

International Journal of Social Sciences and Humanities
Vol. 4 No. 3, October 2026, pages: 1896-1906
e-ISSN: 2985-6469
https://ejournal.45mataram.ac.id/index.php/ijssh

Regulation and Criminal Liability for Artificial Intelligence-Based (Deepfake) Pornography in Indonesian Criminal Law

Amelia Purpita Sari[1]*, Ferry Irawan Febriansyah[2], Aries Isnandar[3]
Corresponding author email : *ameliapuspitasari1527@gmail.com*

Article History

Manuscript submitted:
09 Agustus 2026
Manuscript revised:
19 September 2026
Accepted for publication:
19 Oktober 2026

Keywords

Deepfake Pornography; Artificial Intelligence; Criminal Liability; Consent; Legal Certainty;

Abstract

AI-based deepfake pornography enables a person's face or identity to be placed in sexual material without consent, raising questions about the reach of legal norms, victim protection, and offender liability. This study aimed to examine the regulation of the creation and distribution of such content and to identify the juridical problems in its application under Indonesian criminal law. Normative legal research with statute and conceptual approaches was employed; legal materials were gathered through library research and analysed qualitatively through legal interpretation and deductive reasoning. The results showed that no provision explicitly refers to artificial intelligence or deepfakes, yet the conduct can be reached through the National Criminal Code, the Pornography Law, the Sexual Violence Crimes Law, the Electronic Information and Transactions Law, and the Personal Data Protection Law, provided that the elements of each offence are met. The problems identified include the unclear coverage of pornography over synthetic content, the position of victim consent, the distinction between the liability of creators and distributors, overlapping provisions, and proof of authenticity and intent. The study concluded that clearer norms, regulatory harmonisation, and stronger victim protection are needed to ensure legal certainty and justice.

Copyright © 2025, The Author(s).
This is an open access article under the BY-NC-ND license

Contents

Abstract 1896
Introduction 1897
Methods 1898
Results and Discussions 1898
Conclusion 1903
Reference 1904

[1] Law Study Program (Ilmu Hukum), Universitas Muhammadiyah Ponorogo, Ponorogo, Indonesia
[2] Law Study Program (Ilmu Hukum), Universitas Muhammadiyah Ponorogo, Ponorogo, Indonesia
[3] Law Study Program (Ilmu Hukum), Universitas Muhammadiyah Ponorogo, Ponorogo, Indonesia

Introduction

Advances in artificial intelligence (AI) have changed the way visual and audio content is produced. Images, voices, and videos can now be generated or altered to a degree that makes them hard to distinguish from genuine recordings. Deepfakes are one product of this technology: synthetic material designed to resemble real people or real events. While the technology offers benefits for the creative industries and education, it also opens the door to misleading content that harms others (Brigham et al., 2024). A systematic review of the criminal justice system has further noted that deepfakes may compromise the integrity of evidence and judicial processes (Sandoval et al., 2024). The most troubling form of misuse is deepfake pornography, namely sexual material that uses a person's face or identity without that person's consent. Unlike the distribution of intimate recordings that actually exist, such content portrays the victim engaging in sexual acts that never took place and were never recorded. Brigham et al. (2024), studying perceptions of AI-generated non-consensual intimate imagery, emphasise that the absence of consent lies at the heart of the problem. Aurelita and Lewoleba (2024) note that the impact on victims is highly complex, ranging from psychological trauma, social isolation, and loss of self-confidence to economic losses resulting from damaged reputations. The issue therefore extends beyond the obscene character of the material and touches on the dignity, privacy, and right of individuals to control the use of their identity. The same study identifies women as particularly vulnerable to victimisation owing to social and psychological factors, underlining that the harm suffered by victims deserves particular attention.

The synthetic nature of the content makes victim protection difficult. Because it carries the identity of a real person, the content is easily perceived as authentic even though the depicted event is fictitious. Once uploaded, digital material can be copied and redistributed indefinitely, making its circulation almost impossible to contain. Nasution et al. (2024) show that efforts to restore victims through the right to be forgotten still face numerous practical obstacles. Legal analysis must therefore account for the manipulative character of the content and the harm it causes, rather than merely the existence of sexual imagery. Under positive law, conduct related to deepfake pornography intersects with several statutes, including the National Criminal Code (Law Number 1 of 2023), Law Number 44 of 2008 on Pornography, Law Number 12 of 2022 on Sexual Violence Crimes (TPKS Law), the Electronic Information and Transactions Law as last amended by Law Number 1 of 2024 (ITE Law), and Law Number 27 of 2022 on Personal Data Protection (PDP Law). Each statute has its own scope and elements. Noerman and Ibrahim (2024) observe that Indonesia has not explicitly regulated deepfakes and still relies on general provisions on the falsification of personal data under the PDP Law and on electronic falsification under the ITE Law. Consequently, the availability of several relevant norms does not automatically mean that every act of creating or distributing deepfake pornography can be punished without a careful examination of the elements of the offence.

Legal problems arise when these norms are applied to AI-manipulated sexual content. First, it must be examined how far the definition of pornography extends to images or videos showing a person engaged in sexual conduct that he or she never performed. Second, the unauthorised use of a face or identity must be distinguished from the question of consent to the creation and distribution of content. Third, the liability of the creator is not necessarily identical to that of the distributor, since the conduct, role, and culpability of each must be assessed separately. Fourth, there are obstacles in proving the authenticity of content, tracing perpetrators, and establishing intent. Several studies have addressed this topic. Novera and Fitri Z. (2024) examined the criminal law regulation of image-manipulation technology misused to disseminate pornography through social media accounts,

whereas Putra and Dewi (2024) stressed the urgency of a specific offence for deepfake pornography. Fauzi et al. (2025) concluded that producing pornographic content with deepfake technology fulfils the elements of a criminal offence, including intent, yet the absence of specific rules forces law enforcement to rely on an extensive interpretation of pornography provisions. Polandos et al. (2025) concluded that the ITE Law and the Criminal Code can be used although they lack specificity, and Meliala and Utari (2026) identified the absence of a legal definition of deepfakes and of an accountability mechanism covering the entire AI production chain. Unlike these studies, this article concentrates on both the creation and the distribution of deepfake pornography that uses the face or identity of an adult without consent, examining the interrelation of norms and the problems of their application after the National Criminal Code entered into force on 2 January 2026.

This article does not proceed from the assumption that deepfake pornography lacks any legal basis whatsoever. Its focus is to test the reach and the limits of existing norms, the legal position of the victim's consent, the allocation of liability between creators and distributors, and evidentiary issues. The object of study is limited to pornographic images or videos manipulated by AI that use the face or identity of an adult without consent, so that the analysis remains focused on the specific characteristics of that object. This study aims to analyse the regulation of the creation and distribution of AI-based deepfake pornography under Indonesian criminal law and to identify the juridical problems arising in its application. The findings are expected to offer a more systematic picture of the relationship between the relevant provisions and to inform the reform of legal protection for victims.

Methods

This study is normative legal research of a prescriptive nature, taking as its object the norms governing the creation and distribution of AI-based deepfake pornography. Two approaches were employed: a statute approach to examine the relevant provisions and a conceptual approach to unpack the concepts of pornography, consent, legal certainty, and criminal liability (Marzuki, 2021). This combination of approaches is common in recent normative criminal law scholarship, for instance in assessing the certainty of criminal liability norms and criminalisation under the National Criminal Code (Bimantoro et al., 2026; Maryanto et al., 2026). Primary legal materials comprised legislation on criminal law, pornography, electronic-based sexual violence, electronic information and transactions, and personal data protection. Secondary legal materials consisted of books, journal articles, and relevant research findings, while tertiary materials were used sparingly to clarify terminology (Muhaimin, 2020). Legal materials were collected through library research by tracing, inventorying, selecting, and classifying them according to the two research questions. The analysis was qualitative, using legal interpretation and deductive reasoning: the elements of each provision, the relationships among provisions, and their application to the creation and distribution of deepfake pornography were examined, including the issues of victim consent, criminal liability, and evidence (Muhaimin, 2020).

Results and Discussions

1. Theoretical and Conceptual Framework

a. Theory of Legal Certainty

Legal certainty is one of the aims of law, providing guidance on which acts are permitted and which are prohibited. General rules enable citizens to know the limits of their conduct while protecting them from arbitrary exercise of power. Certainty is therefore not achieved merely by the

existence of statutory text; it also requires clear formulation and consistent application (Oktaviani et al., 2026). In criminal law, certainty is closely tied to the principle of legality: punishment may be imposed only on the basis of applicable rules and after the elements of an offence have been proven. Vague formulations open the way to divergent interpretations of what is prohibited and of the limits of an offender's liability. Maryanto et al. (2026) demonstrate how conflicting, overlapping, and vague norms produce inconsistent judicial interpretation, calling for clearer legislative formulation.

This theory is used to assess whether provisions on pornography, electronic-based sexual violence, and offences committed through electronic systems can be applied to manipulated sexual content that uses a person's identity without consent. The absence of a provision expressly mentioning deepfakes is not immediately read as a legal vacuum; what is tested is the clarity, interrelation, and limits of application of the existing norms.

b. Theory of Criminal Liability

Criminal liability is the basis for determining whether the perpetrator of an offence may be punished. Fulfilment of the actus reus is insufficient on its own, as the culpability and circumstances of the offender must still be assessed (Rusianto, 2016). In this context, the act of creating content must be separated from the act of distributing it. A creator is involved in manipulating an image or video, whereas a distributor performs a different act, such as uploading or forwarding the content. The doctrine of participation (deelneming) requires that principal perpetrators and participants be distinguished according to their respective roles so that sentencing reflects each person's degree of culpability (Wasolo et al., 2026). Criminal liability must accordingly rest on concrete conduct, the elements of the offence, and the culpability of each party, not merely on the fact that someone stored or once accessed the content.

c. The Concept of AI-Based Deepfake Pornography

A deepfake is image, audio, or video content generated or altered by AI so as to resemble a particular person or event. The technology can swap faces, animate expressions, or create visuals that look real even though the depicted event never occurred. In this article, deepfake pornography is confined to AI-manipulated sexual images or videos that use the face or identity of an adult without consent (Brigham et al., 2024). This characteristic allows a person to be depicted as taking part in sexual activity he or she never engaged in. The problem therefore concerns not only the pornographic nature of the material but also the use of identity, consent, honour, and privacy. The unlawful use of personal data can cause reputational harm and psychological effects for the persons whose data are misused (Armanda & Nasution, 2024). Moreover, the use of AI does not by itself prove that the elements of a particular offence are fulfilled, so every provision must still be tested against its wording and elements.

2. Regulation of the Creation and Distribution of AI-Based Deepfake Pornography in Indonesian Criminal Law

The defining feature of deepfake pornography lies in the use of a real person's identity in a synthetic sexual representation. Criminal law assessment must therefore consider the form of the content, its sexual substance, the perpetrator's conduct, and its conformity with the elements of the offences defined by statute (Brigham et al., 2024). Previous studies have concluded that the liability of perpetrators can still be constructed through existing provisions even though no specific deepfake offence exists (Fauzi et al., 2025; Sonia et al., 2025).

a. Regulation under the National Criminal Code

The National Criminal Code is one of the main foundations of the analysis. Article 172 defines pornography, while Article 407 governs offences relating to the production and dissemination of pornography. Because its wording does not restrict the method of production to any particular technology, the provision is open to application to AI-generated content, provided that the object and the perpetrator's conduct satisfy its elements (Law Number 1 of 2023; Law Number 1 of 2026). The application of Article 407 must be differentiated according to the form of conduct. A person who knowingly produces deepfake pornography may be assessed under the elements of producing or making, whereas a person who duplicates, uploads, sends, or disseminates it must be assessed under the elements specifically formulated for those acts. The use of deepfake technology does not in itself determine liability; law enforcement authorities must still prove the pornographic nature of the content and the fulfilment of the elements of the offence charged.

Changes to criminal provisions following the entry into force of the National Criminal Code must also be considered. Through Article 622, several penal provisions of the Pornography Law were re-referenced, including the reference to Article 29, which now points to Article 407(1) of the National Criminal Code. Analysis of deepfake pornography thus cannot simply cite the old provisions of the Pornography Law; it must take into account the validity and amendment of the relevant norms. The formulation of morality offences in the National Criminal Code must also be tested against the harm principle and proportionality to avoid overcriminalisation (Bimantoro et al., 2026); in non-consensual deepfake cases, however, the harm to the victim is concrete, which strengthens the legitimacy of punishment.

b. Regulation under the Pornography Law

Law Number 44 of 2008 remains relevant for assessing the character and substance of the content, bearing in mind the amendment of its penal provisions. Article 1 point 1 defines pornography through various forms, including drawings, photographs, moving images, animations, and other messages containing obscenity or sexual exploitation that violate the norms of decency. Although the term deepfake does not appear, this definition can be used to test whether AI-manipulated content qualifies as pornography based on its form and substance (Law Number 44 of 2008). Article 4(1) prohibits, among other things, producing, making, reproducing, duplicating, disseminating, broadcasting, offering, trading, and providing certain pornography. Under this wording, the act of creating and the act of distributing deepfake content can be analysed separately according to the form of conduct. Fauzi et al. (2025) caution that reliance on such extensive interpretation may create legal uncertainty and sit uneasily with the principle of legality. Its application nonetheless depends on the fulfilment of the elements, not merely on the fact that the content was produced with AI. Another relevant provision is Article 9 in conjunction with Article 35, which prohibits making another person an object or model of pornographic content and sets out the corresponding penalty. In deepfake cases, the use of a person's face or identity in a synthetic sexual representation raises the question of whether that person can be regarded as an object or model. Because the statute does not address the use of digital identity in synthetic content, its application requires careful interpretation of the elements of the provision and the nature of the conduct.

c. Regulation under the TPKS Law, the ITE Law, and the PDP Law

The TPKS Law regulates electronic-based sexual violence, notably in Article 14. This provision covers recording or taking sexually explicit images without right and without consent, transmitting sexually explicit electronic information against the will of the recipient, and other conduct set out

therein (Law Number 12 of 2022). When applied to deepfake pornography, it must be examined whether the perpetrator's conduct satisfies these specific elements, since synthetic content does not always originate from direct recording of the victim's body. Beyond punishment, victim protection needs strengthening because the TPKS Law, the Witness and Victim Protection Law, and the PDP Law have not been accompanied by rules specifically addressing deepfake pornography (Aurelita & Lewoleba, 2024).

The ITE Law contains provisions on the manipulation of electronic information or documents so that they appear authentic. Article 35 in conjunction with Article 51(1) may be relevant where a perpetrator intentionally and without right creates or manipulates an electronic document so that the content is regarded as genuine (Law Number 1 of 2024). Polandos et al. (2025) also regard the ITE Law as one of the bases available to prosecute perpetrators, even though its wording lacks specificity. Not every deepfake, however, automatically falls under this provision, since the purpose of the manipulation and the elements of the offence must be proven in each concrete case. The PDP Law is also relevant because a facial image is data capable of identifying a person. Processing such data to produce sexual content without a lawful basis opens the possibility of applying the prohibitions on unlawfully using another person's personal data and on creating or falsifying personal data (Law Number 27 of 2022; Noerman & Ibrahim, 2024). Nevertheless, unlawfulness and the perpetrator's purpose must still be proven in every case.

d. Interrelation of Provisions and Their Application to Creators and Distributors

The relevant norms are spread across several statutes with different protective orientations. The National Criminal Code and the Pornography Law focus on pornographic content and on its production and dissemination, while the TPKS Law and the ITE Law become relevant where the conduct satisfies the elements of electronic-based sexual violence or the manipulation of electronic documents, and the PDP Law applies insofar as personal data are processed unlawfully. These norms must be read systematically so that the basis for punishment rests on the fulfilment of elements, not merely on a shared object or electronic medium. Distinguishing creators from distributors is equally important. Creators generate or manipulate content, while distributors upload, send, duplicate, or make it available to others. These roles are not always performed by the same person and are not always accompanied by identical forms of culpability, so the liability of each must be determined on the basis of conduct, culpability, and the provisions proven to apply. In addition, the digital platforms on which content circulates exercise substantial operational control, yet regulatory fragmentation often creates accountability gaps for losses suffered by users (Erlyani et al., 2026).

It follows that Indonesian criminal law provides several provisions for assessing the creation and distribution of deepfake pornography, but their application demands careful examination of the character of the content and the elements of the offence. The absence of a provision naming the phenomenon does not mean that the conduct lies entirely beyond the reach of the law. What requires further scrutiny is the clarity of the norms' coverage of manipulated content, the position of victim consent, the interrelation of provisions, and the determination of the liability of creators and distributors.

3. Juridical Problems in the Regulation of AI-Based Deepfake Pornography

a. Unclear Scope of the Definition of Pornography for Manipulated Content

The first problem is the absence of any explicit reference to AI-manipulated pornography. The National Criminal Code and the Pornography Law define pornography broadly but do not clearly distinguish between authentic content, conventionally edited content, and synthetic content generated

by AI. Meliala and Utari (2026) likewise found that the lack of a legal definition of deepfakes is a key deficiency across the ITE Law, the National Criminal Code, and the PDP Law. This does not necessarily amount to a legal vacuum, but it raises interpretive problems when a person's identity is used to create a sexual representation of events that never occurred. The falsity of content does not remove its pornographic character. Prohibited sexual images or videos are still assessed on the basis of their substance and the elements of the provision, even if produced by AI. The difficulty is that existing formulations do not clarify the status of digital identity, false sexual representations, and content that has been created but not yet disseminated.

b. Use of Identity without Consent

The unauthorised use of a face or identity is the core of deepfake pornography. Victims may be portrayed engaging in sexual activity without ever having taken part in it or consented to the use of their identity for sexual purposes. Permission to use a photograph in one context cannot be construed as permission to turn it into pornographic content. The legal position of consent must be read according to the wording of each statute. The TPKS Law regulates electronic-based sexual violence with elements that must be proven independently, while the PDP Law governs the processing of personal data on lawful bases. Reporting mechanisms and claims for compensation for the misuse of personal data are considered important to safeguard individual rights (Armanda & Nasution, 2024). The victim's lack of consent is thus a crucial fact, but punishment must still rest on the fulfilment of the elements of the relevant offence.

c. Liability of Creators and Distributors

Deepfake pornography also complicates the allocation of liability among the parties involved. The creator, the person who commissions the content, the first uploader, and subsequent sharers may have different roles and levels of knowledge (Rusianto, 2016). Aurelita and Lewoleba (2024) found that the absence of specific rules complicates proof, the naming of suspects, and the choice of applicable provisions, so the role of each party must be assessed separately. Involvement in the circulation of content therefore cannot simply be equated with involvement in its creation. Liability must be determined by considering concrete conduct, the element of culpability, and the link between the perpetrator's act and the content produced or disseminated. Evidence that a person uploaded content differs from evidence that he or she created or manipulated it in the first place. Accordingly, the doctrine of participation must distinguish principal perpetrators from participants based on their actual roles so that the sentences imposed are proportionate (Wasolo et al., 2026). This distinction prevents punishment based solely on suspicion or on a person's mere association with circulating content.

d. Interrelation and Application of Provisions

The relevant norms have different focuses and elements: the National Criminal Code and the Pornography Law concern pornographic content and its circulation, the TPKS Law regulates particular forms of sexual violence, and the ITE Law addresses the manipulation of electronic information or documents to make them appear authentic. Consequently, the choice of legal basis must begin with identifying the concrete conduct and testing the elements of each provision. Experience in other areas of law shows that where both general and specific provisions are available, courts may be inconsistent in determining which norm applies, thereby undermining legal certainty (Maryanto et al., 2026). Problems may arise when several provisions are deemed to apply simultaneously to a single course of conduct without adequate analysis of their respective scopes. The application of law must also take into account amendments to legislation and the norms in force at the

time the act was committed. Legal certainty is therefore not secured by the sheer number of legal bases but requires precision in selecting the provision that fits the facts of the case and the elements to be proven (Oktaviani et al., 2026).

e. Evidentiary Problems and Directions for Legal Reform

Proof is challenging because content can be designed to look authentic even though the victim never engaged in the depicted act. Law enforcement authorities must prove the manipulative nature of the content, the identity used, the involvement of the creator or distributor, and the culpability of each perpetrator. Digital forensic examination of metadata, communication traces, account information, and electronic devices can help link the content to the persons suspected of responsibility. The systematic review by Sandoval et al. (2024) confirms that deepfakes threaten the integrity of evidence, so detection capabilities and legal safeguards need continuous strengthening. Proof that an image is a deepfake does not automatically reveal who created or distributed it or whether that person acted intentionally. Technical proof of content authenticity must be distinguished from proof of the perpetrator's identity and culpability. Electronic evidence must therefore be examined carefully with due regard to its authenticity, integrity, and lawful acquisition in accordance with the applicable procedural law (Law Number 20 of 2025).

Legal reform could be directed toward clearer provisions on non-consensual synthetic intimate imagery, the use of a person's face or identity, and the distinction between creating and disseminating. Meliala and Utari (2026) propose a layered accountability model accompanied by mandatory labelling of synthetic content, while Putra and Dewi (2024) emphasise the need for a specific legal umbrella. Any new formulation must address intent, certainty regarding consent, and limits of application so as not to expand criminalisation excessively (Bimantoro et al., 2026). Clearer regulation is expected to strengthen victim protection while preserving legal certainty for all parties. Accordingly, the juridical problems of deepfake pornography are not accurately understood as an absolute legal vacuum, consistent with the finding that legal protection against this crime can still be pursued through the Criminal Code, the ITE Law, the PDP Law, and the Pornography Law (Putra & Dewi, 2024). The core problems are the unclear coverage of norms over synthetic content, the position of victim consent, the distinction between the liability of creators and distributors, the interrelation of provisions, and evidentiary difficulties. Harmonisation of legislation and guidelines for applying the law are needed so that cases can be handled accurately and proportionately while affording adequate protection to victims.

Conclusion

The creation and distribution of AI-based deepfake pornography can in principle be reached by several provisions of Indonesian criminal law, namely the National Criminal Code, the Pornography Law, the TPKS Law, the ITE Law, and the PDP Law. However, no single norm specifically regulates deepfake pornography as synthetic sexual content that uses a person's face or identity without consent. The application of existing provisions must therefore consider the character of the content, the form of conduct, the elements of the offence, and the liability of each party. The juridical problems identified include the unclear coverage of pornography over manipulated content, the position of victim consent, the distinction between the liability of creators and distributors, the interrelation of provisions, and the difficulty of proving content authenticity and intent. These problems are better understood as limitations and vagueness of norms than as an absolute legal vacuum; harmonised regulation, application guidelines, stronger evidentiary mechanisms, and victim protection are therefore required to achieve legal certainty and justice.

Lawmakers should formulate clearer provisions on AI-based deepfake pornography, particularly concerning the use of a face or identity without consent, the limits of punishable conduct, the element of intent, and the distinction between the liability of creators and distributors, accompanied by harmonisation across statutes to prevent divergent interpretations. Law enforcement authorities need to enhance their capacity to identify manipulated digital content, trace perpetrators, and assess the validity of electronic evidence, while protecting the identity, privacy, and condition of victims so that legal proceedings do not cause further harm. Public literacy on the risks of AI misuse and respect for consent and the right to one's identity in the digital sphere should also be improved. Future research could examine court decisions on deepfake pornography to test the consistency with which the norms analysed in this article are applied.

Acknowledgments

The authors are grateful to the anonymous reviewers for their valuable comments on the earlier version of this paper.

References

Armanda, M. A. G., & Nasution, K. (2024). Legal protection for employees who are harmed by data misuse by the company. *International Journal of Social Sciences and Humanities, 2*(3), 94–98. https://doi.org/10.55681/ijssh.v2i3.1504

Aurelita, M., & Lewoleba, K. K. (2024). Perempuan sebagai korban deepfake pornografi dalam perspektif viktimologi [Women as victims of deepfake pornography from a victimological perspective]. *Kertha Semaya: Journal Ilmu Hukum, 12*(12), 3382–3396. https://doi.org/10.24843/KS.2024.v12.i12.p19

Bimantoro, C. D., Jayanuarto, R., Arisandi, F., & Padmi, H. (2026). Criminalization of cohabitation in the new criminal code (A philosophical review in legal pluralism and privacy rights). *International Journal of Social Sciences and Humanities, 4*(2), 800–809. https://doi.org/10.55681/ijssh.v4i2.2824

Brigham, N. G., Wei, M., Kohno, T., & Redmiles, E. M. (2024). "Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 373–392). USENIX Association. https://www.usenix.org/conference/soups2024/presentation/brigham

Erlyani, R., Kolib, A., & Bakhtiar, H. S. (2026). Vicarious liability in Indonesian telemedicine: Reconstructing the legal status of digital health platforms. *International Journal of Social Sciences and Humanities, 4*(2), 364–372. https://doi.org/10.55681/ijssh.v4i2.2622

Fauzi, S. S., Rusmana, I. P. E., Darma, I. M. W., & Wulandari, N. G. A. A. M. T. (2025). Pengaturan sanksi pidana terhadap pelaku pembuat konten pornografi dengan menggunakan teknologi deepfake di Indonesia [Regulation of criminal sanctions against creators of pornographic content using deepfake technology in Indonesia]. *Al-Zayn: Jurnal Ilmu Sosial & Hukum, 3*(6), 9612–9623. https://doi.org/10.61104/alz.v3i6.2661

Law Number 1 of 2023 on the Criminal Code (Republic of Indonesia).

Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (Republic of Indonesia).

Law Number 1 of 2026 on Criminal Penalty Adjustment (Republic of Indonesia).

Law Number 12 of 2022 on Sexual Violence Crimes (Republic of Indonesia).

Law Number 20 of 2025 on the Code of Criminal Procedure (Republic of Indonesia).

.

Law Number 27 of 2022 on Personal Data Protection (Republic of Indonesia).

Law Number 44 of 2008 on Pornography (Republic of Indonesia).

Maryanto, Kolib, A., & Bakhtiar, H. S. (2026). Legal uncertainty in the criminal liability of health workers: A normative analysis of Article 440 of the Health Law and Article 360 of the Criminal Code. *International Journal of Social Sciences and Humanities, 4*(2), 604–614. https://doi.org/10.55681/ijssh.v4i2.2764

Marzuki, P. M. (2021). *Penelitian hukum* [Legal research] (Rev. ed.). Kencana.

Meliala, A. P. P. S., & Utari, I. S. (2026). Policy on the formulation of artificial intelligence accountability for the creation and dissemination of deepfake videos from a criminal law perspective in Indonesia. *Law Research Review Quarterly, 12*(2), 953–981. https://doi.org/10.15294/lrrq.v12i2.44714

Muhaimin. (2020). *Metode penelitian hukum* [Legal research methods]. Mataram University Press.

Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2024). Prospek pemenuhan right to be forgotten bagi korban deepfake pornography akibat penyalahgunaan artificial intelligence di Indonesia [The prospect of fulfilling the right to be forgotten for victims of deepfake pornography due to the abuse of artificial intelligence in Indonesia]. *Diponegoro Law Journal, 13*(2). https://ejournal3.undip.ac.id/index.php/dlr/article/view/43617

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk pelindungan negara [Criminalization of deepfakes in Indonesia as a form of state protection]. *Jurnal USM Law Review, 7*(2), 603–621. https://doi.org/10.26623/julr.v7i2.8995

Novera, O., & Fitri Z., Y. (2024). Analisis pengaturan hukum pidana terhadap penyalahgunaan teknologi manipulasi gambar (deepfake) dalam penyebaran konten pornografi melalui akun media sosial [Analysis of criminal law regulation of the misuse of image-manipulation technology (deepfake) in disseminating pornographic content through social media accounts]. *El-Faqih: Jurnal Pemikiran dan Hukum Islam, 10*(2), 460–474. https://doi.org/10.58401/faqih.v10i2.1539

Oktaviani, A., Hayati, D. R., Sinaga, E. S., Deris, D. N., & Irawan, T. I. (2026). Between innovation and legal vacuum: Evaluating Indonesia's criminal law readiness against deepfake artificial intelligence. *Jurnal Media Hukum, 33*(1), 158–177. https://doi.org/10.18196/jmh.v33i1.29574

Polandos, T. L., Lolong, W. R. J., & Kumajas, M. L. (2025). Pertanggungjawaban pidana pelaku deepfake porn menggunakan artificial intelligence (AI) [Criminal liability of deepfake porn perpetrators using artificial intelligence]. *Jurnal Rectum, 7*(2), 217–224. https://doi.org/10.46930/jurnalrectum.v7i2.5618

Putra, K. B. W., & Dewi, G. A. A. P. (2024). Urgensi pengaturan tindak pidana deepfake pornografi di Indonesia [The urgency of regulating deepfake pornography offences in Indonesia]. *Kertha Wicara: Journal Ilmu Hukum, 13*(10), 530–541. https://doi.org/10.24843/KW.2024.v13.i10.p5

Rusianto, A. (2016). *Tindak pidana dan pertanggungjawaban pidana: Tinjauan kritis melalui konsistensi antara asas, teori, dan penerapannya* [Criminal acts and criminal liability: A critical review through consistency between principles, theory, and application]. Prenadamedia Group.

Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science, 13*, Article 41. https://doi.org/10.1186/s40163-024-00239-1

Sonia, S., Sudarti, E., & Erwin, E. (2025). Tindak pidana deepfake porn berbasis artificial intelligence (AI) dalam hukum Indonesia [AI-based deepfake porn offences in Indonesian law]. *PAMPAS: Journal of Criminal Law, 6*(3), 342–354. https://doi.org/10.22437/pampas.v6i3.45188

Wasolo, A. T., Ollong, E., Latuconsina, R., Toisuta, P., & Zainuddin. (2026). The doctrine of participation in abuse of authority offenses: Toward proportional sentencing in Indonesia's anti-corruption law. *International Journal of Social Sciences and Humanities, 4*(2), 996–1013. https://doi.org/10.55681/ijssh.v4i2.2972