966

Putra, A. S., & Haq, L. M. H. (2024). Tanggung Jawab Hukum Penggunaan Artificial Intelligence Terhadap Pelanggaran Data Pribadi Pada Platform E-Commerce. *Commerce Law*, *4*(1). https://doi.org/10.29303/commercelaw.v4i1.4675

Qamar, N., Syarif, M., Busthami, D. S., Hidjaz, M. K., Aswari, A., Djanggih, H., & Rezah, F. S. (2017). *Metode Penelitian Hukum (Legal Research Methods)*. CV. Social Politic Genius (SIGn).

Ramadhan, A. R. P. P., & Muttaqin, L. (2023). The Role of The State Towards Victims of Electronic-Based Sexual Violence in Law No. 12 Years 2022. *Proceeding International Conference Restructuring and Transforming Law*, *2*(1), 38–46. https://proceedings.ums.ac.id/icrtlaw/article/view/3548

Ruslinia, A., Alfa, A. A., & Triantama, F. (2023). Analisis Aktor Non Negara dan Ketahanan Psikologi: Studi Kasus Kekerasan Berbasis Gender Online (KBGO). *Jurnal Ketahanan Nasional*, *29*(2), 178–198. https://doi.org/10.22146/jkn.86516

Sugiyanto, O. (2021). Perempuan dan revenge porn: Konstruksi sosial terhadap perempuan Indonesia dari preskpektif viktimologi. *Jurnal Wanita Dan Keluarga*, *2*(1), 22–31. https://doi.org/10.22146/jwk.2240

Tempo. (2025, Agustus | 20.40 WIB). *Ledakan Pornografi Deepfake di Era AI | tempo.co*. Tempo. https://www.tempo.co/newsletter/ledakan-pornografi-deepfake-di-era-ai-2056243

Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). *Pemolisian Digital dengan Artificial Intelligence*. PT. RajaGrafindo Persada - Rajawali Pers.

Wibowo, F. A., & Permana, I. S. (2025). Legal Study On Handling Cases Of Sextortion Involving Minors As Perpetrators And Victims In Indonesia. *JURNAL HUKUM SEHASEN*, *11*(1), 45–50. https://doi.org/10.37676/jhs.v11i1.7306

Zaltina, P., & Nurtjahyo, L. (2024). Right to be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases. *The Indonesian Journal of Socio-Legal Studies*, *3*(2). https://doi.org/10.54828/ijsls.2024v3n2.4

