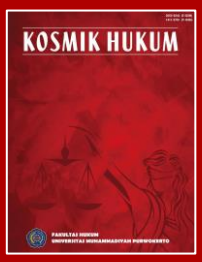

Kosmik Hukum

Faculty of Law - Universitas Muhammadiyah Purwokerto
Volume 26 Issue 2, May 2026

Print ISSN: 1411-9781 | Online ISSN: 2655-9242
Homepage: https://jurnalnasional.ump.ac.id/index.php/KOSMIK

Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China

Ikama Dewi Setia Triana[1]✉, **Aniek Periani**[2], **Arka Atyanta**[3]

[1,2,3] Faculty of Law, Universitas Wijayakusuma Purwokerto, Indonesia

Corresponding: ikamadewisetiatriana@unwiku.ac.id

Received: 2025-01-26 | **Accepted:** 2026-04-25 | **Published:** 2026-05-07

Abstract

The rapid development of artificial intelligence (AI) technology has accelerated the emergence of deepfake media capable of manipulating audio, video, and images with highly realistic results. Although deepfake technology offers creative and economic benefits, its misuse has created serious legal, ethical, and social challenges, including digital fraud, political disinformation, identity theft, and non-consensual pornography. Indonesia currently lacks a comprehensive legal framework specifically regulating deepfake and generative AI technologies, resulting in regulatory fragmentation and weak victim protection. This study aims to analyze comparative regulatory models regarding deepfake crimes in the European Union, the United States, and the People's Republic of China, as well as to examine the urgency of legal reform in Indonesia. This research employs normative legal research using statutory, conceptual, and comparative approaches. The findings demonstrate that the European Union adopts a risk-based and transparency-oriented model through the Artificial Intelligence Act, the United States applies fragmented sectoral regulations prioritizing freedom of expression, while China emphasizes state-centered digital governance and platform liability. Meanwhile, Indonesia still experiences legal uncertainty, limited digital forensic capacity, and the absence of platform accountability mechanisms. This study argues that Indonesia urgently requires a comprehensive AI and deepfake regulatory framework integrating mandatory labeling obligations, victim-oriented protection, AI forensic standards, and platform responsibility mechanisms to ensure digital security, legal certainty, and the protection of human rights in cyberspace.

Keywords: Artificial Intelligence; Comparative Law; Cybercrime; Deepfake

I. Introduction

The rapid advancement of artificial intelligence (AI) technology has transformed the global digital ecosystem and created new forms of synthetic media known as deepfakes. Deepfake technology utilizes machine learning and generative artificial intelligence algorithms to manipulate audio, video, and images with highly realistic results that are often indistinguishable from authentic content. Although this technology provides significant opportunities in entertainment, education, and digital innovation, its misuse has generated serious concerns regarding privacy, democracy, cybersecurity, and human rights protection.[1]

[1] Danielle Keats Citron and Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1755–1760, https://doi.org/10.15779/Z38RV0D15J

The misuse of deepfake technology has increasingly evolved into a transnational cybercrime phenomenon. Deepfakes are now widely used for political disinformation, identity theft, financial fraud, digital extortion, and non-consensual pornography.[2] the emergence of generative AI systems has further accelerated the accessibility and sophistication of deepfake production, enabling individuals with limited technical expertise to create highly convincing synthetic media. Consequently, deepfake-related crimes have become more difficult to detect and regulate within existing legal frameworks.[3]

Indonesia has also experienced a significant increase in deepfake-related crimes. In February 2025, the Indonesian National Police Cyber Crime Directorate uncovered a fraud scheme using deepfake videos featuring President Prabowo Subianto and Finance Minister Sri Mulyani. Approximately 100 victims across 20 provinces suffered financial losses, while the perpetrators gained around IDR 65 million within one month.[4] Furthermore, the Ministry of Communication and Digital Affairs estimated that losses resulting from AI-based fraud and deepfake scams had reached approximately IDR 700 billion.[5] These incidents illustrate how deepfake technology has evolved beyond a technological issue into a serious legal and national security concern.

In addition to financial fraud, deepfake technology has facilitated the spread of non-consensual pornography, political disinformation, digital impersonation, and social manipulation through various digital platforms such as Instagram, TikTok, Telegram, WhatsApp, and X (formerly Twitter). The rapid expansion of social media combined with low digital literacy among users has intensified the dissemination of manipulated AI-generated content.[6] Moreover, many cyber fraud operations involving deepfake technologies are allegedly linked to transnational criminal networks operating in Cambodia alongside online gambling and scamming industries.[7]

Despite the increasing risks posed by deepfake technology, Indonesia still lacks a comprehensive legal framework specifically regulating generative AI and deepfake-related crimes. Existing regulations, including Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and Law Number 44 of 2008 concerning Pornography, only provide fragmented and partial protections. These laws do not clearly define deepfake technology, establish AI transparency obligations, regulate platform accountability, or provide adequate victim oriented protection mechanisms.[8] As a result, law enforcement agencies continue to face difficulties in addressing deepfake related offenses within the existing legal system.

Comparative legal developments demonstrate that several jurisdictions have adopted more structured and adaptive approaches toward deepfake regulation. The European Union introduced a risk-based governance model through the Artificial Intelligence Act, the Digital Services Act, and the General Data Protection Regulation (GDPR), emphasizing transparency

---

2 Maria Pawelec, "Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions," *Digital Society* 1, no. 19 (2022): 4–9, https://doi.org/10.1007/s44206-022-00010-6

3 Thanh Thi Nguyen et al., "Deep Learning for Deepfakes Creation and Detection: A Survey," *Computer Vision and Image Understanding* 223 (2022): 103525, https://doi.org/10.1016/j.cviu.2022.103525

4 Kompas.com, "100 Orang Jadi Korban Penipuan Pakai Video Deepfake Prabowo, Kerugian Capai Rp65 Juta," *Kompas.com*, February 7, 2025, https://nasional.kompas.com/read/2025/02/07/18360001/100-orang-jadi-korban-penipuan-pakai-video-deepfake-prabowo-kerugian-capai

5 DetikInet, "Penyalahgunaan AI Meresahkan, Kasus Penipuan Deepfake Capai Rp700 M," *Detik.com*, October 24, 2025, https://inet.detik.com/law-and-policy/d-8177140/penyalahgunaan-ai-meresahkan-kasus-penipuan-deepfake-capai-rp-700-m

6 Adrienne de Ruiter, "The Distinct Wrong of Deepfakes," *Philosophy & Technology* 34, no. 4 (2021): 1318–1324, https://doi.org/10.1007/s13347-021-00459-2

7 Kompas.com, "Interpol Polri Sebut Banyak WNI yang Kerja di Perusahaan Judi Online hingga Scamming di Kamboja," *Kompas.com*, April 14, 2025, https://nasional.kompas.com/read/2025/04/14/12202301/interpol-polri-sebut-banyak-wni-yang-kerja-di-perusahaan-judi-online-hingga

8 Suteki A. V. A. Nasution, and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38, no. 7 (2025): 5–11, https://doi.org/10.1007/s11196-025-10265-0

obligations, algorithmic accountability, and mandatory labeling for AI-generated synthetic content.[9] The United States, meanwhile, employs fragmented sectoral regulations primarily focusing on election manipulation, non-consensual pornography, and consumer protection.[10] In contrast, the People's Republic of China adopts a state centered governance approach emphasizing platform liability, identity verification, and digital surveillance through the Provisions on the Administration of Deep Synthesis Internet Information Services.[11]

Previous studies concerning deepfake regulation and artificial intelligence governance have demonstrated the growing urgency of establishing adaptive legal frameworks capable of addressing the misuse of synthetic media technologies. Suteki, Angelica Vanessa Audrey Nasution, and Anggita Doramia Lumbanraja examined the legal challenges relating to deepfake pornography and the implementation of the right to be forgotten in Indonesia. Their research emphasized that Indonesian positive law remains fragmented and insufficient in protecting victims of AI-generated sexual abuse, particularly because existing regulations do not specifically regulate synthetic pornography and biometric data misuse.[12] However, the study primarily focused on victim protection and privacy rights without conducting a broader comparative analysis concerning international regulatory models of AI governance.

In addition, Robert Chesney and Danielle Keats Citron analyzed the implications of deepfake technology for privacy, democracy, and national security within the United States legal context.[13] Their study highlighted how deepfake technology has transformed disinformation, digital impersonation, and political manipulation into serious transnational threats requiring comprehensive legal responses. Nevertheless, the study concentrated mainly on the constitutional and cybersecurity dimensions of deepfake regulation in the United States and did not specifically examine comparative legal models applicable to developing countries such as Indonesia.

Furthermore, Yisroel Mirsky and Wenke Lee explored the technological dimensions of deepfake creation and detection by analysing the evolution of generative AI systems and digital forensic methods.[14] Their research demonstrated that the increasing sophistication of AI-generated synthetic media poses significant challenges for digital authentication, cybersecurity, and law enforcement investigations. However, the study predominantly focused on technical detection mechanisms and did not address the broader legal and institutional governance frameworks necessary for regulating deepfake related crimes.

This research possesses novelty compared to previous studies because it not only examines deepfake crimes within the Indonesian legal framework, but also critically analyses comparative regulatory models from the European Union, the United States, and China as foundations for legal reform concerning artificial intelligence governance in Indonesia. Furthermore, this study proposes an integrated regulatory framework combining victim-oriented protection, mandatory labeling obligations, platform accountability, AI forensic standards, and national AI governance mechanisms. The significance of this research lies in its contribution to the development of a comprehensive and adaptive legal framework capable of addressing emerging AI based cybercrimes while simultaneously strengthening digital security, protecting

---

9 Michèle Finck, "Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems," in *The EU Artificial Intelligence Act: A Commentary* (Oxford: Oxford University Press, 2026), 464–481, https://doi.org/10.1093/law/9780198925705.003.0005

10 Daphne Keller, "Regulating Deepfakes after Generative AI," *Journal of Free Speech Law* 3, no. 2 (2023): 260–271, https://doi.org/10.2139/ssrn.4389686

11 Lyu Zhang, "Regulating Deepfakes in China: A Subject-Based Approach," *Asian Journal of Law and Society* 8, no. 2 (2021): 361–367, https://doi.org/10.1017/als.2021.23

12 Angelica Vanessa Audrey Nasution, Suteki, and Anggita Doramia Lumbanraja, "Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489–2517, https://doi.org/10.1007/s11196-025-10265-0

13 Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753–1819.

14 Yisroel Mirsky and Wenke Lee, "The Creation and Detection of Deepfakes: A Survey," *ACM Computing Surveys* 54, no. 1 (2021): 1–41, https://doi.org/10.1145/3425780

human rights, and providing policy recommendations for future AI governance reform in Indonesia.

II. Research Problems

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

1. How are deepfake-related crimes and artificial intelligence (AI) technologies regulated in the legal systems of the United States of America, the European Union, and the People's Republic of China?
2. What regulatory gaps exist within the Indonesian legal framework regarding deepfake and generative artificial intelligence technologies?
3. What legal reform model should Indonesia develop in order to establish a comprehensive, victim-oriented, and adaptive regulatory framework for deepfake and artificial intelligence governance based on comparative approaches from the United States, the European Union, and the People's Republic of China?

III. Research Methods

This study employs normative legal research focusing on the analysis of legal norms, legal principles, and comparative regulatory frameworks concerning the misuse of deepfake technology and generative artificial intelligence (AI). Normative legal research is utilized because this research aims to examine the existence of legal vacuum, regulatory fragmentation, and the urgency of establishing a comprehensive legal framework governing deepfake-related crimes in Indonesia.[15] the research applies several approaches, namely the statutory approach (statute approach), conceptual approach (conceptual approach), and comparative approach (comparative approach). The statutory approach is used to analyze legislation and policy instruments related to cybercrime, AI governance, personal data protection, and digital platforms. The conceptual approach examines legal doctrines and theoretical perspectives concerning digital governance, cyber law, and human rights protection in cyberspace. Meanwhile, the comparative approach compares regulatory models implemented in the European Union, the United States of America, and the People's Republic of China in order to identify regulatory patterns, strengths, weaknesses, and their potential applicability within the Indonesian legal system.[16]

The legal materials used in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation, international legal instruments, government regulations, and official policy documents concerning artificial intelligence and deepfake technology. Secondary legal materials consist of books, reputable international journal articles, research findings, and legal doctrines discussing deepfake regulation, digital governance, cybersecurity, and personal data protection. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting references relevant to the study. The collection of legal materials was conducted through library research by systematically examining legal documents and academic literature. Furthermore, the legal materials were analyzed qualitatively using prescriptive and comparative legal analysis methods. Prescriptive analysis was employed to formulate legal arguments regarding the necessity of establishing a specific AI and deepfake regulatory framework in Indonesia, while comparative analysis was conducted to formulate policy recommendations and legal reform models based on comparative experiences from the European Union, the United States, and the People's Republic of China.[17]

---

15 Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif* (Jakarta: Rajawali Pers, 2020), 13–15.
16 Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2021), 133–172.
17 Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif* (Malang: Bayumedia, 2019), 300–305.

IV. Results and Discussion

1. Regulatory Models of Deepfake Crimes in Developed Countries

a. European Union: Risk-Based and Transparency-Oriented Regulation

The European Union represents one of the most progressive jurisdictions in regulating artificial intelligence technologies, including deepfake technology. Such regulation is institutionalized through the Artificial Intelligence Act (AI Act), which categorizes deepfake systems as AI technologies capable of posing risks to fundamental rights, democracy, and public security. The regulation requires synthetic AI generated content to be accompanied by clear labeling obligations and transparency measures directed toward the public.[18] This approach reflects the European Union's broader regulatory philosophy that artificial intelligence should not merely be treated as a technological innovation, but also as a socio-legal instrument capable of producing significant political, ethical, and legal consequences if left inadequately regulated.[19]

Through Article 50 of the AI Act, the European Union mandates that any individual or service provider generating or distributing deepfake content must clearly disclose that the content has been synthetically manipulated using artificial intelligence.[20] This obligation reflects the principle of digital transparency, which constitutes one of the primary foundations of AI governance within the European Union.[21] The provision aims to prevent disinformation, political manipulation, digital fraud, and violations of individual privacy rights. In addition, the regulation strengthens the accountability of digital platforms by requiring service providers to implement risk mitigation mechanisms against the dissemination of deepfake content through content moderation systems, automated detection technologies, and algorithmic oversight measures.[22]

The European Union's regulatory initiative is fundamentally intended to preserve the integrity of information ecosystems, particularly within the sphere of public communication, while simultaneously preventing technological developments that may threaten privacy, security, and democratic stability.[23] uch concerns have become increasingly significant because deepfake technology is capable of generating highly realistic synthetic audio and visual content that is often indistinguishable from authentic materials. Consequently, deepfakes possess substantial potential to be utilized for political propaganda, manipulation of public opinion, financial fraud, and digital exploitation of individuals.[24] Accordingly, the European Union seeks to construct a regulatory framework capable of anticipating the adverse consequences of AI development without unnecessarily restricting technological innovation and digital economic growth.

The European Union's approach demonstrates a risk-based regulatory model that seeks to balance technological innovation with the protection of human rights. In this context, the European Union does not exclusively rely upon criminal sanctions; rather, it develops a broader digital governance framework emphasizing algorithmic transparency, platform accountability, and consumer protection in digital environments.[25] This preventive regulatory paradigm

---

[18] I Bień-węgłowska, "Deepfakes in the Light of the Artificial Intelligence Act". *Prawo i Wiez*, 58 (5) (2025): 151–169., https://doi.org/10.36128/4dr67e80

[19] European Parliament, Artificial Intelligence Act, Regulation (EU) 2024/1689, art. 50, https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[20] T. Gils. A detailed analysis of Article 50 of the EU's Artificial Intelligence Act. In C. N. Pehlivan, N. Forgó, & P. Valcke (Eds.), The EU Artificial Intelligence (AI) Act:" *Kluwer Law International*. (2025): 776–823. https://doi.org/10.2139/ssrn.4865427

[21] Lilian Edwards, "Regulating AI in Europe: Four Problems and Four Solutions," *Ada Lovelace Institute* (2023): 5–8

[22] Martin Ebers, "Liability for AI and EU Consumer Law," *Journal of European Consumer and Market Law* 10, no. 5 (2021): 204–209, https://doi.org/10.21552/eur/2021/5/5

[23] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Transparent, Explainable, and Accountable AI for Robotics," *Science Robotics* 2, no. 6 (2017): 1–2, https://doi.org/10.1126/scirobotics.aan6080

[24] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753–1820, https://doi.org/10.15779/Z38RV0D15J

[25] Karen Yeung, "A Study of the Implications of Advanced Digital Technologies for the Concept of Responsibility within a Human Rights Framework," *Human Rights Law Review 19*, no. 2 (2019): 257–283, https://doi.org/10.1093/hrlr/ngz007

illustrates the European Union's preference for ex ante risk mitigation rather than ex post punitive enforcement. Such an approach may serve as an important reference for Indonesia, particularly because the current Indonesian legal framework still lacks a comprehensive legal definition of deepfake technology as well as explicit obligations concerning the labeling of synthetic media. Therefore, the European Union model may provide valuable guidance in developing a more adaptive, comprehensive, and technologically responsive national legal framework concerning artificial intelligence governance in Indonesia.[26]

Furthermore, the European Union does not merely perceive deepfake technology as an issue of digital misinformation, but also as a threat to fundamental rights, including the rights to privacy, freedom of expression, and democratic integrity. Consequently, the AI Act is designed in conjunction with the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) in order to establish a multi-layered digital governance system.[27] This integrated regulatory structure demonstrates that the European Union adopts a preventive governance model emphasizing the mitigation of societal risks before widespread harm occurs. Nevertheless, several scholars have criticized the potentially excessive rigidity of the AI Act, arguing that overly burdensome compliance obligations may inhibit innovation and disproportionately increase compliance costs for startups and small-scale AI developers.[28]

In addition, the AI Act also functions as a regulatory instrument requiring digital platforms to implement mechanisms capable of detecting and mitigating deepfake content distributed through social media platforms. Such obligations include transparency requirements regarding algorithmic operations and stricter supervision concerning the creation and dissemination of synthetic videos and manipulated images.[29] Accordingly, the European Union continues to construct a digital legal ecosystem that not only imposes sanctions upon perpetrators, but also emphasizes prevention, accountability, and integrated technological governance through administrative and technical regulatory measures.[30]

b. United States of America: Fragmented and Sectoral Regulation

The fragmented nature of deepfake regulation in the United States is largely influenced by the strong constitutional protection of freedom of speech under the First Amendment of the Constitution of the United States. This constitutional framework creates substantial challenges for the federal government in enacting overly restrictive deepfake regulations, as such measures may be viewed as infringing upon constitutionally protected expressive rights.[31] Consequently, the regulatory approach adopted by the United States tends to be reactive and harm-based, particularly in relation to non-consensual pornography, electoral manipulation, and digital fraud.[32] However, this sectoral regulatory model has frequently been criticized as inadequate in addressing the rapid transnational development of generative artificial intelligence technologies.[33]

---

26 Suteki, A. V. A. Nasution, and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38, no. 7 (2025): 5–11, https://doi.org/10.1007/s11196-025-10265-0

27 European Parliament and Council, Digital Services Act, Regulation (EU) 2022/2065, https://eur-lex.europa.eu/eli/reg/2022/2065/oj ; European Parliament and Council, General Data Protection Regulation, Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj

28 Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act," *Computer Law Review International* 22, no. 4 (2021): 97–112, https://doi.org/10.9785/cri-2021-220402

29 A. Fernandez, "Deep fakes": disentangling terms in the proposed EU Artificial Intelligence Act. UFITA – *Archiv für Medienrecht und Medienwissenschaft*, (2), (2021): 392–433. https://doi.org/10.5771/2568-9185-2021-2-392

30 I Bień-węgłowska, Deepfakes in the Light of the Artificial Intelligence Act. *Prawo i Wiez*, 58 (5), (2025): 151–169. https://doi.org/10.36128/4dr67e80

31 Amy Kapczynski, "The First Amendment and the Regulation of Disinformation," *Yale Law Journal Forum* 131 (2021): 227–240, https://www.yalelawjournal.org/forum/the-first-amendment-and-the-regulation-of-disinformation

32 Bobby Chesney and Danielle Citron, "Deepfakes and the New Disinformation War," *Foreign Affairs* 98, no. 1 (2019): 147–155, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

33 Daniel J. Solove, "Deepfakes, Privacy, and the First Amendment," *Boston University Law Review* 103, no. 2 (2023): 499–528, https://doi.org/10.2139/ssrn.4303959

To date, the United States has not enacted a comprehensive federal statute specifically governing deepfake technology. Existing legal measures remain dispersed across state legislation and sector-specific laws relating to elections, consumer protection, and non-consensual synthetic pornography.[34] This fragmented framework creates significant legal uncertainty because each state adopts different regulatory standards and enforcement mechanisms. States such as California, Texas, and Virginia have enacted legislation specifically targeting political deepfakes and synthetic sexual content; however, substantial inconsistencies remain regarding the scope of prohibited conduct, evidentiary standards, and sanctions.[35] As a result, legal protection for victims often varies considerably depending upon the jurisdiction in which the offense occurs.[36]

Moreover, scholars have emphasized that the absence of a unified federal framework causes state-based regulatory approaches to lag behind the rapid evolution of AI technologies.[37] As deepfake systems become increasingly sophisticated, accessible, and difficult to detect, sectoral legislation is often incapable of providing comprehensive legal protection, particularly in cases involving sexual exploitation, reputational harm, and political disinformation.[38] These developments have intensified calls for the United States federal government to establish a comprehensive national legal framework capable of addressing the ethical, social, and legal implications of deepfake technology more effectively.[39]

Despite these weaknesses, the regulatory approach adopted by the United States highlights the continuing importance of protecting freedom of expression within democratic societies. Unlike the European Union, which prioritizes digital security and personal data protection, the United States remains cautious in imposing extensive restrictions upon synthetic media due to constitutional concerns regarding free speech protections.[40] Accordingly, the American model illustrates the ongoing tension between safeguarding civil liberties and addressing the increasingly harmful consequences of AI-generated disinformation.

2. People's Republic of China: State-Centered Digital Governance

The People's Republic of China has developed a considerably stricter model of deepfake regulation through a governance framework centered upon the liability of digital service providers. The Chinese government requires online platforms to conduct identity verification procedures, supervise synthetic content, and apply mandatory labeling mechanisms to AI-generated or manipulated media.[41]

China's principal regulation concerning deepfake technology is embodied in the Provisions on the Administration of Deep Synthesis Internet Information Services, which entered into force in 2023. The regulation imposes obligations upon service providers to prevent the dissemination of false information capable of disrupting social order or threatening national security.[42] Furthermore, the Chinese government possesses extensive authority to supervise, censor, and regulate digital activities conducted within cyberspace.

China's regulatory approach toward deepfake technology is strongly influenced by the doctrine of cyber sovereignty, which positions the state as the primary actor controlling digital

---

[34] United States Congressional Research Service, "Deepfakes and National Security", *IF11333* (2023), https://crsreports.congress.gov/product/pdf/IF/IF11333

[35] Rebecca Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization," *Fordham Law Review* 88, no. 3 (2019): 887–938, https://ir.lawnet.fordham.edu/flr/vol88/iss3/2

[36] D. K Citron., & R. Chesney, (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

[37] Henry Ajder et al., *The State of Deepfakes: Landscape, Threats, and Impact* (Amsterdam: Deeptrace Labs, 2020), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

[38] Danielle Keats Citron, "Sexual Privacy," *Yale Law Journal* 128, no. 7 (2019): 1870–1960, https://www.yalelawjournal.org/article/sexual-privacy

[39] *Ibid*.

[40] Eugene Volokh, "Freedom of Speech and Deepfake Regulation," Journal of Free Speech Law 1, no. 2 (2021): 221–248, https://www.journaloffreespeechlaw.org/volokh.pdf

[41] Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services* (2023), http://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm

[42] *Ibid.*

spaces and information flows.[43] In this context, deepfake regulation functions not merely as an instrument for protecting society from digital disinformation, but also as part of a broader national strategy aimed at preserving political stability and strengthening state control over information dissemination. Consequently, digital platforms operating within China are granted and simultaneously required to exercise extensive powers relating to content censorship, identity verification, and AI algorithm supervision.[44]

This governance model reflects a broader state-centered digital governance paradigm prioritizing social stability and governmental authority over cyberspace. While the Chinese model is often regarded as highly effective in enabling rapid mitigation of harmful deepfake content, numerous scholars have criticized it for potentially undermining civil liberties, privacy rights, and freedom of expression.[45] In particular, critics argue that the integration of AI governance with extensive state surveillance mechanisms risks reinforcing the emergence of a modern surveillance state within digital society.[46]

Nevertheless, the Chinese regulatory framework demonstrates the importance of integrating AI governance, cybersecurity policy, and platform accountability within a unified legal structure. For Indonesia, the Chinese experience illustrates the practical significance of establishing coordinated responsibilities between government institutions and digital service providers in combating deepfake-related harms. However, any potential adoption of similar mechanisms within Indonesia must remain consistent with democratic constitutional principles, the protection of human rights, and proportional limitations upon state surveillance authority. Therefore, while China's model offers valuable lessons regarding regulatory effectiveness and institutional coordination, its implementation within democratic jurisdictions requires careful adaptation to avoid excessive restrictions upon civil liberties and digital freedoms.

3. Comparative Court Cases and Legal Enforcement on Deepfake Crimes

The following table illustrates several comparative court cases and legal enforcement mechanisms relating to deepfake crimes across different jurisdictions, namely the European Union, the United States, the People's Republic of China, and Indonesia. The table demonstrates that deepfake-related offenses have evolved into a transnational legal issue affecting various sectors, including political stability, privacy protection, digital security, and public trust in information systems. In practice, the misuse of deepfake technology has generated diverse forms of harm, ranging from political disinformation and non-consensual pornography to financial fraud and digital impersonation.[47] Accordingly, different jurisdictions have developed distinct regulatory and enforcement approaches depending upon their respective constitutional principles, governance models, and cybersecurity priorities.

Table 1. Comparative Court Cases and Legal Enforcement on Deepfake Crimes

Country, Year	Defendant/ Perpetrator	Chronology of the Case	Regulations Applied	Court Decision
Italy (EU) 2020 [48]	Anonymous perpetrators distributing political	AI-generated videos manipulating political figures were	General Data Protection Regulation (GDPR) (EU) 2016/679; Artificial Intelligence	The defendants faced prosecution before the Sassari Court. Giorgia Meloni requested

[43] Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," Australian Strategic Policy Institute (2019): 10–15, https://www.aspi.org.au/report/engineering-global-consent

[44] Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cyber Policy* 7, no. 1 (2022): 1–18, https://doi.org/10.1080/23738871.2021.2008770

[45] Min Jiang and Ran Wei, "Deepfake Governance in China: Law, Policy, and Platform Responsibility," *Internet Policy Review* 12, no. 2 (2023): 1–19, https://doi.org/10.14763/2023.2.1689

[46] *Ibid.*

[47] Danielle Keats Citron and Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1768–1775, https://doi.org/10.15779/Z38RV0D15J

[48] Kevin Carboni, "Il Processo per i Deepfake Porno con il Volto di Giorgia Meloni," Wired Italia, March 21, 2024, https://www.wired.it/article/giorgia-meloni-deepfake-porno-processo/;

Country, Year	Defendant/ Perpetrator	Chronology of the Case	Regulations Applied	Court Decision
	deepfake videos	disseminated online to spread disinformation and influence public opinion during political discourse.	Act (Article 50 on transparency obligations); Italian Cybercrime Law; Digital Services Act (DSA)	€100,000 in damages, while Italian law provides sanctions of 1–5 years' imprisonment for unlawful deepfake dissemination.
Virginia (USA) 2023 [49]	Creator of non-consensual deepfake pornography	The perpetrator created and distributed AI-generated pornographic videos using victims' facial identities without consent through social media and online platforms.	Virginia Code 18.2-386.2 concerning non-consensual pornography; California AB 602; Texas Election Code 255.004; state privacy and cybercrime law	Under Virginia law, offenders may face up to 12 months imprisonment and fines up to US$2,500, while civil liability under California law allows victims to claim financial damages and injunctive relief.
People's Republic of China (2023) [50]	Deep synthesis platform operator	A digital platform failed to implement mandatory labeling and identity verification for AI-generated synthetic media distributed online.	Provisions on the Administration of Deep Synthesis Internet Information Services (2023); Cybersecurity Law of the People's Republic of China (2017); Data Security Law (2021)	Chinese cyberspace authorities imposed administrative fines, mandatory corrective actions, suspension of platform services, and potential revocation of operating licenses for repeated violations
Indonesia (2025)[51]	Deepfake fraud syndicate using President Prabowo Subianto and Minister Sri Mulyani's likeness	The perpetrators used AI-generated deepfake videos impersonating Indonesian public officials to deceive victims into transferring money through online platforms. Approximately 100 victims across 20 provinces	Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law); Law No. 27 of 2022 concerning Personal Data Protection; Indonesian Criminal Code (KUHP)	Indonesian authorities initiated criminal prosecution. Based on Article 378 KUHP and the amended ITE Law, perpetrators potentially face up to 4–6 years' imprisonment, financial restitution, confiscation of digital assets, and

[49] Danielle Keats Citron and Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1768–1775, https://doi.org/10.15779/Z38RV0D15J

[50] Lyu Zhang, "Regulating Deepfakes in China: A Subject-Based Approach," *Asian Journal of Law and Society* 8, no. 2 (2021): 361–367, https://doi.org/10.1017/als.2021.23

[51] Kompas.com, "100 Orang Jadi Korban Penipuan Pakai Video Deepfake Prabowo, Kerugian Capai Rp65 Juta," *Kompas.com*, February 7, 2025, https://nasional.kompas.com/read/2025/02/07/18360001/100-orang-jadi-korban-penipuan-pakai-video-deepfake-prabowo-kerugian-capai.

Country, Year	Defendant/ Perpetrator	Chronology of the Case	Regulations Applied	Court Decision
		suffered financial losses.	provisions on fraud (Article 378 KUHP)	electronic evidence seizure.

Source: Author's Analysis.

The table highlights that legal responses toward deepfake crimes are no longer limited to conventional criminal sanctions but increasingly incorporate broader digital governance mechanisms such as platform accountability, transparency obligations, identity verification systems, and administrative enforcement measures.[52] The comparative perspective presented in the table is important in identifying the strengths and weaknesses of each jurisdiction's regulatory framework while simultaneously illustrating the urgency for Indonesia to establish a comprehensive legal framework specifically governing generative artificial intelligence and deepfake-related harms. Through comparative legal analysis, the table provides a foundation for evaluating how Indonesia may adopt adaptive and balanced regulatory mechanisms capable of protecting digital rights, maintaining cybersecurity, and ensuring effective law enforcement against emerging AI-based crimes.

The table demonstrates that the European Union adopts a preventive and rights-oriented regulatory model emphasizing transparency obligations and platform accountability through the Artificial Intelligence Act, GDPR, and Digital Services Act. The case involving deepfake pornography and political manipulation in Italy illustrates how European legal frameworks combine privacy protection, administrative obligations, and criminal sanctions in addressing synthetic media harms. This model reflects the European Union's broader commitment to protecting democratic integrity and fundamental rights within digital environments.[53] Nevertheless, the European approach also reveals challenges concerning regulatory complexity and potentially high compliance costs for digital platforms and AI developers.

In contrast, the United States employs a fragmented and sectoral enforcement approach primarily focused on specific harms such as non-consensual pornography and election manipulation. The Virginia case demonstrates that state-level legislation remains the primary mechanism for prosecuting deepfake-related offenses, particularly in relation to synthetic sexual content. However, the absence of a unified federal framework creates inconsistent legal standards and varying levels of victim protection among states.[54] Meanwhile, China adopts a considerably stricter governance model emphasizing platform liability, mandatory identity verification, and administrative enforcement under state-centered digital governance principles. Indonesia, by comparison, still relies upon general provisions within the ITE Law, Personal Data Protection Law, and the Criminal Code, resulting in legal uncertainty and limited institutional capacity in addressing AI-generated harms. This comparison indicates that Indonesia urgently requires integrated legal reform combining transparency obligations, platform responsibility, victim protection mechanisms, and AI forensic standards in order to effectively respond to deepfake-related crimes in the future.

4. Regulatory Gaps and Legal Reform Urgency in Indonesia

Compared to the regulatory frameworks adopted by the European Union, the United States, and the People's Republic of China, Indonesia remains within a fragmented regulatory stage, lacking a specific and comprehensive legal framework governing generative artificial intelligence and deepfake technology. This condition demonstrates that Indonesia has not yet

[52] Karen Yeung, "A Study of the Implications of Advanced Digital Technologies for the Concept of Responsibility within a Human Rights Framework," *Human Rights Law Review* 19, no. 2 (2019): 257–283, https://doi.org/10.1093/hrlr/ngz007

[53] Michèle Finck, "Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems," in The EU Artificial Intelligence Act: A Commentary (Oxford: Oxford University Press, 2026), 464–481, https://doi.org/10.1093/law/9780198925705.003.0005

[54] Rebecca Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization," *Fordham Law Review* 88, no. 3 (2019): 887–938, https://ir.lawnet.fordham.edu/flr/vol88/iss3/2

developed an adaptive AI governance framework capable of responding effectively to the rapid evolution of global digital technologies.[55] At present, legal provisions relating to digital technology misuse are dispersed across several sectoral statutes, resulting in overlapping norms and regulatory gaps that are insufficient to address the complexity of AI-based crimes.[56]

In law enforcement practice, Indonesian authorities continue to encounter substantial obstacles in addressing deepfake-related crimes. One of the principal problems is the absence of a formal legal definition of deepfake technology within national legislation.[57] The absence of such a definition creates considerable uncertainty for law enforcement officials in determining the appropriate legal construction, particularly when distinguishing between ordinary digital manipulation and AI-generated synthetic content produced through machine learning or deep neural network technologies. As a result, many deepfake cases are prosecuted using general criminal provisions relating to defamation, dissemination of false information, decency violations, or personal data misuse, despite the fact that such provisions were not specifically designed to address the technical and evidentiary complexities of generative AI systems.[58]

Furthermore, although the amended ITE Law regulates unlawful electronic information, including defamatory content, hate speech, misinformation, and manipulation of electronic information, the law does not impose obligations relating to the transparency of AI-generated synthetic content in particular, Indonesian legislation has not yet introduced mandatory labeling obligations requiring disclosure that audio, video, or visual materials have been manipulated through deepfake technology. This regulatory deficiency creates serious risks for society because the public often cannot distinguish between authentic and manipulated digital content, especially within contexts involving political disinformation, digital fraud, and social media propaganda. The increasing sophistication of deepfake technology poses serious threats to public trust, democratic processes, and national security because manipulated synthetic media may substantially influence public opinion and damage individual reputations.

On the other hand, although the PDP Law provides protection against the unauthorized use of personal data, it does not specifically regulate the use of biometric data such as facial images, voice recordings, and visual expressions utilized in deepfake creation.[59] This issue is particularly significant because deepfake technology generally relies upon biometric data collected from social media platforms and digital environments without the consent of the data subject. The absence of specific biometric protection mechanisms creates substantial risks relating to privacy violations, identity exploitation, and large-scale misuse of digital personal data.[60]

More serious concerns arise in relation to AI-generated pornography and synthetic sexual abuse. Although Law Number 44 of 2008 concerning Pornography prohibits the production and dissemination of illegal pornographic materials, the law remains inadequate in addressing generative AI technologies capable of producing synthetic pornographic content without direct physical involvement of the victim. In many cases, victims' faces are digitally superimposed onto other bodies using AI systems, creating realistic but fabricated pornographic materials. Such crimes generate severe psychological, social, and economic harms for victims, particularly

---

55 M. Syamsudin, "Perlindungan Hukum terhadap Korban Kejahatan Siber di Indonesia," *Jurnal Hukum IUS QUIA IUSTUM* 28, no. 1 (2021): 1–20, https://doi.org/10.20885/iustum.vol28.iss1.art1

56 Arifin, Fernando, and Handayani, "Legal Implications of The Second Amendment to The Electronic Information and Transactions Law," *Jurnal Litigasi* 26, no. 1 (2025), https://doi.org/10.23969/litigasi.v26i1.21555

57 R. Herlambang Perdana Wiratraman, "Digital Constitutionalism and Freedom of Expression in Indonesia," *Hasanuddin Law Review* 8, no. 2 (2022): 145–160, https://doi.org/10.20956/halrev.v8i2.3600

58 Rabith Madah Khulaili Harsya, "Tinjauan Yuridis terhadap Tanggung Jawab Platform Digital atas Konten Ilegal Menurut Hukum Indonesia," *Sanskara Hukum dan HAM* 4, no. 1 (2025): 276–286, https://doi.org/10.58812/shh.v4i01.609

59 Sinta Dewi Rosadi and Rika Ratna Permata, "Perlindungan Data Pribadi dalam Era Ekonomi Digital di Indonesia," *Veritas et Justitia* 8, no. 1 (2022): 91–112, https://doi.org/10.25123/vej.v8i1.5136

60 Hary Oktafiana, Muhammad Miftah Nurhidayatulloh, "Tanggung Jawab Hukum Platform Digital dalam Mengendalikan Penyebaran Konten Ilegal di Internet," *Jurnal Pendidikan Tambusai* 10, no. 1 (2026): 6776–6781, https://doi.org/10.31004/jptam.v10i1.37260

women and vulnerable groups.[61] Victims frequently experience psychological trauma, online harassment, reputational destruction, employment loss, and long-term mental health consequences resulting from the uncontrollable dissemination of synthetic sexual content within digital environments.[62]

The fragmented nature of Indonesian regulation demonstrates the existence of substantial legal uncertainty regarding AI governance and deepfake-related harms. This legal vacuum is further exacerbated by the limited forensic capabilities of Indonesian law enforcement institutions in identifying and proving AI-based manipulation. In practice, the evidentiary process for deepfake-related crimes requires sophisticated digital forensic technologies capable of analyzing metadata, facial synthesis patterns, voice manipulation structures, and algorithmic traces embedded within synthetic media content.[63] Nevertheless, Indonesia continues to face limitations in terms of technological infrastructure, forensic expertise, human resources, and AI-based evidentiary standards.[64]

Based upon these regulatory deficiencies, Indonesia urgently requires comprehensive legal reform through the establishment of a specialized regulatory framework governing artificial intelligence and deepfake technology. Such reform should encompass several essential aspects. First, the legal framework must establish a clear statutory definition of deepfake technology and generative AI systems in order to provide legal certainty in law enforcement processes.[65] Second, Indonesia should introduce mandatory labeling obligations for all AI-generated synthetic content to ensure that the public can distinguish authentic materials from manipulated content. Third, the law must regulate platform liability concerning the detection, moderation, and removal of deepfake content. Fourth, Indonesia requires a victim protection mechanism grounded in human rights principles and gender-sensitive approaches, particularly in cases involving synthetic pornography and digital exploitation targeting women.[66] Fifth, the government should strengthen national digital forensic capacity through the development of AI evidentiary standards and specialized training for law enforcement personnel. Sixth, comprehensive sanctions criminal, civil, and administrative—must be formulated concerning the misuse of deepfake technology. Seventh, Indonesia should establish a rapid response and takedown mechanism capable of addressing the widespread dissemination of harmful synthetic content in digital spaces.[67]

In addition to challenges concerning criminal law enforcement, Indonesia also lacks a clear framework governing the liability of digital platforms in addressing the dissemination of deepfake content. Social media platforms such as Instagram, TikTok, Telegram, Facebook, and X (formerly Twitter) have become the primary channels for distributing AI-generated manipulative content.[68] However, Indonesian law does not yet impose explicit obligations upon digital platforms to implement automated detection systems, labeling mechanisms, content moderation procedures, or rapid takedown systems concerning harmful deepfake content.[69] This situation differs significantly from the European Union's approach under the Artificial Intelligence Act

---

61 Suteki A. V. A. Nasution and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38, no. 7 (2025): 5–11, https://doi.org/10.1007/s11196-025-10265-0

62 Arifin, Fernando, and Handayani, "Legal Implications of The Second Amendment to The Electronic Information and Transactions Law," *Jurnal Litigasi* 26, no. 1 (2025), https://doi.org/10.23969/litigasi.v26i1.21555

63 Thanh Thi Nguyen et al., "Deep Learning for Deepfakes Creation and Detection: A Survey," *Computer Vision and Image Understanding* 223 (2022): 103525, https://doi.org/10.1016/j.cviu.2022.103525

64 M. D. Prasetya et al., "Subordinate Justice to Forensic Scientists: Indonesia's Authority and Regulation Gap," *Media Iuris* 9, no. 1 (2026): 21–29, https://doi.org/10.20473/mi.v9i1.77587

65 Maskun, "Kejahatan Siber (Cyber Crime) dalam Perspektif Hukum Indonesia," *Jurnal Media Hukum* 25, no. 1 (2018): 58–72, https://doi.org/10.18196/jmh.2018.0108

66 Mary Anne Franks, "Deepfakes and the Law," *Fordham Law Review* 89, no. 5 (2021): 1965–1978, https://doi.org/10.2139/ssrn.3852255

67 M. D. Prasetya, et al., "Subordinate Justice to Forensic Scientists: Indonesia's Authority and Regulation Gap," *Media Iuris* 9, no. 1 (2026): 21–29, https://doi.org/10.20473/mi.v9i1.77587

68 Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* (Jakarta: Rajawali Pers, 2020), 144–156.

69 Arifin, Fernando, and Handayani, "Legal Implications of The Second Amendment to The Electronic Information and Transactions Law," *Jurnal Litigasi* 26, no. 1 (2025), https://doi.org/10.23969/litigasi.v26i1.21555

and the Digital Services Act, both of which expressly impose platform accountability obligations concerning synthetic AI-generated content.[70]

In addition to legislative reform, Indonesia also needs to establish a national AI supervisory authority responsible for oversight, certification, algorithmic auditing, and cross-sectoral coordination concerning AI governance and misuse prevention.[71] Such an institution could adopt a governance model similar to the European Union's risk-based AI supervisory framework emphasizing preventive digital governance and algorithmic accountability. The existence of a national AI oversight institution would be essential to ensure that AI development in Indonesia remains balanced between technological innovation, digital economic growth, human rights protection, cybersecurity, and legal certainty.[72] Accordingly, legal reform concerning artificial intelligence and deepfake governance constitutes an urgent necessity for Indonesia in order to develop an adaptive legal system capable of responding effectively to the challenges posed by global digital transformation while simultaneously ensuring adequate protection for society.[73]

Table 2. Comparative Regulatory Models of Deepfake Governance

Jurisdiction	Regulatory Model	Main Characteristics	Advantages	Weaknesses
European Union	Risk-Based Regulation	Transparency obligations, AI labeling, platform accountability	Strong human rights protection	High compliance costs
United States	Sectoral Regulation	State-based laws, election and pornography focus	Protects freedom of expression	Fragmented enforcement
China	State-Centered Governance	Digital surveillance, mandatory identity verification	Rapid enforcement capability	Risks to civil liberties
Indonesia	Fragmented Regulation	Partial regulation under ITE and PDP Laws	Existing cyber law foundation	No specific deepfake framework

Source: Author's Analysis.

The following table presents a comparative overview of regulatory models governing deepfake technology and artificial intelligence across several major jurisdictions, namely the European Union, the United States, China, and Indonesia. The table illustrates that each jurisdiction adopts a distinct regulatory philosophy shaped by its constitutional values, political system, and digital governance objectives. The European Union emphasizes a risk-based and transparency-oriented approach focused on protecting human rights and ensuring algorithmic accountability. The United States prioritizes freedom of expression through fragmented sectoral regulation, while China adopts a centralized state-oriented governance model emphasizing surveillance, identity verification, and strong platform control.[74] Indonesia, however, remains within a fragmented regulatory stage because existing legal instruments only partially regulate deepfake-related harms without establishing a comprehensive AI governance framework.

---

70 Nur Rochaeti, "Kebijakan Hukum Pidana dalam Penanggulangan Cyber Crime di Indonesia," *Masalah-Masalah Hukum* 49, no. 2 (2020): 136–148, https://doi.org/10.14710/mmh.49.2.2020.136-148

71 Michèle Finck, "Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems," in *The EU Artificial Intelligence Act: A Commentary* (Oxford: Oxford University Press, 2026), 464–481, https://doi.org/10.1093/law/9780198925705.003.0005.

72 Wirianingsih, "Analisis Yuridis Tanggung Jawab Platform Media Sosial terhadap Konten Berbahaya bagi Anak di Indonesia," *Journal Evidence of Law* 5, no. 1 (2026), https://doi.org/10.59066/jel.v5i1.2125

73 Jimly Asshiddiqie, Konstitusi dan Konstitusionalisme Indonesia (Jakarta: Sinar Grafika, 2021), 211–219.

74 Lyu Zhang, "Regulating Deepfakes in China: A Subject-Based Approach," Asian Journal of Law and Society 8, no. 2 (2021): 361–367, https://doi.org/10.1017/als.2021.23

Analytically, the table demonstrates that no single regulatory model is entirely perfect or universally applicable. The European Union's framework offers strong legal protection and preventive governance mechanisms but may impose significant compliance burdens upon technology companies and AI developers. Conversely, the United States model protects constitutional civil liberties yet suffers from inconsistent enforcement due to fragmented state-based legislation. China's governance system provides rapid enforcement capability and effective platform supervision; however, it simultaneously raises serious concerns regarding privacy rights, freedom of expression, and excessive state surveillance.[75] Indonesia's position within the table highlights the urgent necessity for legal reform because the current regulatory framework lacks clear definitions, mandatory labeling obligations, platform accountability mechanisms, and AI-specific enforcement standards. Therefore, the comparative analysis indicates that Indonesia should adopt a balanced and adaptive governance framework integrating legal certainty, victim protection, digital security, and democratic accountability in regulating deepfake and generative AI technologies.

V. Conclusion

This study demonstrates that the rapid development of deepfake technology has created significant legal, social, and ethical challenges, particularly in the context of cybercrime, privacy violations, and digital misinformation. While deepfake technology offers innovative benefits, its misuse has evolved into a serious transnational threat affecting democracy, security, and individual rights. Through comparative analysis, it is evident that different jurisdictions adopt distinct regulatory approaches. The European Union implements a comprehensive, risk-based framework emphasizing transparency and platform accountability; the United States relies on fragmented, sectoral regulations that prioritize freedom of expression; and China adopts a strict state-centered governance model focusing on platform liability and digital control. Each model presents both strengths and weaknesses in balancing innovation, security, and civil liberties.

In contrast, Indonesia remains in a fragmented regulatory position, lacking a specific and comprehensive legal framework governing deepfake and artificial intelligence technologies. Existing laws such as the ITE Law, PDP Law, and Pornography Law provide only partial solutions and are insufficient to address the complexity of AI-generated harms. This regulatory gap leads to legal uncertainty, weak victim protection, limited law enforcement capacity, and the absence of clear obligations for digital platforms.

Therefore, this study concludes that Indonesia urgently needs to establish a comprehensive and adaptive legal framework for deepfake and AI governance. Such a framework should include clear legal definitions, mandatory labeling of synthetic content, platform accountability mechanisms, strengthened digital forensic capabilities, and victim-oriented protection systems. Additionally, the establishment of a national AI supervisory authority is crucial to ensure effective oversight and coordination. Ultimately, legal reform in this area is essential not only to address current regulatory gaps but also to ensure digital security, uphold human rights, and maintain public trust in the rapidly evolving digital ecosystem.

References

Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. *The State of Deepfakes: Landscape, Threats, and Impact*. (Amsterdam: Deeptrace Labs, 2020). https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

Arifin, Fernando, and Handayani. "Legal Implications of The Second Amendment to The Electronic Information and Transactions Law." *Jurnal Litigasi* 26, no. 1 (2025). https://doi.org/10.23969/litigasi.v26i1.21555.

[75] Min Jiang and Ran Wei, "Deepfake Governance in China: Law, Policy, and Platform Responsibility," Internet Policy Review 12, no. 2 (2023): 1–19, https://doi.org/10.14763/2023.2.1689

Asshiddiqie, Jimly. *Konstitusi dan Konstitusionalisme Indonesia*. (Jakarta : Sinar Grafika, 2021).

Bień-Węgłowska, I. "Deepfakes in the Light of the Artificial Intelligence Act." *Prawo i Wiez* 58(5), (2025): 151–169. https://doi.org/10.36128/4dr67e80.

Carboni, Kevin. "Il Processo per i Deepfake Porno con il Volto di Giorgia Meloni." *Wired Italia*, March 21, 2024. https://www.wired.it/article/giorgia-meloni-deepfake-porno-processo/.

Chesney, Bobby, and Danielle Citron. "Deepfakes and the New Disinformation War." *Foreign Affairs,* 98 (1) (2019): 147–155. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

Citron, Danielle Keats, and Robert Chesney. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753–1820. https://doi.org/10.15779/Z38RV0D15J.

_____. "Sexual Privacy." *Yale Law Journal* 128, no. 7 (2019): 1870–1960. https://www.yalelawjournal.org/article/sexual-privacy.

Creemers, Rogier. "China's Emerging Data Protection Framework." *Journal of Cyber Policy* 7, no. 1 (2022): 1–18. https://doi.org/10.1080/23738871.2021.2008770.

Cyberspace Administration of China. *Provisions on the Administration of Deep Synthesis Internet Information Services*. 2023. http://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm.

de Ruiter, Adrienne. "The Distinct Wrong of Deepfakes." *Philosophy & Technology* 34, no. 4 (2021): 1311–1332. https://doi.org/10.1007/s13347-021-00459-2 .

Delfino, Rebecca. "Pornographic Deepfakes: The Case for Federal Criminalization." *Fordham Law Review* 88, no. 3 (2019): 887–938. https://ir.lawnet.fordham.edu/flr/vol88/iss3/2.

DetikInet. "Penyalahgunaan AI Meresahkan, Kasus Penipuan Deepfake Capai Rp700 M." *Detik.com*, October 24, 2025. https://inet.detik.com/law-and-policy/d-8177140/penyalahgunaan-ai-meresahkan-kasus-penipuan-deepfake-capai-rp-700-m .

Ebers, Martin. "Liability for AI and EU Consumer Law." *Journal of European Consumer and Market Law* 10, no. 5 (2021): 204–209. https://doi.org/10.21552/eur/2021/5/5.

Edwards, Lilian. "Regulating AI in Europe: Four Problems and Four Solutions." *SSRN Electronic Journal* (2024). https://doi.org/10.2139/ssrn.5026691.

European Parliament and Council. *Digital Services Act*. Regulation (EU) 2022/2065. https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

_____. *General Data Protection Regulation*. Regulation (EU) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

_____. *Artificial Intelligence Act*. Regulation (EU) 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

Fernandez, A. "'Deep Fakes': Disentangling Terms in the Proposed EU Artificial Intelligence Act." *UFITA – Archiv für Medienrecht und Medienwissenschaft*, no. 2 (2021): 392–433. https://doi.org/10.5771/2568-9185-2021-2-392.

Finck, Michèle. "Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems." In *The EU Artificial Intelligence Act: A Commentary*, 464–481. (Oxford: Oxford University Press, 2026). https://doi.org/10.1093/law/9780198925705.003.0005.

Franks, Mary Anne. "Deepfakes and the Law." *Fordham Law Review* 89, no. 5 (2021): 1965–1978. https://doi.org/10.2139/ssrn.3852255.

Gils, T. "A Detailed Analysis of Article 50 of the EU's Artificial Intelligence Act." In *The EU Artificial Intelligence (AI) Act*, edited by C. N. Pehlivan, N. Forgó, and P. Valcke, 776–823. Kluwer Law International, 2025. https://doi.org/10.2139/ssrn.4865427.

Hao-Ping Lee, et al. "Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks." *arXiv* (2023): 8–12. https://arxiv.org/abs/2310.0879.

Harsya, Rabith Madah Khulaili. "Tinjauan Yuridis terhadap Tanggung Jawab Platform Digital atas Konten Ilegal Menurut Hukum Indonesia." Sanskara Hukum dan HAM 4, no. 1 (2025): 276–286. https://doi.org/10.58812/shh.v4i01.609 .

Hoffman, Samantha. "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion." *Australian Strategic Policy Institute* (2019): 10–15. https://www.aspi.org.au/report/engineering-global-consent.

Ibrahim, Johnny. *Teori dan Metodologi Penelitian Hukum Normatif*. (Malang: Bayumedia, 2019).

Jiang, Min, and Ran Wei. "Deepfake Governance in China: Law, Policy, and Platform Responsibility." *Internet Policy Review* 12, no. 2 (2023): 1–19. https://doi.org/10.14763/2023.2.1689.

Kapczynski, Amy. "The First Amendment and the Regulation of Disinformation." *Yale Law Journal Forum* 131 (2021): 227–240. https://www.yalelawjournal.org/forum/the-first-amendment-and-the-regulation-of-disinformation.

Keller, Daphne. "Regulating Deepfakes after Generative AI." *Journal of Free Speech Law* 3, no. 2 (2023): 260–271. https://doi.org/10.2139/ssrn.4389686.

Kompas.com. "100 Orang Jadi Korban Penipuan Pakai Video Deepfake Prabowo, Kerugian Capai Rp65 Juta." *Kompas.com*, February 7, 2025. https://nasional.kompas.com/read/2025/02/07/18360001/100-orang-jadi-korban-penipuan-pakai-video-deepfake-prabowo-kerugian-capai.

_____. "Interpol Polri Sebut Banyak WNI yang Kerja di Perusahaan Judi Online hingga Scamming di Kamboja." *Kompas.com*, April 14, 2025. https://nasional.kompas.com/read/2025/04/14/12202301/interpol-polri-sebut-banyak-wni-yang-kerja-di-perusahaan-judi-online-hingga.

Lee, Hao-Ping, et al. "Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks." *arXiv* (2023): 8–12. https://arxiv.org/abs/2310.07879.

Makarim, Edmon. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. (Jakarta: Rajawali Pers, 2020).

Marzuki, Peter Mahmud. *Penelitian Hukum*. (Jakarta: Kencana, 2021)

Maskun. "Kejahatan Siber (Cyber Crime) dalam Perspektif Hukum Indonesia." Jurnal Media Hukum 25, no. 1 (2018): 58–72. https://doi.org/10.18196/jmh.2018.0108.

Nasution, Suteki A. V. A., and A. D. Lumbanraja. "Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse." *International Journal for the Semiotics of Law* 38, no. 7 (2025): 5–11. https://doi.org/10.1007/s11196-025-10265-0.

Nguyen, Thanh Thi, et al. "Deep Learning for Deepfakes Creation and Detection: A Survey." *Computer Vision and Image Understanding* 223 (2022): 103525. https://doi.org/10.1016/j.cviu.2022.103525.

Oktafiana, Hary, and Muhammad Miftah Nurhidayatulloh. "Tanggung Jawab Hukum Platform Digital dalam Mengendalikan Penyebaran Konten Ilegal di Internet." *Jurnal Pendidikan Tambusai* 10, no. 1 (2026): 6776–6781. https://doi.org/10.31004/jptam.v10i1.37260.

Pawelec, Maria. "Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions." *Digital Society* 1, no. 19 (2022): 4–9. https://doi.org/10.1007/s44206-022-00010-6.

Prasetya, M. D., et al. "Subordinate Justice to Forensic Scientists: Indonesia's Authority and Regulation Gap." *Media Iuris* 9, no. 1 (2026): 21–29. https://doi.org/10.20473/mi.v9i1.77587.

Rochaeti, Nur. "Kebijakan Hukum Pidana dalam Penanggulangan Cyber Crime di Indonesia." *Masalah-Masalah Hukum* 49, no. 2 (2020): 136–148. https://doi.org/10.14710/mmh.49.2.2020.136-148.

Rosadi, Sinta Dewi, and Rika Ratna Permata. "Perlindungan Data Pribadi dalam Era Ekonomi Digital di Indonesia." *Veritas et Justitia* 8, no. 1 (2022): 91–112. https://doi.org/10.25123/vej.v8i1.5136.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif*. (Jakarta: Rajawali Pers, 2020).

Solove, Daniel J. "Deepfakes, Privacy, and the First Amendment." *Boston University Law Review* 103, no. 2 (2023): 499–528. https://doi.org/10.2139/ssrn.4303959.

Syamsudin, M. "Perlindungan Hukum terhadap Korban Kejahatan Siber di Indonesia." *Jurnal Hukum IUS QUIA IUSTUM* 28, no. 1 (2021): 1–20. https://doi.org/10.20885/iustum.vol28.iss1.art1.

van der Sloot, Bart, and Yvette Wagensveld. "Deepfakes: Regulatory Challenges for the Synthetic Society." *Computer Law & Security Review* 46 (2022): 9–15. https://doi.org/10.1016/j.clsr.2022.105716.

Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act." *Computer Law Review International* 22, no. 4 (2021): 97–112. https://doi.org/10.9785/cri-2021-220402.

Volokh, Eugene. "Freedom of Speech and Deepfake Regulation." *Journal of Free Speech Law* 1, no. 2 (2021): 221–248. https://www.journaloffreespeechlaw.org/volokh.pdf.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Transparent, Explainable, and Accountable AI for Robotics." *Science Robotics* 2, no. 6 (2017): 1–2. https://doi.org/10.1126/scirobotics.aan6080.

Wiratraman, R. Herlambang Perdana. "Digital Constitutionalism and Freedom of Expression in Indonesia." *Hasanuddin Law Review* 8, no. 2 (2022): 145–160. https://doi.org/10.20956/halrev.v8i2.3600.

Wirianingsih. "Analisis Yuridis Tanggung Jawab Platform Media Sosial terhadap Konten Berbahaya bagi Anak di Indonesia." *Journal Evidence of Law* 5, no. 1 (2026). https://doi.org/10.59066/jel.v5i1.2125.

Yeung, Karen. "A Study of the Implications of Advanced Digital Technologies for the Concept of Responsibility within a Human Rights Framework." *Human Rights Law Review* 19, no. 2 (2019): 257–283. https://doi.org/10.1093/hrlr/ngz007.

Zhang, Lyu. "Regulating Deepfakes in China: A Subject-Based Approach." *Asian Journal of Law and Society* 8, no. 2 (2021): 361–367. https://doi.org/10.1017/als.2021.23.