International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulfindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Legal Protection and Law Enforcement of Sexual Crimes Through Deepfake Programs in Indonesia

I Made Yudha Pradnyana
Universitas Pendidikan Nasional, Indonesia
NI Gusti Agung Ayu Mas Tri Wulandari
Universitas Pendidikan Nasional, Indonesia

Corresponding Author: uncleyeey@gmail.com

Abstract

The proliferation of Artificial Intelligence (AI) has inadvertently fostered malicious software like deepfake, which is widely exploited to facilitate non-consensual sexual content. This study investigates the legal parameters and enforcement efficacy regarding deepfake-facilitated sexual offenses in Indonesia. While existing literature largely examines deepfakes through the lens of fraud, a significant legal lacuna remains concerning AI-generated obscenity. Adopting a doctrinal legal framework, this inquiry integrates statutory, conceptual, factual, and comparative lenses. The analysis uncovers a critical statutory gap within Indonesia's legal architecture, specifically across the National Criminal Code, the ITE Law, and the PDP Law, as these instruments lack explicit provisions for synthetic media. This regulatory void undermines the lex certa principle, thereby generating substantial obstacles in both investigation and prosecution phase. Drawing lessons from civil law jurisdictions such as France and South Korea, this paper advocates for the enactment of a specialized legal framework to enhance victim protection and solidify legal certainty.

Keywords: Deepfake; Sexual Crimes; Law Enforcement; Regulation, Artificial Intelligence

INTRODUCTION

Over the past twenty years, the technology of development Artificial Intelligence has drastically altered global societal structures. The borderless connectivity offered by the internet has not only revolutionized the economic, communication, and education sectors but has also

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

created a new anonymous space for social interaction (Syahirah & Prasetyo, 2025). Advances in AI have given birth to innovations such as machine learning, deep learning, and Generative Adversarial Networks (GAN) that can mimic human cognitive abilities to a certain extent.

However, digital space is often misused as an instrument to commit unlawful acts (Yar & Steinmetz, 2019). This cybercrime phenomenon places computers as tools to launch criminal actions that are difficult to trace and have widespread impacts. One of the most concerning forms of cybercrime is sexual crimes in the digital realm. Traditionally, sexual crimes are regulated in the Criminal Code (KUHP) as acts that violate decency norms and public morality.

Entering the digital era, this paradigm has shifted. The escalation of threats in the digital realm is increasingly evident with the presence of deepfake programs that utilize AI technology. The term "deepfake" is a coinage of "deep learning" and "fake," referring to AI-based programs capable of manipulating audio-visual data to create highly realistic fake content, as if someone is doing something they never did (Nurkholisah et al., 2025). Deepfake programs use the GAN architecture consisting of two main components: a generator that produces new data resembling the original, and a discriminator that distinguishes between real and fake data.

Deepfake programs began to gain popularity in 2017 when an anonymous user on the Reddit online forum uploaded pornographic videos edited using the GAN algorithm. A study on the global deepfake landscape revealed shocking facts: 96% of all deepfake content circulating on the internet is pornography, and almost all of it targets women (Kasita, 2022). This phenomenon is categorized as a prevalent form of online gender-based violence, where perpetrators steal the authority of the victim's body in cyberspace.

The phenomenon of deepfake began to enter Indonesia around 2018-2019. The latest event that shocked the public occurred in January 2024, when explicit sexual images engineered by AI targeted a famous international singer and spread widely to Indonesia. The latest case in the public spotlight in Indonesia is the verdict against Chiko Radityatama Agung Putra. In the verdict hearing at the Semarang District Court, the panel of judges sentenced him to one year in prison and a fine of IDR 2 billion. Chiko was proven to have produced more than 1,100 files of photos and videos containing pornography using a deepfake program. It is interesting to note that in this case, the prosecution did not use Article 35 of the ITE Law but rather Article 407 paragraph (1) of the National Criminal Code regarding pornography (Putusan PN Semarang No. 12/Pid.Sus/2026/PN Smg, 2026).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

This inconsistency in the application of articles indicates a fundamental problem in regulations in Indonesia. There are several regulations intersecting with deepfake crimes, yet each contains ambiguous formulations. The ITE Law (Articles 27 and 35) uses phrases that lack clear operational definitions. The National Criminal Code (Article 407) inherits old provisions without providing clarity on digital content engineered by AI. The Personal Data Protection Law (Articles 65 and 66) regulates biometric data but does not specifically reach face manipulation through deepfake programs (Wiguna & Lestari, 2025). Consequently, law enforcement officials lack clear guidelines on what elements must be proven in deepfake cases.

Recent research confirms that the current regulations are reactive, do not contain technical definitions of deepfake, and have not fulfilled the principle of legal certainty (lex certa) in handling AI-based crimes (Cahyaningtyas & Harris, 2026). The absence of specific norms regarding deepfake results in blurred boundaries of criminal liability, both in terms of legal subjects and the forms of fault that can be imposed (mens rea and actus reus).

Based on a gap analysis of previous research, studies on deepfake generally focus on the aspects of fraud or defamation. This study offers novelty by specifically examining the legality and law enforcement mechanisms of deepfake-based sexual crimes in Indonesia based on the lex certa principle, as well as comparing them with civil law countries to formulate clear and unambiguous norm formulations.

PROBLEM FORMULATION

Based on the background described above, the research problems in this study are:

1. What is the legality of sexual crimes through deepfake programs in the Indonesian legal system?
2. How is the law enforcement mechanism for sexual crimes with deepfake programs in Indonesia?

LITERATURE REVIEW

The discourse on deepfake crimes has garnered significant academic attention. Waldyan and Hasibuan (2026) noted that while Indonesian positive law can prosecute perpetrators, it remains fragmented without specific regulations. Irawati (2025) conducted a comparative study revealing that Indonesia lags behind Australia and South Korea, which have implemented

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

progressive legal frameworks. Similarly, Budiman (2025) asserted that current regulations (UU ITE and KUHP) are overly general and fail to explicitly cover AI abuses like deepfakes.

This research distinguishes itself by simultaneously analyzing the disharmonization among the National Criminal Code, UU ITE, and UU PDP. It employs Gustav Radbruch's Legal Certainty Theory (lex certa) to assess the clarity of legal norms and Lawrence M. Friedman's Legal System Theory to evaluate the holistic effectiveness of law enforcement (substance, structure, and legal culture).

RESEARCH METHODOLOGY

This article employs a doctrinal legal inquiry, adopting a normative framework to dissect legal principles, doctrines, and statutory rules (Marzuki, 2021). The research relies on qualitative legal data. Authoritative primary sources include the 1945 Constitution, the National Criminal Code, the ITE Law, the PDP Law, the TPKS Law, and the Semarang District Court Decision No. 12/Pid.Sus/2026/PN Smg. Secondary materials are drawn from relevant academic literature and legal books, supplemented by tertiary sources such as legal dictionaries. As a purely doctrinal study, no human informants are involved. The researcher functions as the primary instrument, utilizing a documentation checklist to collect data through comprehensive library research and document analysis.

To ensure a multifaceted analysis, four distinct approaches are utilized:

1. *Statute Approach*: Evaluating relevant legislative texts, specifically focusing on the National Criminal Code, ITE Law, and PDP Law concerning sexual offenses and data manipulation.
2. *Conceptual Approach*: Applying Radbruch's theory of legal certainty (lex certa) and Friedman's legal system theory to scrutinize the regulatory framework.
3. *Fact Approach*: Contextualizing the legal discussion by analyzing the real-world implications of the Semarang District Court ruling.
4. *Comparative Approach*: Benchmarking Indonesia's regulations against those of civil law jurisdictions, particularly France and South Korea, to identify best practices.

The collected legal materials are processed using descriptive qualitative analysis. The reasoning follows a deductive structure, moving from overarching legal principles to specific conclusions regarding deepfake-facilitated sexual crimes. The findings are presented prescriptively, offering actionable legal recommendations. To maintain data credibility, the study

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

employs source triangulation by verifying the hierarchical consistency and synchronization of the cited regulations.

RESULT OF RESEARCH AND DISCUSSION

Legality of Sexual Crimes Through Deepfake Programs in the Indonesian Legal System

The first research problem requires an answer regarding the status or validity (legality) of sexual crimes through deepfake based on the principle of legality (lex certa). The findings show that regulations regarding sexual crimes in Indonesia have not explicitly regulated deepfake programs as a standalone criminal offense, thus creating a vague norm.

The National Criminal Code (Law No. 1 of 2023) regulates the crime of pornography in Article 407 with a minimum imprisonment of 6 months and a maximum of 10 years. The definition of pornography in Article 172 includes moving images, animations, cartoons, conversations, body movements, or other message sounds containing obscenity. However, from the perspective of the legality principle (lex certa), the definition does not explicitly state whether synthetic content engineered by AI programs (deepfake) falls into the category of moving images or animations intended (Hiariej & Santoso, 2025). This ambiguity implies that the application of Article 407 can only reach perpetrators at the distribution stage but does not specifically regulate the process of making deepfake content for private consumption (Noerman & Ibrahim, 2024).

The ITE Law (Articles 27 and 35) bans decency violations but lacks operational definition for deepfakes without an operational definition, while Article 35 prohibits the manipulation of electronic information but does not provide a strict boundary between "criminal forgery" and "digital creativity" (such as parody). The phrase "intentionally" also creates ambiguity when faced with deepfakes generated automatically by AI. Research on norm ambiguity concludes that the ITE Law can only prosecute perpetrators at the downstream stage (distribution) and cannot criminalize the process of making deepfakes if done for private offline consumption (Sompotan et al., 2026).

Meanwhile, the PDP Law (Articles 65 and 66) has not explicitly regulated the processing of biometric data using AI to create synthetic content. Article 66 prohibits the falsification of personal data, but it is unclear whether deepfake content using someone's face automatically falls into the category of personal data falsification (Wiguna & Lestari, 2025). As a result, victims of deepfake experience extreme difficulties in obtaining personal data protection (Cahyaningtyas & Harris, 2026).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Table 1. Analysis of Norm Ambiguity in Three Regulations

No	Regulation	Norm Formulation	Form of Ambiguity	Impact
1	National Criminal Code (Articles 172 and 407)	Pornography includes moving images, animations, cartoons	Unclear whether synthetic content engineered by AI is included in the definition	Only reaches the distribution stage, does not regulate production for private consumption
2	ITE Law (Articles 27 and 35)	Prohibition of content violating decency and manipulation of electronic information	Phrases "violating decency", "manipulation", and "intentionally" lack operational definitions	Officials perform extensive interpretation which potentially violates the legality principle
3	PDP Law (Articles 65 and 66)	Prohibition of falsification and unlawful use of personal data	Unclear whether manipulated victim's face/voice constitutes fake personal data	Does not regulate biometric data processing using AI; victims struggle to get personal data protection

Based on Table 1 above, it can be analyzed that the three regulations have intersection points but overlap. This vague norm causes law enforcement officials to perform extensive interpretation, which potentially violates the legality principle (Nurkholisah et al., 2025). Under Radbruch's Legal Certainty Theory, ambiguity in the KUHP undermines legal objectives: certainty, justice, and utility (Hiariej, 2016). This is evident from the disparity in judges' verdicts in similar cases, the difficulty for victims to obtain justice, and the ineffectiveness of the regulation's preventive function.

Law Enforcement Mechanism for Sexual Crimes with Deepfake Programs in Indonesia

According to the Legal System Theory (Lawrence M. Friedman), deepfake law enforcement in Indonesia faces obstacles in three main components: substance, structure, and legal culture (Friedman, 1975).

At the investigation stage, officials face obstacles in tracking perpetrators using anonymous identities and encryption technology, as well as limited digital forensic laboratories

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

for AI-engineered content (Wicaksono et al., 2026). At the prosecution stage, there is uncertainty in determining the appropriate article due to norm ambiguity. At the judicial stage, judges do not have clear guidelines for classifying offenses, resulting in varying verdicts. At the content takedown stage, the mechanism regulated in Article 26 of the ITE Law has not been effective because victims must go through a long court process while deepfake content can spread virally in hours (Setiawan et al., 2026).

Table 2. Analysis of Obstacles in Law Enforcement Mechanisms

No	Type of Obstacle	Explanation
1	Substantive Obstacle	Norm ambiguity, absence of specific regulations, ambiguous article formulations
2	Structural Obstacle	Limited technical capacity of officials, minimal digital forensic infrastructure
3	Cultural Obstacle	Low digital literacy, stigma against victims (victim blaming)

The review of Table 2 shows that substantive obstacles are the root of the problem. Without clear norms (lex certa), the legal structure lacks operational guidelines, and the legal culture of society is not optimally formed. This is exacerbated by the low digital literacy of the community and the high stigma against victims (victim blaming), causing victims to be reluctant to report their cases (Soekanto, 2013).

To measure the urgency of clarifying regulations in Indonesia, a comparative study with countries that have formulated clearer rules is crucial, especially countries adhering to the same legal system (civil law system).

Table 3. Comparison of Deepfake Regulations with Civil Law Countries

No	Country	Regulation	Advantages
1	Netherlands	Progressive judge jurisprudence (Amsterdam Court Decision November 2, 2023)	Overcomes legal ambiguity through adaptive judge decisions
2	France	Article 226-8-1 of the French Criminal Code regarding sexual visual/audio content resulting from algorithms	Explicitly regulates content resulting from algorithmic engineering

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

3	South Korea	Criminalizes deepfake viewers with a threat of 3 years imprisonment	Protects victims by criminalizing content consumers
4	Germany	Drafting Bill § 201b StGB-E regarding the criminalization of deepfake pornography	Currently formulating comprehensive specific regulations

Based on Table 3, it can be analyzed that France and South Korea have successfully exited norm ambiguity by formulating explicit regulations. France mentions "sexual visual or audio content generated by algorithmic processing," while South Korea even criminalizes viewers. Meanwhile, the Netherlands proves that regulatory ambiguity can be overcome through progressive judge jurisprudence (Limiardo, n.d.). This shows that Indonesia is still lagging in terms of regulatory clarity.

According to Friedman's Legal System Theory, the three components of the legal system (substance, structure, culture) must work synergistically for the legal system to function effectively in society (Friedman, 1975). These three components have not worked synergistically in handling sexual crimes with deepfake programs, mainly due to norm ambiguity in the substance component, which then impacts structure and culture.

Therefore, the ideal law enforcement mechanism in Indonesia must include reform in three areas: (1) Legal Substance, through the establishment of specific regulations (lex specialis) defining deepfake and harmonizing laws; (2) Legal Structure, through strengthening the digital forensic capacity of officials and proactive obligations of digital platforms; and (3) Legal Culture, through increasing national digital literacy and gender-sensitive victim protection.

CONCLUSION

Based on the discussion above, it can be concluded that:

1. The legality of sexual crimes through deepfake programs in the Indonesian legal system is still ambiguous and has not fulfilled the lex certa principle. The three existing regulations (National Criminal Code, ITE Law, and PDP Law) have not explicitly regulated deepfake as a separate criminal offense, so the formulations of the articles are ambiguous. This has an impact on the disparity in judges' verdicts and the non-fulfillment of the values of legal certainty, justice, and utility as per Gustav Radbruch's theory.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

2. The law enforcement mechanism for sexual crimes with deepfake programs in Indonesia is currently not running effectively. There are obstacles at the investigation stage (forensic limitations), prosecution (article uncertainty), judiciary (no offense classification guidelines), and content takedown. Comprehensive legal system reform is needed, including the establishment of a special law (lex specialis) adaptive to AI, strengthening the capacity of law enforcement institutions, and increasing public digital literacy to provide optimal protection for victims.

RECOMMENDATION

1. Legislators and Ministry of Law: Enact a lex specialis that explicitly defines deepfake and artificial intelligence to avoid ambiguity. This regulation must include a technical definition of deepfake, elements of the offense, and criminal sanctions that are proportional and adaptive to AI development. Harmonization between the National Criminal Code, ITE Law, and PDP Law is also needed to eliminate overlapping legal regimes.
2. Law Enforcement Officials (Police, Prosecutors, Judges): Capacity building through continuous training on AI and deepfake, especially in digital forensics and evidence in deepfake cases. Modernization of investigation facilities and the addition of accredited digital forensic laboratories. Establishment of a special task force involving Komdigi and the PDP Agency to handle deepfake cases and accelerate the takedown of illegal content.
3. Community and Digital Platforms: Increasing national digital literacy to reduce public vulnerability. Digital platforms must to proactively detect and remove illegal deepfake content while implementing gender-sesitive victim protection mechanisms.

REFERENCES

Arief, B. N. (2007). *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan I*. Kencana Prenada Media Group.

Cahyaningtyas, P., & Harris, F. (2026). *The Urgency of Regulations Related to Deepfakes and AI-Based Disinformation: A Review of Political Stability. International Journal of New Approaches to Law and Rationality in Nationhood*, 1(2), 728–736. https://doi.org/10.56861/Nalarnagara.V1i2

Friedman, L. M. (1975). *The Legal System: A Social Science Perspective.* Russell Sage Foundation.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Hiariej, E. O. S. (2016). *Prinsip-Prinsip Hukum Pidana.* Cahaya Atma Pustaka.

Hiariej, E. O. S., & Santoso, T. (2025). *Anotasi KUHP Nasional*. Rajawali Pers.

JDIH Kemenkeu. (2007). Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas. https://jdih.kemenkeu.go.id

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

Limiardo, M. (n.d.*). A Comparative Legal Analysis of Deepfake Transparency: Contrasting Indonesia's Absence of Law with China's Legislative Approach*. Dusturiyah Journal, 15(1). https://doi.org/10.22373

Marzuki, P. M. (2021). *Penelitian Hukum Edisi Revisi* (Vol. 55). Kencana Prenada Media.

Noerman, C. T., & Ibrahim, A. L. (2024). *Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara*. Jurnal USM Law Review, 7(2), 603–621. https://doi.org/10.26623/Julr.V7i2.8995

Nurkholisah, S., et al. (2025). *Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia*. Jurnal USM Law Review, 8(3), 2421–2445. https://doi.org/10.26623/Jurl.V8i3.13060

Putusan Pengadilan Negeri Semarang Nomor 12/Pid.Sus/2026/PN Smg. (2026).

Setiawan, R., et al. (2026). *Risiko 'Double Victimisation' Pada Korban Kekerasan Seksual Berbasis Elektronik (KSBE) Dalam Penegakan Hukum Deepfake Pornografi*. Lex Journal: Kajian Hukum & Keadilan, 10(2), 342–357. https://doi.org/10.25139/Lex.V10i2.11849

Soekanto, S. (2013). *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum* (1st ed.). Rajawali Pers.

Sompotan, S. A., et al. (2026). *Kekosongan Hukum (Rechtsvacuum) Dalam Penjeratan Tindak Pidana Pembuatan Dan Penyebaran Deepfake Pornografi Menggunakan Kecerdasan Buatan Di Indonesia*. Jurnal Fakultas Hukum Unsrat, 15(3), 1–12.

Syahirah, S. N., & Prasetyo, B. (2025). *Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia*. Jurnal Inovasi Hukum Dan Kebijakan, 6(1), 191–192. https://Ejurnals.Com/Ojs/Index.Php/Jihk

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wicaksono, D. T., et al. (2026). *Penegakan Hukum Pelaku Tindak Pidana Artificial Intelegence (Deepfake) Dalam Perspektif Hukum Positif Indonesia*. Jurnal Fakta Hukum, 4(2), 63–70.

Wiguna, A. A., & Lestari, P. A. A. (2025). *Perlindungan Hukum Terhadap Perempuan Korban Deepfake Pornography Di Indonesia. Jurnal Kajian Hukum Dan Kebijakan Publik,* 3(1). https://doi.org/10.24843/JMHU.2025.V14.103

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime And Society (N. Aguilera, Ed.; 3rd ed.).* SAGE Publications Ltd.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License