Received: 2025-08-06
Accepted: 2025-11-18
Issued: 2026-02-27
p-ISSN: 2541-2345, e-ISSN: 2580-8842


*DOI: 10.26623/jic.v11i2.12664*

Jurnal Ius Constituendum Volume 11 (2) June 2026
This work is licensed under a. Creative Commons Attribution 4.0 International License

# *Bridging Legal Gaps in AI-Generated Deepfake Pornography: A Comparative Approach to Privacy and Digital Ethics*

**Gefy Caesarati Zumarno[1], Sri Jaya Lesmana[2], Ratna Indayatun[3], Adlan Abdul Bin Razak[4]**
[1,2,3] Faculty of Law, Syekh-Yusuf Islamic University, Tangerang, Indonesia
[4] Fakulti Undang Undang, Universiti Teknologi MARA, Selangor, Malaysia
sjlesmana@unis.ac.id

***Abstract***

*This study aims to examine the legal gaps in regulating AI-generated deepfake pornography and to develop a comparative regulatory model to strengthen privacy protection and digital ethics in Indonesia. The rapid advancement of artificial intelligence has facilitated the creation and dissemination of non-consensual synthetic pornographic content, posing serious threats to individual privacy, dignity, and psychological well-being, while existing Indonesian laws remain fragmented and inadequate. This research employs normative legal research using statutory, conceptual, and comparative approaches, focusing on Indonesian regulations and comparative frameworks from California and South Korea. The findings reveal that current Indonesian legal instruments, including the Electronic Information and Transactions Law, the Pornography Law, and the Personal Data Protection Law, do not explicitly regulate deepfake pornography, resulting in legal uncertainty, enforcement challenges, and insufficient victim protection. In contrast, comparative jurisdictions provide clearer definitions, consent-based standards, and comprehensive victim remedies. This study proposes a regulatory reform model based on lex specialis principles, digital ethics, victim-centered protection, and adaptive legal governance to address AI-based digital crimes. The originality of this research lies in its integrative comparative framework that connects criminal law, personal data protection, and digital ethics to formulate a comprehensive and future-oriented legal response. These findings contribute to the development of responsive legal policies and provide a normative foundation for regulating synthetic media to safeguard digital privacy and human dignity in the artificial intelligence era.*
***Keywords:*** *Artificial Intelligence; Deepfake Pornography; Digital Ethics; Legal Reform; Privacy Protection*

## 1. INTRODUCTION

The Industrial Revolution 4.0 marks the rapid advancement of science and technology that is driving global digital transformation.[1] One of the important innovations[2] is artificial intelligence (AI),[3] including deepfake technology, which is digital engineering that uses deep learning to

[1] Rida Ristiyana, Eko Trianto, and Sri Jaya Lesmana, "Upaya Menghadapi Era Society 5 . 0 Melalui Sosialisasi Pembentukan Jiwa Entepreneur Dan Penyajian Laporan Keuangan Pada Generasi Muda Di Tangerang," *Jurnal SOLMA* 13, no. 2 (2024): 777–88, https://doi.org/10.22236/solma.v13i2.15193.

[2] Inas Sofia Latif, Hudaya Latuconsina, and Sri Jaya Lesmana, "Digitalisasi UMKM Di Kelurahan Selapajang Jaya: Strategi Social Media Marketing Dalam Menyongsong Era Modern (Digitalization of MSMEs in Selapajang Jaya Village: Social Media Marketing Strategy in Welcoming the Modern Era)," *Yumary: Jurnal Pengabdian Kepada Masyarakat* 5, no. 1 (2024): 45–55, https://doi.org/10.35912/yumary.v5i1.2939.

[3] Asri Gresmelian Eurike Hailtik and Wiwik Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia," *Asian Journal of Social and Humanities* 2, no. 4 (2024): 776–95, https://doi.org/10.59888/ajosh.v2i4.222.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

create fake audio, images, or videos that are very similar to the real thing. Initially, this technology was used positively, for example, in the broadcasting sector during the pandemic to replace the role of broadcasters virtually. But since 2017, deepfake technology has begun to be abused, especially to create fake pornographic content by attaching celebrity faces to the bodies of adult film actors. The rapid spread through digital platforms shows that these technologies are now easily accessible and usable, posing serious threats to privacy, digital ethics, and individual reputations.[4]

In line with the ease of access to technology, Online Gender-Based Violence (KBGO) is now an increasingly worrying issue in Indonesia, reflecting the structured and systematic forms of violence against women in the digital space. In 2023, there were 1,081 cases of GBV reported to Komnas Perempuan.[5] Meanwhile, in the first quarter of 2024, the Southeast Asia Freedom of Pression Network (SAFEnet) received 480 reports of GBV,[6] with the most common form is the threat of spreading intimate content, which reached 253 cases.[7] On the other hand, the production and spread of deepfake content has increased rapidly, with reports showing a nearly 100% increase in the number of deepfake videos on the internet between December 2018 until September 2019. Worryingly, 96% of the videos are pornographic content,[8] and all of them exploit women as objects.[9]

This phenomenon requires serious attention from various parties, including the government, non-governmental organizations, and civil society,[10] to strengthen protection for victims of GBV and prevent the spread of similar cases. Several cases of deepfake pornography have also occurred in Indonesia, one of which befell the public figure Nagita Slavina. Based on Kompas.com report, in early 2022 the public was shocked by the circulation of a 61-second video featuring a figure with a face similar to Nagita.[11] The results of the investigation by the Metro Jaya Police Cyber Team showed that the video was the result of deepfake technology manipulation, where the victim's

[4] Hanqing Zhao et al., "Multi-Attentional Deepfake Detection," in *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)* (Nashville: IEEE: Insitute of Electrical and Electronics Engineers, 2021), https://doi.org/10.1109/CVPR46437.2021.00222.

[5] Komnas Perempuan, "Siaran Pers Gerak Bersama Dalam Data: Laporan Sinergi Database Kekerasan Terhadap Perempuan Tahun 2023," Komnas Perempuan, 2024, https://komnasperempuan.go.id/siaran-pers-detail/siaran-pers-gerak-bersama-dalam-data-laporan-sinergi-database-kekerasan-terhadap-perempuan-tahun-2023.

[6] Biro Hukum dan Humas KemenPPPA, "Gandeng Sejumlah Pihak, Kemen PPPA Dorong Aksi Bersama Lindungi Perempuan Dan Anak Dari Kekerasan Di Ranah Daring," KemenPPPA, 2024, https://kemenpppa.go.id/siaran-pers/gandeng-sejumlah-pihak-kemen-pppa-dorong-aksi-bersama-lindungi-perempuan-dan-anak-dari-kekerasan-di-ranah-daring.

[7] Tim CNN Indonesia, "SAFEnet: Kekerasan Berbasis Gender Naik, Terbanyak Usia 18-25 Tahun," *CNN Indonesia*, 2024, https://www.cnnindonesia.com/teknologi/20240509094321-192-1095678/safenet-kekerasan-berbasis-gender-naik-terbanyak-usia-18-25-tahun.

[8] Henry Ajder et al., "The State of Deepfakes: Landscape, Threats, and Impact," 2019, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

[9] *Ibid.*

[10] Sri Jaya Lesmana et al., "Pemberdayaan Masyarakat Melalui Teknologi Pengelolaan Sampah Menggunakan Rocket Eco Stove Incinerator (REST-I) Di Kelurahan," *Solma* 13, no. 3 (2024): 2789–99, https://doi.org/10.22236/solma.v13i3.16389.

[11] Galuh Putri Riyanto and Wahyunanda Kusuma Pertiwi, "Menilik Teknologi 'Deepfake' Di Balik Video Diduga Mirip Nagita Slavina," *Kompas.Com*, 2022, https://tekno.kompas.com/read/2022/01/18/15490077/menilik-teknologi-deepfake-di-balik-video-diduga-mirip-nagita-slavina?page=all#google_vignette.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

face was digitally exchanged using artificial intelligence technology. This case is an important highlight regarding privacy violations and defamation, which occur in the context of gender-based violence.

One of the causes of the emergence of the phenomenon of deepfake pornography is the rapid advancement of technology that is actually abused by certain individuals, especially those who have knowledge in the field of digital technology.[12] They take advantage of this loophole to produce and disseminate manipulative content through social media and the dark web, which has the potential to damage the reputation and dignity of the victim.[13] In addition, the lack of public awareness about the limits of privacy in the digital world, Such as arbitrary uploads in the form of personal audio, images, and videos, also trigger data security and reputation risks. As a result, many victims experience deep psychological trauma, accompanied by the emergence of various legal issues that must be faced.

Provisions related to the use of personal data have been listed in "Law Number 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law)". Meanwhile, the pornography aspect is regulated through "Law Number 4 of 2008 concerning Pornography (Pornography Law)", and the issue of defamation is regulated in "Law Number 1 of 2024 jo. Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments (ITE Law)". Although these regulations are available, they have not been able to effectively address the new challenges posed by the development of artificial intelligence, especially in the case of deepfakes. So that Indonesia until now does not have regulations that specifically and comprehensively regulate the misuse of AI technology, including the use of deepfakes that have the potential to be ethical, legal, and socially harmful.[14]

Research on deepfakes in Indonesia shows important developments in the legal field, especially related to the implementation of the ITE Law and legal protection of victims. In this context, there are several studies that offer an in-depth analysis of these issues. Among them, research by Rangkuti et al. which emphasizes the application of the ITE Law to deal with the misuse of deepfake technology. The advantage of this research lies in its comprehensive juridical analysis and its relevance to the current legal situation in Indonesia. However, the shortcomings include a lack of discussion of the social and ethical impacts of deepfake use, which is an important aspect of understanding this phenomenon holistically.[15]

---

[12] Dewi Yanti Liliana et al., "Kajian Pemanfaatan Teknologi Artificial Intelligence Generatif Dalam Aktivitas Akademik Di Politeknik Negeri Jakarta," in *SNIV: Seminar Nasional Inovasi Vokasi*, vol. 2, 2023, 523–33.

[13] *Ibid*

[14] Renata Christa Auli, "Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya," Hukumonline.com, 2024, https://www.hukumonline.com/klinik/a/apa-itu-deepfake-porn-dan-jerat-pidana-bagi-pelakunya-lt6530d3546d9c4/.

[15] Putri Ramadhani Rangkuti et al., "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE: Studi Kasus Di Media Sosial Indonesia," *Deposisi: Jurnal Publikasi Ilmu Hukum* 3, no. 2 (2025): 111–20, https://doi.org/10.59581/deposisi.v3i2.5080.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

Furthermore, the research conducted by Bagus and Arya is titled which focuses on the formation of new legal norms in the context of pornographic content related to deepfakes, in accordance with global trends. The advantage of this study lies in the importance of introducing stricter regulations to protect individuals from exploitation as well as raising the issue of gender and vulnerability of victims, which is also a major concern in the international literature related to deepfake pornography. However, one glaring drawback is that the study may not consider technological solutions that can be used to detect and prevent the spread of deepfake-based pornographic content, which is increasingly algorithmically developed.[16]

Then Syahputra's research focuses on victim protection, in line with the literature that highlights the psychological, social, and economic impact of deepfakes on individuals. This research has the advantage of proposing the use of AI for legal protection, which is relevant to global trends in the development of deepfake detection and mitigation technologies. However, it has its drawbacks in terms of the challenges of implementing AI in the Indonesian legal system in detail, even though the literature highlights the limitations of current deepfake detection technology. In addition, related to its focus on the criminal aspect, it can ignore non-legal protections (e.g., education, psychological recovery) which are also important according to the literature.[17]

Of the three studies, none have comprehensively highlighted the urgency of regulating deepfake pornography through a comparative approach to laws between countries, which is the main focus of this study. In fact, this approach is important to explore and analyze how other countries have responded to the emergence of deepfake technology, both in terms of regulations, victim protection, and law enforcement, so that it can be used as a reference material in formulating legal policies in Indonesia. The absence of this regulation causes legal uncertainty and weak protection for victims. In this context, the state should be present to ensure the digital security of its citizens, especially considering that Indonesia is a country of law that upholds the principles of certainty, justice, and human rights protection.[18]

Clear regulation of artificial intelligence and all forms of criminal acts arising from the use of this technology, especially in the case of deepfake crimes, is an urgent need. The existing legal vacuum causes law enforcement to experience difficulties in conducting legal processes effectively. This condition is exacerbated by the enactment of the principle of legality which is a

[16] Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "Urgensi Pengaturan Tindak Pidana Deepfake Pornografi Di Indonesia," *Jurnal Kertha Wicara* 13, no. 10 (2024): 530–41, https://doi.org/10.1016/j.cviu.2022.103525.1.

[17] Rendi Syaputra Nur Haida and Eko Nuriyatman, "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia," *Jurnal Hukum Respublica* 24, no. 01 (2024): 5–12, https://doi.org/10.31849/respublica.v24i01.23327.

[18] Neneng Anjarwati, Sri Jaya Lesmana, and Tiara Ayu Lestari, "Analisis Yuridis Tentang Perlindungan Hukum Terhadap Anak Jalanan Di Kabupaten Tangerang," *Jurnal Crepido* 05, no. 02 (2023): 161–73, https://doi.org/10.14710/crepido.5.2.161-173.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

fundamental pillar in the Indonesian criminal law system.[19] Thus, the urgency and purpose of this research is not only to identify existing legal gaps, but also to provide comparative-based regulatory recommendations in order to create a legal protection system that is adaptive, progressive, and responsive to the development of digital technology, especially in dealing with the crime of deepfake pornography.

## 2. METHOD

This study uses a normative legal research method with a descriptive nature. The normative or doctrinal approach is used to examine legal principles, norms, theories, and doctrines that are relevant in identifying and solving legal problems, including norm gaps, rule conflicts, and regulatory ambiguities.[20] This method was chosen because the issues studied are directly related to positive legal norms and the need to reconstruct legal policies against the phenomenon of deepfake pornography. This research applies several approaches, namely the legislative approach, the conceptual approach, and the comparative approach.[21]

The collection of legal materials is carried out through literature studies, which include primary legal materials in the form of relevant laws and regulations, such as the ITE Law, the Pornography Law, and the Personal Data Protection Law. In addition, secondary legal materials consist of legal literature, scientific journals, previous research results, and international academic articles that discuss arrangements related to deepfake pornography. Meanwhile, tertiary legal materials include legal dictionaries and digital legal encyclopedias, which are used to strengthen the understanding of legal terms and concepts relevant to this research.

## 3. RESULTS AND DISCUSSION

### 3.1 Weaknesses of Applicable Laws and Privacy Vulnerabilities Due to Deepfake Pornography

As social beings, humans live in a legal order that functions to maintain order, justice, and balance in society.[22] The establishment of laws is an important instrument to overcome various forms of crime,[23] especially when faced with new challenges born from the advancement of digital technology. One of these contemporary challenges is the misuse of artificial intelligence

[19] Chiquita Thefirstly Noerman and Aji Lukman Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara; Criminalization of Deepfake in Indonesia as a Form of State Protection," *USM Law Review* 7, no. 2 (2024): 1–4, https://doi.org/10.26623/julr.v7i2.8995.

[20] Yati Nurhayati, Ifrani Ifrani, and M. Yasir Said, "Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum," *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20, https://doi.org/10.51749/jphi.v2i1.14.

[21] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2017).

[22] Sri Jaya Lesmana, "Kajian Yuridis Atas Pelaksanaan Pengawasan Terhadap Jabatan Notaris Menurut Undang-Undang Nomor 2 Tahun 2014 Di Kota Tangerang," *Supremasi Hukum* 15, no. 1 (2019): 32–39, https://doi.org/10.33592/jsh.v15i1.244.

[23] Amelia Noviana Tiessa, Sri Jaya Lesmana, and Ratna Indayatun, "Analisis Efektivitas Electronic Traffic Law Enforcement (ETLE) Dalam Sistem Penegakan Hukum Di Kabupaten Tangerang," *SOSCIED: Journal Social, Science, and Education* 8, no. 1 (2025): 1–11, https://doi.org/10.32531/jsoscied.v8i1.829.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

technology, such as deepfakes, which manipulate images, sounds, or videos to appear real.[24] Although it was originally developed for positive purposes such as film, education, or research, nowadays, deepfake technology is often misused to create fake sexual content (deepfake porn)[25] that attacks the privacy and dignity of individuals, especially women. The ease of access to personal data and images in cyberspace further increases the risk of misuse of this technology, making it a tool for exploitation, extortion, and defamation against vulnerable groups.

In the legal context in Indonesia, the abuse of deepfakes shows that there is a gap between the rapid innovation of AI technology and the slow adaptation of the law.[26] A reactive legal system is unable to keep up with the pace of technological change, thus creating a legal vacuum that has the potential to be used by perpetrators to commit crimes without being effectively prosecuted. As a result, the protection of individual rights,[27] such as the right to digital privacy, the security of personal data, and the dignity and honor of a person, becomes weak. In the absence of an explicit rule of law, law enforcement officials face difficulties in determining the right legal basis to ensnare perpetrators, because the act of deepfake pornography has not been expressly qualified as a criminal offense under the applicable law.[28]

The regulatory weaknesses related to the phenomenon of deepfake pornography can be analyzed using the theoretical framework of the legal system, Lawrence M. Friedman, which consists of three main elements, namely the substance of the law, the legal structure, and the legal culture. In terms of legal substance, Indonesia has not yet had a regulation that specifically defines and regulates deepfake pornography. Some existing laws, such as the ITE Law, the Pornography Law, and the Personal Data Protection Law, only cover a small part of these problems without reaching the technical and digital forensic aspects needed to prove deepfake crimes. As a result, there is an overlap in interpretation and difficulties in the application of sanctions against the perpetrators. In terms of legal structure, law enforcement officials such as the police, prosecutor's office, and judicial institutions still face limited technical capacity and understanding in detecting and proving artificial intelligence-based crimes. The lack of digital forensic experts and weak coordination between agencies also hampers the effectiveness of law enforcement. Meanwhile, in terms of legal culture, public awareness of the dangers of the misuse of deepfake technology is still low. Many social media users do not understand the legal and ethical consequences of digital

[24] Rebecca A Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act," *Fordham Law Review* 88, no. 3 (2019): 887–938.

[25] Kellianne Hickey, "Using Technology to Impede Privacy and Consent: A Survey of Revenge Porn Laws," *American Criminal Law Review Online* 55, no. 19 (2018): 19–22, https://www.law.georgetown.edu/american-criminal-law-review/aclr-online/volume-55/using-technology-to-impede-privacy-and-consent-a-survey-of-revenge-porn-laws/.

[26] Karolina Mania, "Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study," *Trauma, Violence, and Abuse* 25, no. 1 (2024): 117–29, https://doi.org/10.1177/15248380221143772.

[27] Sri Jaya Lesmana and Nikmatul Husna, "Analisis Yuridis Terhadap Sikap Pemerintah Kabupaten Tangerang Dalam Menyikapi Sengketa Lahan," *Supremasi Hukum* 16, no. 2 (2020): 51–57, https://doi.org/10.33592/jsh.v16i2.743.

[28] Sri Jaya Lesmana and Inas Sofia Latif, "Law Enforcement in Efforts to Combat Cyber Crime in Indonesia: Building Future Digital Security," *IJLRSA: The International Journal of Law Review and State Administration* 1, no. 3 (2023): 120–28, https://doi.org/10.58818/ijlrsa.v1i3.90.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

media, so the spread of manipulative content is often considered commonplace. This low level of digital literacy reinforces a permissive culture that allows technology abuse to continue to thrive without adequate social control.

The weaknesses in the three elements of the legal system were evident in the Nagita Slavina deepfake case, which had gone viral on social media. The manipulative video that resembles a public figure is widespread and causes an uproar, but law enforcement officials do not have a clear legal basis to ensnare the perpetrator, specifically because no rule explicitly regulates the creation and dissemination of deepfake pornographic content. Law enforcement can only be carried out with general articles related to defamation or moral violations in the ITE Law, which, in practice, do not reflect the complexity of AI-based digital crimes. This condition shows that the positive legal system in Indonesia is not adaptive to the dynamics of modern technology. Therefore, special regulations are needed that expressly regulate the prevention and enforcement of deepfake pornography. The regulation should include a clear definition of deepfakes, digital forensics-based proof mechanisms, proportionate criminal sanction provisions, and protection and recovery mechanisms for victims. In addition, collaboration between the government, law enforcement officials, digital platforms, and civil society is essential to strengthen digital ethics and create a legal system that is adaptive and responsive to technological advances.

### 3.1.1 Deepfake Pornography in the Perspective of the ITE Law

Until now, Indonesia has not had a specific regulation that explicitly regulates the use of AI technology. However, AI technology has similar characteristics to "electronic agents" as referred to in the ITE Law and its amendments. Based on "Article 1 number 8 of Law Number 19 of 2016", an electronic agent is defined as part of an electronic system designed to automatically perform actions on certain electronic information and run by individuals. The ability to perform functions automatically is what causes the term "automatic" to often be juxtaposed with the concept of AI.[29] In addition, AI can also be defined as a computing system that has the ability to think and make decisions independently. These similarities in autonomy, decision-making, and adaptive capabilities make AI comparable to electronic agents in the context of Indonesia's positive law.

In practice, the misuse of AI technology to create manipulative content such as deepfake pornography is a form of violation of the law, especially as stipulated in "Article 27 paragraph (1) of Law Number 1 of 2024". The article states that "every person intentionally and without the right broadcasts, performs, distributes, transmits, and/or makes accessible Electronic Information and/or Electronic Documents that have content that violates morality to be known to the public." In this context, the two important elements to be analyzed hermeneutically are "intentionally"

[29] Bintang M.D and Muh. Ali Masnun, "Prospek Artificial Intelligence Sebagai Quasi Subjek Hukum: Dinamika Pengaturan Hukum Perdata Di Indonesia," *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora* 4, no. 2 (2024): 1–19, https://doi.org/10.53697/iso.v4i2.2063.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

and "without rights", because both are key in determining whether an act can be categorized as a criminal act or not. In the interpretation of criminal law, the element of "intentionally" means the intention and awareness of the perpetrator to commit an act that is prohibited by law, as well as being aware of the consequences that may arise from his actions. However, in the case of deepfake pornography, this element of intentionality becomes blurred.

AI technology can be used to generate manipulative content without the user's direct involvement in the final creation process. For example, one can upload a photo of the victim to an AI-based platform, and the system automatically generates deepfake pornography videos without further intervention from the user. In the context of legal hermeneutics, this causes a shift in the meaning of intention (*mens rea*) from human intentionality to a form of technological intentionality, where algorithmic systems take over part of the function of human will. The grammatical interpretation of the word "intentionally" requires a conscious will, but a teleological interpretation requires an understanding that the purpose of criminal law is to protect the legal interests of society and the victim, not simply to punish the subjective intentions of the perpetrator. Therefore, hermeneutical interpretations can expand the meaning of "intentionally" to include actions that logically and predictably cause consequences of violating morality, even if done with the help of automated systems such as AI.

Furthermore, the element of "without rights" means that the act is carried out without permission, authorization, or a valid legal basis. In practice, deepfake pornography perpetrators do not have the right to the image, identity, or personal data of others used to create manipulative content. However, challenges arise when perpetrators argue that content is generated by automated systems, or that data (e.g., facial photos) is obtained from public spaces such as social media. In the interpretation of hermeneutics, the meaning of "without rights" must be interpreted systematically and teleologically, namely by paying attention to the protection of the right to privacy, human dignity, and the integrity of digital identities. Thus, even though the data is sourced from the public sphere, uses that lead to digital sexual exploitation are still categorized as "without rights" because they are contrary to the legal purpose of preserving the decency and honor of individuals.

In law enforcement practice, various obstacles hinder the effectiveness of the application of "Article 27 paragraph (1) of the ITE Law" to deepfake pornography cases. One of the main obstacles lies in the difficulty of the element of intentionality. Many perpetrators use artificial intelligence-based applications that work automatically, making it difficult to prove the existence of intentions or conscious intentions to create pornographic content. The perpetrator can argue that he only uploaded a photo without intending to produce immoral content, thus creating ambiguity in proving *mens rea*, which is an essential element in criminal law. In addition, there are also difficulties in proving that the perpetrators really "create" or "distribute" deepfake content. In many cases, the creators of manipulative content aren't always the same as the party

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

that first spread it. Identification of perpetrators is often hampered by the use of anonymous accounts, virtual private networks (VPNs), or platforms based abroad, so that the law enforcement process often stops at the investigation stage without concrete results.

The next obstacle is the limitation of digital forensic capabilities and AI detection technology among law enforcement officials. Not all law enforcement institutions have adequate tools, expertise, and resources to detect and prove AI-based digital manipulation. In fact, digital proof is essential to ensure the fulfillment of elements such as "broadcast", "distribute", or "make accessible". Furthermore, there is still a gap in special legal norms related to synthetic media-based crimes. The ITE Law does not explicitly recognize legal terms or categories regarding deepfakes, so its application depends on general articles that are multi-interpreted. This condition creates legal uncertainty and weakens the position of victims in obtaining justice.

From the point of view of the principle of legality and the principle of *nullum crimen sine lege certa*, namely that no act can be punished without clear legal provisions, the application of Article 27 paragraph (1) to the case of deepfake pornography becomes problematic. The elements in the article do not explicitly include the content of artificial intelligence engineering, so law enforcement officials often interpret norms extensively to reach acts that have not been strictly regulated. Although this is done to close the legal vacuum, such an approach has the potential to violate the principle of legality because it can create legal uncertainty and open up opportunities for excessive criminalization. Therefore, there is a need for legal reform that strictly regulates AI-based crimes, including deepfake pornography.

### 3.1.2 Deepfake Pornography in the Perspective of the Pornography Act

In Indonesia, regulations related to pornography are regulated in "Law Number 44 of 2008". In Article 1, pornography is defined as "any form of representation, whether in the form of images, sketches, illustrations, photographs, writings, sounds, audio, moving images, animations, cartoons, conversations, gestures, or other forms of communication through various media and/or performances in public spaces that contain obscene elements or sexual exploitation that are contrary to the norms of decency that apply in society."

One of the important provisions of this law is Article 4, which expressly "prohibits any person from producing, making, duplicating, providing, disseminating, offering, or trading pornographic material." This provision provides a strong legal basis in tackling the circulation of pornographic content, both in physical form and through digital media. Furthermore, Article 29 stipulates that violations of the provisions in Article 4 paragraph (1) "may be subject to criminal sanctions in the form of imprisonment for a minimum of six months and a maximum of twelve years, and/or a fine of at least IDR 250 million and a maximum of IDR 6 billion."

Today, advances in deepfake technology have reached the public widely, enabling the misuse of digital content with malicious motives that can damage an individual's reputation, weaken social

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

institutions, and cause negative transformations in society. Therefore, it is important to highlight the urgency of addressing a treatment that not only covers aspects of criminal law but also includes mechanisms for the rapid removal of content, the restoration of victims' good names, and the provision of comprehensive psychological support.

In the context of the development of deepfake technology, deepfake pornography creators should be seen as creators of new pornographic content, not just digital editors. This is based on the fact that deepfake technology not only makes minor modifications to existing content but also creates entirely new visual representations through data processing and algorithmic engineering based on artificial intelligence. Thus, even if the material is originally sourced from a legitimate image or video, the end result presents a synthetic reality that resembles reality, and therefore must be categorized as the "creation" of pornographic content within the legal sense.

From the perspective of material criminal law, the element of "producing" or "making" as contained in Article 4 paragraph (1) of the Pornography Law can be interpreted in a dynamic interpretation. In the digital age, the "creation" process is not always done manually by humans, but can be realized through an AI-based automated system that works on user instructions. This means that perpetrators who use deepfake technology to produce pornographic content consciously initiate the creation process, thereby fulfilling the element of intentionality and legal responsibility as content creators. This view is also in line with the doctrine of "causation in digital act", which is that a person can be held legally responsible for the consequences caused by the digital act under his control, even though most of the process is done automatically by the system.

In addition, sociologically and morally, the impact caused by deepfake pornographic content is equal to, or even more damaging than, conventional pornographic content. Deepfake victims often never pose or engage in any sexual activity, but their faces are realistically pasted onto someone else's body in an obscene context. This leads to reputational damage, psychological distress, and extreme data privacy violations. Thus, if the creator of the deepfake is only considered a "digital editor", then the law fails to represent the level of moral and social error that such actions cause. In other words, deepfakes are not simply the result of "editing," but are new engineered products that contain obscene and exploitative value, so they should be subject to the same articles as the creation of conventional pornography.

In terms of policy argument, the Pornography Law needs to be revised to accommodate the phenomenon of digital synthetic content, such as deepfakes. This law was born at a time when digital manipulation technology had not developed rapidly, so the definition is still limited to "real" content and does not include AI-based engineering. In fact, today, forms of digital pornography have transcended traditional boundaries, including simulations, animations, avatars, and synthetic media that appear to be real but are entirely algorithmically generated.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

### 3.1.3 Deepfake Pornography in the Perspective of the Personal Data Protection Act

AI is closely related to personal data, forming complex and interdependent relationships.[30] To carry out the training process and optimize its performance, AI requires large amounts of personal data sets.[31] However, the use of such personal data, particularly in the process of analysis and decision-making, raises serious concerns regarding the protection of privacy and information security. One type of personal data that receives special attention is biometric data, which is information related to the physical, physiological, or behavioral characteristics of individuals that can be used for unique identification processes. Examples include facial scans, fingerprints, retina of the eye, and DNA samples. Due to its unique and immutable nature, biometric data requires extra tight safeguards from the risk of misuse.

The faces and voices used in deepfake technology fall under the category of biometric data, which is legally classified as sensitive personal data. Biometric data represents a person's unique and irreplaceable biological and personal identity, such as facial patterns, lip shapes, voice intonation, or expression. When this data is taken, analyzed, or engineered to create false representations without permission, it directly violates the privacy rights of individuals as guaranteed in the Personal Data Protection Act. In the legal context, face and voice not only serve as a means of identification, but also as part of a person's inherent identity, so their misuse can be qualified as the processing of sensitive personal data without a legitimate legal basis.

Furthermore, the concept of data subject consent is a central element in determining whether or not the processing of personal data is lawful. Article 20 of the Personal Data Protection Law emphasizes that any form of collection, storage, utilization, or distribution of personal data must be carried out based on the explicit consent of the data subject. In the case of deepfake pornography, the creation and dissemination of content that displays a person's face or voice without consent is clearly a violation of the principle of consent, so it can be categorized as unlawful processing of personal data. This violation becomes even more severe if the content causes losses to the data subject, both morally, psychologically, and socially.

In addition to deepfakes creators, electronic system operators (PSEs) such as social media platforms, video-sharing sites, or hosting services have a legal and ethical responsibility to

[30] Arvi Erawan Palindria, Muhammad Sulthan Thufail, and Muhammad Rieval Febrian, "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia," *Spektrum Hukum* 21, no. 2 (2024): 110–21, https://doi.org/10.56444/sh.v21i2.5319.

[31] *Ibid.*

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

protect victims' personal data. Based on Article 35 of the Personal Data Protection Law, PSE is obliged to ensure that the personal data processed through its system is guaranteed to be secure, and is obliged to follow up on data deletion requests if the data is used unlawfully. In the context of deepfake victims, the role of the PSE includes: (a) promptly handling reports of breaches, including blocking or removing content that contains unauthorized processing of personal data, (b) ensuring content detection and moderation systems work proactively, using technologies such as AI forensics to recognize and prevent the spread of deepfakes, and (c) providing a redress mechanism for victims, such as the right to delete data or request the removal of content from digital platforms.

This obligation is in line with the principle of the right to be forgotten as stipulated in Article 15 of the Personal Data Protection Law. This principle gives individuals the right to request that their personal data be deleted, destroyed, or no longer publicly displayed if the data is no longer relevant, used without consent, or causes harm. In the context of deepfake pornography, the application of this principle is an important legal recovery tool for victims to regain control of their digital identity. In addition, the principle of data minimization in Article 31 of the Personal Data Protection Law emphasizes that any data collection and processing should be carried out only to the extent necessary for a particular purpose. This means that AI systems, including models used for deepfake training, should not collect or exploit excessive biometric data without relevance and a legitimate legal basis. By applying this principle, the state can prevent data misuse from the early stages of technology development.

Thus, faces and voices in deepfake technology are not just visual or audio elements, but are part of a legally protected personal identity as sensitive personal data. The use without a data subject's consent is a form of violation of the right to privacy and security of personal data, and demands accountability from electronic system operators to protect victims through the application of the principles of right to be forgotten and data minimization. This approach not only strengthens the aspect of legal protection but also upholds moral and humanitarian values in an artificial intelligence-based digital ecosystem.

### 3.2 The Importance of Digital Ethics in the Prevention of Deepfake Pornography

Digital ethics refers to a set of principles and procedures that aim to minimize the negative impact of the use of digital technologies, emphasizing the importance of safeguarding the common interest so that the technology can still be enjoyed as part of modern social life.[32] In Indonesia, arrangements that explicitly regulate digital ethics are still not comprehensively available. However, a number of provisions in the ITE Law provide a relevant normative basis. One of them is Article 28, which contains a prohibition on the dissemination of false information

[32] Happy Budyana Sari et al., "Digital Ethics and Citizenship Challenges in Cyberspace: An Overview From Perspective Morals and Laws," *Jurnal Notariil* 9, no. 1 (2024): 33–39, https://doi.org/10.22225/jn.9.1.2024.33-39.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

that harms consumers in electronic transactions, as well as the spread of hate speech based on ethnic, religious, racial, and inter-group elements (SARA).

This provision is complemented by Article 29, which prohibits the transmission of electronic information that contains threats of violence or intimidation to individuals, and Article 30 which prohibits illegal access to electronic systems or computers belonging to others, including the act of breaking into security systems to obtain information. In the context of digital ethics, there are fundamental principles that must be upheld in interacting in cyberspace, such as the responsibility[33] to convey information correctly, stay away from the spread of fake news, and include sources of information that can be accounted for.[34] In addition, digital ethics also underlines the importance of maintaining the privacy and security of user data, including reasonable data collection practices, clear consent, the use of data protection technologies, and preventive measures against privacy breaches.

Technologies such as deepfakes pose complex ethical issues because they allow a person to be manipulated into certain situations without consent, including in explicit content or manipulation in political discourse. This practice raises a moral dilemma regarding the limits of privacy in the digital age.[35] From an ethical point of view, actors involved in the production and dissemination of deepfake content have a moral responsibility to consider the social impact that may arise on the individuals and communities that are victims.[36] Although freedom of expression is a guaranteed right, it is not absolute and is limited by the rights and dignity of others.[37] Therefore, any act of spreading deepfake content should be based on ethical considerations, weighing the risk of harm that may outweigh the expected benefits.[38]

Furthermore, digital platforms and technology companies also bear ethical responsibilities to prevent the circulation of deepfake content and protect users from potential harm. To address the challenges posed by this technology, strict content moderation regulations, the use of advanced technology-based detection systems, and cross-sector collaboration between policymakers, academics, and civil society organizations are needed. The impact of deepfake abuse can be devastating to individuals, especially when fake content depicts indecent acts that can destroy reputations, social relationships, professional careers, and public trust. Unfortunately, victims of

[33] *Ibid.*
[34] Ni Putu Suci Meinarni and Ida Bagus Ary Indra Iswara, "Hoax and Its Mechanism in Indonesia," in *Advances in Social Science, Education and Humanities Research: 2nd International Conference of Communication Science Research (ICCSR 2018)*, vol. 165 (Atlantis Press, 2018), 183–86, https://doi.org/10.2991/iccsr-18.2018.39.
[35] Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 2019, 1753–1820, https://doi.org/10.15779/Z38RV0D15J.
[36] Stamatis Karnouskos, "Artificial Intelligence in Digital Media: The Era of Deepfakes," *IEEE Transactions on Technology and Society* 99 (2020): 1–10, https://doi.org/10.1109/TTS.2020.3001312.
[37] Chidera Okolie, "Artificial Intelligence-Altered Videos (Deepfakes) and Data Privacy Concerns," *Journal of International Women's Studies* 25, no. 2 (2023): 1–16, https://vc.bridgew.edu/jiws/vol25/iss2/11%0AThis.
[38] Mekhail Mustak et al., "Deepfakes: Deceptions, Mitigations, and Opportunities," *Journal of Business Research* 154, no. 2 (2023): 1–33, https://doi.org/10.1016/j.jbusres.2022.113368.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

this practice often do not have adequate legal avenues to obtain justice, as existing regulations do not specifically address the harm caused by synthetic media such as deepfakes.

Digital ethics play an important role in maintaining a balance between freedom of expression and moral responsibility in the use of technology. In the context of Human Rights (HAM) in cyberspace, the principles of digital ethics are directly related to the concept of privacy, the concept of good reputation, the concept of security, and the right to be free from treatment that degrades human dignity as guaranteed in Articles 28G and 28I of the 1945 Constitution, as well as the Universal Declaration of Human Rights (DUHAM) Article 12 which affirms that "no one shall arbitrarily interfere with his or her private life." The misuse of deepfake technology, especially in the context of pornography, clearly violates these rights. Manipulating a person's face into explicit content without consent not only harms privacy but is also a form of digital violence that can cause psychological trauma and social harm to victims. From a human rights perspective, this act ignores the basic principles of non-maleficence (not harming others) and autonomy (the individual's right to self-control and his or her personal image).

The absence of specific regulations governing synthetic media, such as deepfakes, also has implications for weak legal protection for victims. The State, as the main guarantor of the fulfillment of human rights, has an obligation to protect citizens from rights violations caused by technological advances, including in the digital space. Therefore, strengthening the digital ethical aspect in regulations is important so that it not only takes action against the perpetrators, but also creates a fair and sustainable prevention system. Digital ethics must be used as the main foundation in the formation of new laws in the era of artificial intelligence. Laws built without an ethical basis will only be reactive and incapable of keeping up with rapid technological developments. By using digital ethics as a basis, Indonesia can form an adaptive, fair, and oriented legal framework for the protection of human dignity in cyberspace, so that digital transformation remains in line with human values and human rights principles.

### 3.3 The Urgency of Regulation Against Deepfake Pornography

The emergence of deepfake technology in the era of digital disruption and rapid technological advances has created complex challenges to the authenticity and integrity of digital content. This technology, which is capable of manipulating audio and visuals with great convincingness, makes it difficult to maintain the accuracy of information and protect the privacy of individuals in an ever-evolving cyber ecosystem. Therefore, a proactive response, a dynamic mitigation strategy, and an in-depth examination of the ethical implications and their impact on digital security are needed. Deepfake content often exploits a person's likeness without permission, potentially violating privacy rights and causing long-term social harm. The impact of the use of this technology extends to various fields, such as law, intellectual property, and the business

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

world. Therefore, the creation and impact of technologies such as deepfakes need serious attention and consideration in the realm of law and policy.[39]

Several countries have responded to this threat through regulations. In California, United States, AB 602 was enacted. This rule prohibits the creation and dissemination of sexually explicit material that is digitized without the consent of the individual depicted.[40] If a person creates or disseminates such material with the knowledge or strong suspicion that the individual in the content did not give consent, then that individual has the right to sue civilly. Minors cannot legally consent to the creation or distribution of digitally manipulated sexual material. Sanctions for perpetrators can include the return of profits, compensation for material and non-material losses such as psychological distress, and statutory damages ranging from $1,500 to $30,000. If bad faith is proven, statutory damages can increase to $150,000. On the other hand, public prosecutors can demand fines of up to $25,000 for each violation, or $50,000 if done in bad faith.

Meanwhile, South Korea has also regulated deepfake pornography through several legal provisions. Article 14 of the Personal Information Protection Act prohibits the creation and dissemination of images or videos that resemble a person without permission. In addition, Article 13 of the Special Law on Sexual Crimes establishes a prohibition against the distribution of manipulative sexual content that resembles real individuals. The punishment for this offense is aggravated to a maximum of 7 years in prison, both for the perpetrators of its manufacture and distribution, regardless of the intention of distribution. In fact, actions such as buying, storing, or displaying such materials can be subject to imprisonment for up to 3 years or a fine of KRW 30 million.

When compared to other countries, Indonesia still faces regulatory limitations in handling deepfake pornography cases. In "Law Number 1 of 2024", especially Article 27 paragraph (1), it is stated, "Everyone deliberately and without the right to broadcast, perform, distribute, transmit, and/or make accessible Electronic Information and/or Electronic Documents that have content that violates morality to be known to the public." However, this provision does not expressly mention the practice of digital manipulation or technology such as deepfakes. As a result, law enforcement officials are faced with an interpretive challenge: can the dissemination of sexual deepfake content be categorized as an act of "making accessible electronic information that is content to violate morality"? While this interpretation is possible, the absence of explicit regulation on digital manipulation has the potential to create legal uncertainty and weaken the applicability of the article in practice.

[39] Anuragini Shirish and Shobana Komal, "A Socio-Legal Inquiry on Deepfakes," *California Western International Law Journal* 54, no. 2 (2024): 517–60, https://scholarlycommons.law.cwsl.edu/cwilj/vol54/iss2/6.

[40] Legislative Council Bureau, "Assembly Bill No. 602" (2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

In addition, Article 29 of the Pornography Law states "Every person who produces, makes, reproduces, duplicates, disseminates, broadcasts, imports, exports, offers, sells, rents, or provides pornography as referred to in Article 4 paragraph (1) shall be sentenced to imprisonment for a minimum of 6 (six) months and a maximum of 12 (twelve) years and/or a fine of at least Rp250,000,000.00 and a maximum of Rp6,000,000,000, 00. Although this article covers the act of producing and distributing pornographic content, the regulation does not explicitly anticipate the emergence of new production methods such as deepfakes. The next thing that becomes problematic is whether digital manipulation, for example, attaching one's face to another person's body in a sexual scene, can be categorized as the act of "creating" or "producing" new pornographic content, or simply being considered a modification of existing content.

The definition of pornography in the law, which includes sexually charged images, sounds, or writings, is quite general. This creates a legal loophole because it does not specifically cover manipulative technologies such as deepfakes, which in practice often target individuals without their consent and cause serious psychological and social repercussions. In the context of deepfakes, proving the element of intentionality in the process of creating and disseminating pornographic content is a challenge in itself. The perpetrator may argue that they are not directly "producing" pornographic content in the conventional sense, but only manipulating or editing pre-existing material. Such arguments can complicate the application of legal provisions that require the element of manufacture or production in the case of pornography.

Furthermore, the perpetrator's motive in disseminating deepfake pornography is not always related to financial gain. In Article 66 of the Personal Data Protection Law, it is stated that "Everyone is prohibited from making false Personal Data or falsifying Personal Data with the intention of benefiting themselves or others that may result in losses to others." Although this article contains a prohibition against falsification of personal data, it does not explicitly cover the use of manipulative technologies such as deepfakes. In fact, deepfakes are a very complex form of personal data engineering, usually in the form of visual images or individual voices. Therefore, law enforcement against deepfake practices requires a more progressive interpretation of the law in order to include digital manipulation in the category of "falsification of personal data".

On the other hand, perpetrators of the dissemination of deepfake pornographic content often act anonymously through digital platforms, thus complicating the identification and prosecution process, even though there is a criminal legal basis. In addition, the motivation for creating this kind of content is not always economic. Many cases indicate that the goal is harassment, revenge, spreading hatred, or sheer personal gratification. This poses a particular challenge in proving the element of "self-benefit or others," especially when the benefits are non-material or psychological, which are not easily quantified within the existing legal framework.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

Based on the comparison between the United States (California) and South Korea, it can be concluded that both countries have adopted a proactive legal approach in responding to the phenomenon of deepfake pornography. This approach not only focuses on the criminal aspect of the perpetrator, but also provides space for victim protection through compensation, content removal, and reputation restoration mechanisms. On the other hand, Indonesia still relies on the general provisions in the ITE Law, the Pornography Law, and the Personal Data Protection Law, which are reactive and fragmentary. The following comparison shows the differences in legal structure and the relevance of its adaptation for Indonesia:

**Table 1.** Comparison of Deepfake Regulations Between California, South Korea, and Indonesia

| Regulation Aspects | California (AB 602) | South Korea (Specific Laws on Sexual Crimes & PIPA) | Indonesia (ITE Law, Pornography Law, Personal Data Protection Law) | Adaptation Recommendations for Indonesia |
|---|---|---|---|---|
| Definition Scope | Prohibit the creation and dissemination of digital sexual content without the individual's permission | Prohibits the creation and distribution of manipulative images that resemble real individuals without permission | There is no explicit definition of deepfake; it only refers to "moral content" or "falsification of personal data" | Add a definition of "synthetic content" or "AI-based digital engineering" in the ITE Act or the Pornography Act |
| Consent Aspect | There must be explicit permission from the individual depicted | It is strictly forbidden to create or distribute content without the written permission of the subject | It has not explicitly emphasized consent in the digital visual context | It needs to be made clear that the use of a person's image or voice without consent is a violation of the law |
| Sanctions and Compensation | Statute damages of up to $150,000 and civil lawsuits for victims | Criminal punishment of up to 7 years in prison; fine KRW 30 million | The maximum penalty is 12 years (Pornography Law), but it is not specific to digital manipulation | Establish specific penalties for deepfake pornography, with the option of financial compensation and psychological |

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

| | | | | |
|---|---|---|---|---|
| | | | | recovery for the victim |
| Victim Protection | Right to sue, compensation, and removal of content | Personal data protection and strict prohibition of victim re-identification | The right to be forgotten (PDP Law), but it has not been implemented effectively | There needs to be a mechanism for digital reputation restoration and the right to be forgotten automatically for victims |
| Policy Approach | The law is based on the protection of victims' rights | Laws based on the prevention and protection of biometric data | The law is based on moral prohibitions, not on the context of technology | Legal reformulation based on digital ethics and digital human rights |

*Source: **Results processed by researchers**, 2025.*

As shown in Table 1. Comparison of Deepfake Regulations Between California, South Korea, and Indonesia: California and South Korea have established explicit legal frameworks addressing deepfake pornography, including clear definitions, consent requirements, sanctions, and victim protection mechanisms. In contrast, Indonesia still relies on general provisions that do not specifically regulate AI-generated synthetic content, leading to legal uncertainty and weaker protections for victims. This comparison highlights the urgent need for Indonesia to develop specific and adaptive regulations that incorporate clear definitions, consent-based protection, and comprehensive legal remedies for victims.

In the context of victim protection, this study adopts a victim-centered justice mechanism that places victims at the center of legal protection by providing the right to psychological recovery, privacy protection, and the implementation of an automated takedown system by the Electronic System Operator (PSE). Meanwhile, from the aspect of legal reform, the adaptive legal governance approach is proposed as a strategy so that legal norms can be updated periodically in line with the development of artificial intelligence technology and the dynamics of global digital trends. Thus, this research is not only analytical but also normative-prescriptive, as it offers a new legal model design that adapts to Indonesia's needs in dealing with legal threats and risks posed by deepfake technology.

In the policy direction, this research emphasizes the need for progressive steps for Indonesia in formulating new legal norms. First, it is necessary to establish a *lex specialis* on AI-based digital crime, which is a derivative law or regulation that expressly regulates the creation, dissemination, and possession of synthetic content that resembles unauthorized individuals, complete with elements of intentionality, perpetrator responsibility, and specific technological

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

definitions. Second, it is necessary to strengthen the principle of informed consent in the Personal Data Protection Law (PDP Law) and the Pornography Law, which require any use of a person's image, voice, or biometric data to obtain explicit and documented consent. PSE is also obliged to provide a mechanism for withdrawal of consent and automated data erasure to protect individual privacy rights.

Third, it is recommended to revise the Pornography Law and the ITE Law by including a new category of "synthetic sexual content" created using AI technology, and emphasizing that the creation of deepfakes without permission is a form of creation of new pornographic content that has a legal impact. Fourth, it is important to apply the principles of digital ethics and human rights in cyberspace, where the law must be based on respect for digital human dignity, including the right to privacy, integrity of self-image, and freedom from exploitation. For this reason, PSE needs to develop an AI Ethics Compliance system that functions to prevent the spread of manipulative content based on artificial intelligence.

Fifth, it is necessary to carry out multi-sector collaboration and increase digital ethical literacy through synergy between the government, academics, digital platforms, and civil society to build a culture of privacy-awareness, anti-exploitation, and digital responsibility. Legal literacy and digital ethics also need to be integrated into the national education curriculum and public education programs as a long-term prevention effort.

Reflectively, in this era of digital disruption, the speed of technological development must be balanced with the speed of legal adaptation. The establishment of regulations regarding deepfake pornography is not only a technical necessity but also a moral and normative responsibility to maintain human dignity in the digital space. Indonesia can take inspiration from the legal practices of other countries, but adjustments to Pancasila values, moral norms, and human rights principles must be the main basis so that the laws born are not only repressive, but also restorative, ethical, and humane.

In addition, digital community awareness needs to be built as part of technological ethics. Every individual must understand the impact of using technology on their lives, including the potential risks it poses.[41] In the context of digital citizenship, respect for freedom of opinion must be accompanied by a responsibility not to harass, insult, or spread hate speech. A culture of healthy dialogue and mutual respect for differences of views must continue to be developed in order to create a safe and inclusive digital space for all.[42]

### 3.4 Ideal Policy Against Deepfake Pornography Prevention In the Context of Digital Privacy and Ethics Protection

[41] Hera Alvina et al., "The State of Digital Freedom in Indonesia an Assessment of Online Censorship, Privacy, and Free Expression," *Journal of Digital Law and Policy* 1, no. 3 (2022): 141–52, https://doi.org/10.58982/jdlp.v1i3.301.
[42] *Ibid.*

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

The ethical dilemma posed by deepfake technology demands a balance between innovation and moral responsibility.[43] On the one hand, deepfakes have great potential in the arts, education, and entertainment, but on the other hand, their abuse causes serious social and psychological harm.[44] It is in this context that the formation of firm and comprehensive regulations is a national urgency. The speed of technological development has far exceeded the readiness of positive laws, causing a vacuum of norms that endanger the rights of individuals,[45] particularly in the case of deepfake pornography. To close these legal loopholes, Indonesia needs a regulatory framework that is not only reactive, but proactive and adaptive, in line with the moral, humanitarian, and rule of law values that exist in society.

The conceptual-progressive approach put forward by Satjipto Rahardjo emphasizes that the law must place humans as the center of orientation. In this framework, regulations on deepfakes should not stop at the legal text, but should be an instrument to protect human dignity and integrity. Law is not just a normative tool, but a "living law" that develops according to social needs. Therefore, the draft deepfake regulation should affirm the protection of individual privacy, honor, and freedom as the primary values that the state upholds. This principle places law as a means of upholding "substantive justice", not just procedural justice.

Although the current criminal law has been able to regulate a number of forms of fraud or violations of individual rights, the existence of a special law that specifically addresses the problem of deepfakes is very important, given the rapid development of digital technology and artificial intelligence. This regulation needs to contain a clear and detailed definition of deepfake, so that it can be distinguished from other forms of digital manipulation that also use artificial intelligence technology. Individuals or parties who produce or disseminate deepfake content with the aim of harming others must be held legally accountable, both criminally and civilly.

To deal with security threats arising from artificial intelligence-based deepfake technology, six important elements need to be applied in an integrated manner.[46] First, regulatory compliance, which is the importance of following official rules, standards, and guidelines set by the competent authorities, so that the development and use of AI is safe and responsible. Second, ethical governance of artificial intelligence, which emphasizes the establishment of a transparent and accountable internal oversight system to ensure that the use of AI is in line with moral values

[43] Mustafa Kaan Tuysuz and Ahmet Kılıç, "Analyzing the Legal and Ethical Considerations of Deepfake Technology," *Interdisciplinary Studies in Society, Law, and Politics* 2, no. 2 (2023): 4–10, https://doi.org/10.61838/kman.isslp.2.2.2.

[44] Nik Hynek, Beata Gavurova, and Matus Kubak, "Risks and Benefits of Artificial Intelligence Deepfakes: Systematic Review and Comparison of Public Attitudes in Seven European Countries," *Journal of Innovation and Knowledge* 10, no. 5 (2025): 1–19, https://doi.org/10.1016/j.jik.2025.100782.

[45] Furizal et al., "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review," *Social Sciences and Humanities Open* 12, no. January (2025): 1–25, https://doi.org/10.1016/j.ssaho.2025.101882.

[46] Dimitar Trombevski, "Deepfakes and the Future of AI Legislation: Overcoming the Ethical and Legal Challenges," GDPR Local, 2025, https://gdprlocal.com/deepfakes-and-the-future-of-ai-legislation-overcoming-the-ethical-and-legal-challenges/.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

and social responsibility. Third, risk management, which is an effort to identify, analyze, and anticipate potential risks from the use of AI, such as the spread of disinformation, identity theft, and digital harassment, through effective mitigation strategies.

Fourth, technology investment is needed to strengthen AI-based deepfake detection capabilities as a preventive measure against the misuse of manipulated digital content. Fifth, public awareness and education, because the public needs to be equipped with an understanding of how digital technology works, the potential risks of deepfakes, and the ability to verify the truth of information in order to protect themselves from digital manipulation. Sixth, cross-border collaboration, considering that the spread and abuse of AI is transnational, cooperation between countries through information exchange, the establishment of joint monitoring mechanisms, and the establishment of global standards are urgently needed. With the application of these six elements, countering deepfakes can be carried out comprehensively through synergy between global law, technology, and ethics.

In order for regulations on deepfake pornography to be effective and comprehensive, the draft regulation needs to be drafted in the form of laws or government regulations with a systematic structure and based on strong legal principles. Chapter I – General Provisions contains clear legal definitions regarding deepfakes, synthetic media, non-consensual sexual content, and biometric data. The clarity of this terminology is important to prevent multiple interpretations and provide a firm basis for legal behavior. Chapter II – Principles and Objectives governs basic principles such as *lex specialis*, informed consent, protection of digital human dignity, technological accountability, and the public interest. The main objective of this chapter is to protect citizens from misuse of technology that can damage the reputation as well as the privacy of individuals.

Furthermore, Chapter III – Responsibilities and Obligations of Perpetrators and Electronic System Operators (PSE) emphasizes that creators, spreaders, or parties who use deepfakes with harmful intent must be held criminally and civilly accountable. PSEs are also required to implement automated detection & takedown systems, AI Ethics Compliance policies, and fast and transparent content reporting mechanisms. Chapter IV – Victim Protection and Restoration of Rights guarantees the victim's right to psychological recovery, the right to be forgotten, and compensation for the losses incurred. This chapter also accommodates the provisions of restorative justice that focus on restoring the dignity and welfare of victims.

Then, Chapter V – Technology Governance and Ethical Supervision regulates the mechanism for permitting the use of deepfake technology for legitimate purposes such as art, research, and education. This chapter also includes the establishment of a National AI Ethics Council that functions to conduct ethical and technical audits of artificial intelligence algorithms. Chapter VI – Criminal Provisions and Sanctions stipulate strict penalties for perpetrators of creating, distributing, and possessing non-consensual deepfake content, adjusted to the victim's level of loss. In addition, digital platforms that neglect to prevent the spread of illegal content can also be

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

held accountable by corporations. Chapter VI – Closing and Evaluation Provisions contains a mechanism for periodically updating legal norms (adaptive governance) so that regulations remain relevant to technological developments.

In this context, the principle of "internal morality of law" put forward by Lon L. Fuller can be used as an indicator of ideal legal policy. Fuller asserts that good law must have internal morality to be obeyed and enforced fairly. These principles include clarity of norms, transparency, consistency between regulations, legal stability, and the application of proportionate sanctions. The clarity of terms such as deepfakes, biometrics, and synthetic content should be explicitly spelled out so as not to create ambiguity. States such as California and South Korea have shown efforts that are consistent with the Fuller principle by establishing clear definitions of consent and legal accountability. For example, California law strictly defines "digital sexually explicit material" and mandatory consent, while South Korean law prohibits the creation or dissemination of images without permission, which strengthens protections for individual rights.

Regulations must also be transparent and easy for the public to understand through digital socialization and legal education, as well as harmonious with the ITE Law, the Pornography Law, and the Personal Data Protection Law to prevent overlapping norms. If a wedge occurs, it must be determined which one has more specific legal force. This consistency is important so that the legal system remains integrated and does not cause confusion.[47] In addition to formulating norms, policies must also include concrete implementation plans, including increasing the capacity of law enforcement in detecting and handling deepfake cases. Regulations should not just be rules on paper; their success is judged by the extent to which they can be implemented effectively in the field. Evaluation of deepfake technology to be used in Indonesia must be carried out comprehensively,[48] including an assessment of algorithms, training data, and ethical considerations. The development of technology licensing mechanisms is also important. Permits are only granted when the technology meets the previously established ethical, technical, and legal criteria.

By fulfilling these principles, regulations on deepfakes will reflect laws that are "moral from within, laws that are obeyed not because of coercion, but because they are considered fair, rational, and relevant to the values of modern digital society.[49] In the context of digital ethics, respect for individual rights, particularly regarding the control of sexual imagery and representation, is a key principle.[50] Digital ethics must support the values of consent,

[47] Sri Jaya Lesmana and Inas Sofia Latif, *Pengantar Ilmu Hukum (Inleiding Tot De Rechtwetenschap)* (Tangerang Selatan: Berkah Aksara Cipta Karya, 2024).

[48] Sri Jaya Lesmana et al., "Evaluating Surveillance Measures at Airports in Responding to Airline Negligence and Lost Baggage," *Media of Law and Sharia* 6, no. 3 (2025): 228–47, https://doi.org/10.18196/mls.v6i3.368.

[49] Anetta Jedličková, "Ethical Approaches in Designing Autonomous and Intelligent Systems: A Comprehensive Survey towards Responsible Development," *AI and Society* 40, no. 4 (2025): 2703–16, https://doi.org/10.1007/s00146-024-02040-9.

[50] Luciano Floridi, *The Ethics of Information* (Croydon: Oxford University Press, 2014), https://doi.org/10.1093/acprof:oso/9780199641321.001.0001.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

responsibility, and the prevention of negative impacts. Tackling deepfake pornography must involve a cross-sectoral approach that brings together legal regulations, digital platform policies, and improving public literacy. Digital platforms need to tighten content moderation policies, while policymakers need to criminalize the creation and distribution of deepfake content that does not get the consent of its subjects.[51]

In the end, the establishment of regulations regarding deepfake pornography is not just a legal project, but a moral duty of the state to protect human dignity in the digital space.[52] The state must not be passive towards the misuse of technology that threatens the personal integrity of its citizens. The law must be a reflection of human values, side with the victim, protect the weak, and uphold substantive justice. By building a progressive, consistent, and ethical legal framework, Indonesia not only responds to the threat of deepfakes, but also establishes itself as a legal state that upholds digital human dignity in the era of artificial intelligence.

## 4. CONCLUSION

Deepfake pornography technology poses a serious threat to the privacy, dignity, and psychological condition of victims, especially women, with impacts including reputational damage, emotional trauma, and repeated harassment. Although Indonesia already has a number of regulations such as the ITE Law, the Pornography Law, and the Personal Data Protection Law, all three have not specifically regulated or defined deepfake pornography. This study integrates the dimensions of positive law, digital ethics, and international comparisons to build a legal protection model against deepfake pornography, a perspective that is rarely studied in the Indonesian legal literature. An ideal legal policy in regulating deepfake pornography at least includes a clear definition of deepfake content, regulating basic principles such as *lex specialis*, informed consent, protection of digital human dignity, technological accountability, and the public interest, regulating the responsibilities and obligations of perpetrators and PSEs, containing governance and supervision, providing protection and compensation mechanisms for victims, and establishing adequate sanctions for perpetrators. Based on these findings, it is recommended that the government immediately establish special regulations on AI-based crimes based on the principles of human dignity and digital accountability, strengthening digital privacy literacy, and cross-agency collaboration in law enforcement.

## REFERENCES

Afshari, Narges, and Ahmad Mohammadi. “The Legal Implications of Deepfake Technology: Privacy, Defamation, and the Challenge of Regulating Synthetic Media.” *Legal Studies in Digital Age* 2, no. 2 (2020): 13–23. https://jlsda.com/index.php/lsda/article/view/13.

[51] Narges Afshari and Ahmad Mohammadi, “The Legal Implications of Deepfake Technology: Privacy, Defamation, and the Challenge of Regulating Synthetic Media,” *Legal Studies in Digital Age* 2, no. 2 (2020): 13–23, https://jlsda.com/index.php/lsda/article/view/13.

[52] Sri Jaya Lesmana and Muhammad Mpu Samudra, “Legal Protection of Gig Economy Workers: A Comparative Study in Indonesia , Malaysia , and Singapore,” *SASI* 31, no. 3 (2025): 201–18, https://doi.org/10.47268/sasi.v31i3.3006.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. "The State of Deepfakes: Landscape, Threats, and Impact," 2019. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

Alvina, Hera, Lis Julianti, Anak Agung Putu Wiwik Sugiantari, and I Wayan Wahyu Wira Udytama. "The State of Digital Freedom in Indonesia an Assessment of Online Censorship, Privacy, and Free Expression." *Journal of Digital Law and Policy* 1, no. 3 (2022): 141–52. https://doi.org/10.58982/jdlp.v1i3.301.

Anjarwati, Neneng, Sri Jaya Lesmana, and Tiara Ayu Lestari. "Analisis Yuridis Tentang Perlindungan Hukum Terhadap Anak Jalanan Di Kabupaten Tangerang." *Jurnal Crepido* 05, no. 02 (2023): 161–73. https://doi.org/10.14710/crepido.5.2.161-173.

Auli, Renata Christa. "Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya." Hukumonline.com, 2024. https://www.hukumonline.com/klinik/a/apa-itu-deepfake-porn-dan-jerat-pidana-bagi-pelakunya-lt6530d3546d9c4/.

Biro Hukum dan Humas KemenPPPA. "Gandeng Sejumlah Pihak, Kemen PPPA Dorong Aksi Bersama Lindungi Perempuan Dan Anak Dari Kekerasan Di Ranah Daring." KemenPPPA, 2024. https://kemenpppa.go.id/siaran-pers/gandeng-sejumlah-pihak-kemen-pppa-dorong-aksi-bersama-lindungi-perempuan-dan-anak-dari-kekerasan-di-ranah-daring.

Chesney, Bobby, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 2019, 1753–1820. https://doi.org/10.15779/Z38RV0D15J.

Delfino, Rebecca A. "Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act." *Fordham Law Review* 88, no. 3 (2019): 887–938.

Floridi, Luciano. *The Ethics of Information*. Croydon: Oxford University Press, 2014. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001.

Furizal, Alfian Ma'arif, Hari Maghfiroh, Iswanto Suwarno, Denis Prayogi, Kariyamin, Syahrani Lonang, and Abdel Nasser Sharkawy. "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review." *Social Sciences and Humanities Open* 12, no. January (2025): 1–25. https://doi.org/10.1016/j.ssaho.2025.101882.

Haida, Rendi Syaputra Nur, and Eko Nuriyatman. "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (AI) Dari Perspektif Hukum Pidana Indonesia." *Jurnal Hukum Respublica* 24, no. 01 (2024): 5–12. https://doi.org/10.31849/respublica.v24i01.23327.

Hailtik, Asri Gresmelian Eurike, and Wiwik Afifah. "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia." *Asian Journal of Social and Humanities* 2, no. 4 (2024): 776–95. https://doi.org/10.59888/ajosh.v2i4.222.

Hickey, Kellianne. "Using Technology to Impede Privacy and Consent: A Survey of Revenge Porn Laws." *American Criminal Law Review Online* 55, no. 19 (2018): 19–22. https://www.law.georgetown.edu/american-criminal-law-review/aclr-online/volume-55/using-technology-to-impede-privacy-and-consent-a-survey-of-revenge-porn-laws/.

Hynek, Nik, Beata Gavurova, and Matus Kubak. "Risks and Benefits of Artificial Intelligence Deepfakes: Systematic Review and Comparison of Public Attitudes in Seven European Countries." *Journal of Innovation and Knowledge* 10, no. 5 (2025): 1–19. https://doi.org/10.1016/j.jik.2025.100782.

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

Jedličková, Anetta. "Ethical Approaches in Designing Autonomous and Intelligent Systems: A Comprehensive Survey towards Responsible Development." *AI and Society* 40, no. 4 (2025): 2703–16. https://doi.org/10.1007/s00146-024-02040-9.

Kaan Tuysuz, Mustafa, and Ahmet Kılıç. "Analyzing the Legal and Ethical Considerations of Deepfake Technology." *Interdisciplinary Studies in Society, Law, and Politics* 2, no. 2 (2023): 4–10. https://doi.org/10.61838/kman.isslp.2.2.2.

Karnouskos, Stamatis. "Artificial Intelligence in Digital Media: The Era of Deepfakes." *IEEE Transactions on Technology and Society* 99 (2020): 1–10. https://doi.org/10.1109/TTS.2020.3001312.

Komnas Perempuan. "Siaran Pers Gerak Bersama Dalam Data: Laporan Sinergi Database Kekerasan Terhadap Perempuan Tahun 2023." Komnas Perempuan, 2024. https://komnasperempuan.go.id/siaran-pers-detail/siaran-pers-gerak-bersama-dalam-data-laporan-sinergi-database-kekerasan-terhadap-perempuan-tahun-2023.

Latif, Inas Sofia, Hudaya Latuconsina, and Sri Jaya Lesmana. "Digitalisasi UMKM Di Kelurahan Selapajang Jaya: Strategi Social Media Marketing Dalam Menyongsong Era Modern (Digitalization of MSMEs in Selapajang Jaya Village: Social Media Marketing Strategy in Welcoming the Modern Era)." *Yumary: Jurnal Pengabdian Kepada Masyarakat* 5, no. 1 (2024): 45–55. https://doi.org/10.35912/yumary.v5i1.2939.

Legislative Council Bureau. Assembly Bill No. 602 (2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

Lesmana, Sri Jaya. "Kajian Yuridis Atas Pelaksanaan Pengawasan Terhadap Jabatan Notaris Menurut Undang-Undang Nomor 2 Tahun 2014 Di Kota Tangerang." *Supremasi Hukum* 15, no. 1 (2019): 32–39. https://doi.org/10.33592/jsh.v15i1.244.

Lesmana, Sri Jaya, and Nikmatul Husna. "Analisis Yuridis Terhadap Sikap Pemerintah Kabupaten Tangerang Dalam Menyikapi Sengketa Lahan." *Supremasi Hukum* 16, no. 2 (2020): 51–57. https://doi.org/10.33592/jsh.v16i2.743.

Lesmana, Sri Jaya, and Inas Sofia Latif. "Law Enforcement in Efforts to Combat Cyber Crime in Indonesia: Building Future Digital Security." *IJLRSA: The International Journal of Law Review and State Administration* 1, no. 3 (2023): 120–28. https://doi.org/10.58818/ijlrsa.v1i3.90.

———. *Pengantar Ilmu Hukum (Inleiding Tot De Rechtwetenschap)*. Tangerang Selatan: Berkah Aksara Cipta Karya, 2024.

Lesmana, Sri Jaya, Hudaya Latuconsina, Ari Suseno, Aqilah Aulia Yumna, and Cindy Aulia Herawati. "Pemberdayaan Masyarakat Melalui Teknologi Pengelolaan Sampah Menggunakan Rocket Eco Stove Incinerator (REST-I) Di Kelurahan." *Solma* 13, no. 3 (2024): 2789–99. https://doi.org/10.22236/solma.v13i3.16389.

Lesmana, Sri Jaya, Reyhan Alifrinaldy Lesmana, Ratna Indayatun, and Sukhebi Mofea. "Evaluating Surveillance Measures at Airports in Responding to Airline Negligence and Lost Baggage." *Media of Law and Sharia* 6, no. 3 (2025): 228–47. https://doi.org/10.18196/mls.v6i3.368.

Lesmana, Sri Jaya, and Muhammad Mpu Samudra. "Legal Protection of Gig Economy Workers: A Comparative Study in Indonesia, Malaysia , and Singapore." *SASI* 31, no. 3 (2025): 201–18. https://doi.org/10.47268/sasi.v31i3.3006.

Liliana, Dewi Yanti, Rizki Elisa Nalawati, Bambang Warsuta, and Sugiyanto. "Kajian

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

Pemanfaatan Teknologi Artificial Intelligence Generatif Dalam Aktivitas Akademik Di Politeknik Negeri Jakarta." In *SNIV: Seminar Nasional Inovasi Vokasi*, 2:523–33, 2023.

M.D, Bintang, and Muh. Ali Masnun. "Prospek Artificial Intelligence Sebagai Quasi Subjek Hukum: Dinamika Pengaturan Hukum Perdata Di Indonesia." *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora* 4, no. 2 (2024): 1–19. https://doi.org/10.53697/iso.v4i2.2063.

Mania, Karolina. "Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study." *Trauma, Violence, and Abuse* 25, no. 1 (2024): 117–29. https://doi.org/10.1177/15248380221143772.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2017.

Meinarni, Ni Putu Suci, and Ida Bagus Ary Indra Iswara. "Hoax and Its Mechanism in Indonesia." In *Advances in Social Science, Education and Humanities Research: 2nd International Conference of Communication Science Research (ICCSR 2018)*, 165:183–86. Atlantis Press, 2018. https://doi.org/10.2991/iccsr-18.2018.39.

Mustak, Mekhail, Joni Salminen, Matti Mäntymäki, and Yogesh Kumar Dwivedi. "Deepfakes: Deceptions, Mitigations, and Opportunities." *Journal of Business Research* 154, no. 2 (2023): 1–33. https://doi.org/10.1016/j.jbusres.2022.113368.

Noerman, Chiquita Thefirstly, and Aji Lukman Ibrahim. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara; Criminalization of Deepfake in Indonesia as a Form of State Protection." *USM Law Review* 7, no. 2 (2024): 1–4. https://doi.org/10.26623/julr.v7i2.8995.

Nurhayati, Yati, Ifrani Ifrani, and M. Yasir Said. "Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum." *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20. https://doi.org/10.51749/jphi.v2i1.14.

Okolie, Chidera. "Artificial Intelligence-Altered Videos (Deepfakes) and Data Privacy Concerns." *Journal of International Women's Studies* 25, no. 2 (2023): 1–16. https://vc.bridgew.edu/jiws/vol25/iss2/11%0AThis.

Palindria, Arvi Erawan, Muhammad Sulthan Thufail, and Muhammad Rieval Febrian. "Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia." *Spektrum Hukum* 21, no. 2 (2024): 110–21. https://doi.org/10.56444/sh.v21i2.5319.

Putra, Komang Bagus Wicaksana, and Gusti Ayu Arya Prima Dewi. "Urgensi Pengaturan Tindak Pidana Deepfake Pornografi Di Indonesia." *Jurnal Kertha Wicara* 13, no. 10 (2024): 530–41. https://doi.org/10.1016/j.cviu.2022.103525.1.

Rangkuti, Putri Ramadhani, Rahma Fitri Amelia Hasibuan, Vressilia Witama, Maria Arfah Nasution, Siti Kholizah, Nadilah Andini, and Siti Salmiah. "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE: Studi Kasus Di Media Sosial Indonesia." *Deposisi: Jurnal Publikasi Ilmu Hukum* 3, no. 2 (2025): 111–20. https://doi.org/10.59581/deposisi.v3i2.5080.

Ristiyana, Rida, Eko Trianto, and Sri Jaya Lesmana. "Upaya Menghadapi Era Society 5.0 Melalui Sosialisasi Pembentukan Jiwa Entrepreneur Dan Penyajian Laporan Keuangan Pada Generasi Muda Di Tangerang." *Jurnal SOLMA* 13, no. 2 (2024): 777–88. https://doi.org/10.22236/solma.v13i2.15193.

Riyanto, Galuh Putri, and Wahyunanda Kusuma Pertiwi. "Menilik Teknologi 'Deepfake' Di

p-ISSN: 2541-2345, e-ISSN: 2580-8842
https://journals.usm.ac.id/index.php/jic

Balik Video Diduga Mirip Nagita Slavina." *Kompas.Com*, 2022. https://tekno.kompas.com/read/2022/01/18/15490077/menilik-teknologi-deepfake-di-balik-video-diduga-mirip-nagita-slavina?page=all#google_vignette.

Sari, Happy Budyana, Ni Made Ayu Priska Cahya Ningsih, Ni Made Yuli Kristina, Ni Putu Indah Rismayanti, Emmy Febriani Thalib, Ni Putu Suci Meinarni, and Lis Julianti. "Digital Ethics and Citizenship Challenges in Cyberspace: An Overview From Perspective Morals and Laws." *Jurnal Notariil* 9, no. 1 (2024): 33–39. https://doi.org/10.22225/jn.9.1.2024.33-39.

Shirish, Anuragini, and Shobana Komal. "A Socio-Legal Inquiry on Deepfakes." *California Western International Law Journal* 54, no. 2 (2024): 517–60. https://scholarlycommons.law.cwsl.edu/cwilj/vol54/iss2/6.

Tiessa, Amelia Noviana, Sri Jaya Lesmana, and Ratna Indayatun. "Analisis Efektivitas Electronic Traffic Law Enforcement (ETLE) Dalam Sistem Penegakan Hukum Di Kabupaten Tangerang." *SOSCIED: Journal Social, Science, and Education* 8, no. 1 (2025): 1–11. https://doi.org/10.32531/jsoscied.v8i1.829.

Tim CNN Indonesia. "SAFEnet: Kekerasan Berbasis Gender Naik, Terbanyak Usia 18-25 Tahun." *CNN Indonesia*, 2024. https://www.cnnindonesia.com/teknologi/20240509094321-192-1095678/safenet-kekerasan-berbasis-gender-naik-terbanyak-usia-18-25-tahun.

Trombevski, Dimitar. "Deepfakes and the Future of AI Legislation: Overcoming the Ethical and Legal Challenges." GDPR Local, 2025. https://gdprlocal.com/deepfakes-and-the-future-of-ai-legislation-overcoming-the-ethical-and-legal-challenges/.

Zhao, Hanqing, Tianyi Wei, Wenbo Zhou, Weiming Zhang, Dongdong Chen, and Nenghai Yu. "Multi-Attentional Deepfake Detection." In *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. Nashville: IEEE: Institute of Electrical and Electronics Engineers, 2021. https://doi.org/10.1109/CVPR46437.2021.00222.