The Easta Journal Law and Human Rights
Vol. 3, No. 02, February 2025, pp. 101 - 109
ISSN: 2985-7112, DOI: 10.58812/eslhr.v3i02

Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia

Loso Judijanto[1], Andrew Shandy Utama[2], Heri Setiyawan[3]
[1] IPOSS Jakarta
[2] Universitas Lancang Kuning
[3] Sekolah Tinggi Ilmu Ekonomi TRIGUNA Tangerang

Article Info

Article history:

Received Feb, 2025
Revised Feb, 2025
Accepted Feb, 2025

Keywords:

Artificial Intelligence
Deepfakes
Indonesian Law
Legal Ethics
Misinformation Prevention

ABSTRACT

The rapid advancement of artificial intelligence (AI) technologies has introduced new challenges, particularly in the creation and dissemination of deepfakes—manipulated media that can deceive viewers into believing false information. In Indonesia, the existing legal frameworks do not specifically address the issue of deepfakes, leaving a gap in the regulation and prevention of AI-generated misinformation. This paper analyzes the legal application of AI ethics in preventing the misuse of deepfakes, using a normative juridical approach to examine current Indonesian laws, ethical standards in AI, and international legal frameworks. The findings highlight the insufficiency of Indonesia's current legal provisions, including the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law, in addressing deepfake-related issues. The study proposes the introduction of a specific legal framework for deepfakes, integration of AI ethics into national legislation, and international collaboration to mitigate the spread of harmful AI-generated content. By implementing these reforms, Indonesia can better safeguard individuals' rights and maintain digital media integrity.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

The rapid advancement of AI, particularly machine learning (ML) and deep learning (DL), has transformed content creation and consumption across various sectors, enabling hyper-realistic digital media and new opportunities in entertainment, healthcare, and education. Generative AI models, such as ChatGPT, have revolutionized human-machine communication, enhancing productivity in customer service, content creation, and education [1]. AI also automates content marketing, enabling large-scale personalization and real-time strategy optimization for better campaign performance [2]. Additionally, AI-driven digital media fosters personalized experiences and innovation across text, audio, image, and video, benefiting newsrooms, advertising, and entertainment [3]. However, these advancements pose ethical and legal challenges, including algorithmic bias that may lead to unfair outcomes [4]. Ensuring transparency and accountability in AI deployment is essential (Rane et al., 2024), along with addressing data privacy concerns through ethical practices that protect confidentiality [5].

Deepfake technology, powered by AI advancements, threatens digital media integrity and societal trust by creating highly realistic fake videos and audio, making it difficult to distinguish fact from fiction. Its impact extends to media credibility, public perception, and democratic processes, as deepfakes manipulate political narratives, influence voter behavior, and spread propaganda [6]. This technology enables biased campaigns that undermine opposition and sway public opinion [6]. To counteract these risks, AI-driven detection methods like spatial and frequency domain analysis help identify deepfakes [7], while the Blockchain-based Deepfake Authenticity Verification Framework (B-DAVF) offers real-time content authentication to safeguard electoral integrity [6]. Ethically, deepfakes raise concerns over privacy violations and malicious exploitation (-, 2024), further eroding public trust in media [8]. Addressing these challenges requires collaboration among tech companies, governments, and the public [9], supported by stronger legislation, technological safeguards, and public education initiatives [10].

The spread of deepfake disinformation in Indonesia threatens political discourse, social media influence, and public trust by manipulating images and videos to mislead audiences, risking social harmony and stability. The lack of specific legal frameworks worsens the issue, prompting calls for stronger regulations and a multifaceted approach integrating technology, law, and education. AI models like Bidirectional Long Short-Term Memory (BI-LSTM) have shown high accuracy in detecting fake news and can be adapted for deepfake identification, reducing misinformation in critical events like elections [11]. Strengthening detection systems and expanding datasets further enhance their reliability [11]. Legally, Indonesia relies on general data falsification laws, leaving victims unprotected and underscoring the need for explicit regulations [12]. Legal research highlights the necessity of comprehensive laws targeting deepfake-related offenses [13]. Raising public awareness and improving media literacy are also crucial, as education helps individuals recognize synthetic media and combat misinformation [14]. Collaborative efforts across disciplines are essential to enhance digital literacy and critical thinking, empowering the public to differentiate authentic from manipulated content [15]. This paper explores the legal application of AI ethics in Indonesia to prevent the misuse of deepfake technology in spreading disinformation.

2. LITERATURE REVIEW

2.1 Artificial Intelligence and Ethical Implications

The integration of artificial intelligence (AI) across various sectors has driven advancements in automation, decision-making, and content generation but also raises ethical concerns regarding privacy, security, fairness, and accountability. Scholars emphasize the need for ethical guidelines to align AI development with societal values and protect individual rights, focusing on transparency, accountability, and harm prevention to mitigate risks from AI misuse. One major challenge is algorithmic bias, where AI systems trained on biased data can lead to unfair outcomes in hiring, law enforcement, and lending [16]. Privacy concerns also arise due to the vast amounts of data AI systems require, increasing the risk of unauthorized access and misuse in the absence of strong data protection laws [17]. Additionally, AI decision-making processes often lack transparency, making it difficult for users to understand how decisions are made and undermining trust in AI systems [18]. To address these issues, a multidisciplinary approach is essential, incorporating technical and social perspectives to develop responsible AI systems [18]. Establishing comprehensive ethical guidelines emphasizing transparency, accountability, and harm prevention can further ensure responsible AI use [19]. Moreover, implementing robust regulatory frameworks is crucial to safeguarding privacy and ensuring fairness in AI applications [20].

2.2 *Deepfake Technology*

Deepfake technology, powered by AI and machine learning, has revolutionized content creation by enabling highly realistic yet fabricated audiovisual media. While beneficial in entertainment and art, it also poses serious risks, particularly in spreading misinformation and violating privacy. Generative adversarial networks (GANs) facilitate deepfake creation, allowing for the manipulation of images, audio, and video, which can be exploited for misinformation, defamation, and political manipulation. To counter these risks, detection techniques like the MesoNet approach achieve about 90% accuracy in distinguishing real from fake images [8], while deep learning-based algorithms using CNNs and GANs enhance detection, though challenges remain in automation and accuracy [21]. Spatial and frequency domain analysis also play a key role in mitigating deepfake threats [22]. Major concerns include synthetic misinformation that undermines public trust and democracy [22]and privacy violations, especially with non-consensual intimate deepfakes . Public figures, including celebrities[22] and politicians, are particularly vulnerable to deepfake-based defamation and identity theft [23]. Strengthening content moderation is crucial, with social media platforms encouraged to enforce existing policies rather than developing new rules for synthetic content [24].

2.3 *Legal Frameworks for Addressing Deepfakes*

The rise of deepfake technology challenges legal frameworks, particularly in Indonesia, where responses have been slow to adapt. Deepfakes, AI-generated media that mimic real individuals, threaten media credibility and societal trust. Indonesia's Electronic Information and Transactions Law (ITE Law) addresses defamation and misinformation but lacks specific provisions for AI-generated content, limiting its effectiveness [25]. In contrast, the U.S. has enacted laws like the Malicious Deep Fake Prohibition Act of 2018 to criminalize harmful deepfake use [26]. The lack of clear legal definitions complicates enforcement globally [27]. Scholars advocate updating laws to include AI-generated content, ensuring clarity and accountability [28]. Proposed reforms focus on legal categories for deepfakes, transparency, and liability for creators and distributors [10]. Collaborative efforts among governments, tech companies, and civil society are essential for comprehensive regulations [10]. Countries like China and Singapore offer models with legal, ethical, and technological measures to mitigate deepfake risks [26].

2.4 *Ethical Considerations in Regulating AI and Deepfakes*

Ethical considerations are crucial in regulating AI and deepfake technology, as they impact individual rights, privacy, and societal trust. Principles of fairness, transparency, and accountability must guide AI development to mitigate risks such as public manipulation and privacy violations. In Indonesia, balancing freedom of expression with protections against malicious AI-generated content requires a nuanced regulatory approach that respects constitutional rights while addressing ethical concerns. Transparency is vital for accountability in AI systems, allowing scrutiny of decision-making processes [29], with frameworks like the GDPR in the EU serving as benchmarks for data protection and AI transparency [30]. AI can also perpetuate biases, necessitating fairness in development and ethical governance to ensure equitable outcomes [31].

Additionally, AI's ability to process vast datasets poses privacy risks, highlighting the need for stringent data protection aligned with human [32]. The ethical debate on deepfakes revolves around balancing freedom of expression with safeguards against harm, requiring Indonesia's legal measures to protect individuals without infringing on constitutional rights [33].

2.5 *The Role of AI Ethics in Legal Regulation*

Incorporating AI ethics into Indonesia's legal framework can mitigate the risks associated with deepfakes and AI-generated content by ensuring transparency, accountability, and fairness. Ethical AI governance is crucial for responsible development and deployment, emphasizing oversight mechanisms that balance regulation and self-regulation [34]. The European Union's GDPR serves as a model for data protection, demonstrating the need for accountability and transparency in AI operations [35]. Different regions adopt varied regulatory approaches, blending government oversight with market-driven innovation to create adaptable frameworks [31]. Ethical AI frameworks, such as the Ethical Artificial Intelligence Framework Theory (EAIFT), advocate for real-time oversight, open decision-making, and bias detection to ensure ethical AI use [36]. The establishment of "ethical AI watchdogs" and compliance algorithms can further enhance accountability and regulatory adaptation [36]. Additionally, mitigating bias and ensuring transparency remain critical, requiring organizations to implement strategic recommendations that uphold ethical principles in AI deployment [37].

3. RESEARCH METHODS

3.1 *Research Design*

The research had adopted a qualitative research design, focused on legal texts, policies, and ethical frameworks analysis. Qualitative research is especially suitable in this kind of normative juridical analysis because it emphasizes the interpretation of laws and the examination of available frameworks and their efficiency to regulate AI-generated content. This gives clear ideas about how law, technology, and ethics amalgamate to allow the modification of legal norms to tackle the emerging challenges thrown up by technology.

3.2 *Data Collection*

Information to aid this research will be found in legal documents, academic literature reviews, case studies from an international perspective, and interviews with experts. Legal ground for this paper, among others, will refer to Indonesia's ITE Law, the Personal Data Protection Law, and other statutes related to the regulation of digital content, and some international frameworks, namely the General Data Protection Regulation and the US Malicious Deep Fake Prohibition Act. A literature review is needed on the ethics of AI, deepfake technology, and digital misinformation as well as the legal regulations by Indonesian and international scholars. International case studies of countries that have deepfake regulations will be analyzed to find best practices that could be applied in Indonesia. If possible, interviews with legal experts, policymakers, and AI ethics experts will provide insight into Indonesia's AI regulatory landscape: how effective current laws are and what reforms are needed.

3.3 *Data Analysis*

Legal analysis will be done in a few steps: first, to find loopholes that exist in Indonesian law concerning AI and deepfake technology. This covers the examination of the adequacy of existing legal frameworks, such as the ITE Law, to deal with digital content manipulation, misinformation, and unethical use of AI in, among other things, defamation cases, misinformation, and violation of privacy. This will be followed by an ethical evaluation, which will explain whether

Indonesia's legal system applies ethical principles like transparency, accountability, fairness, and privacy and if it includes or may apply international AI ethics standards set forth by organizations like the OECD and IEEE. A comparative analysis will then explore international legal frameworks, focusing on the legislative measures taken within the United States, the European Union, and Australia to identify best practices that can be adapted for Indonesia's legal, social, and technological contexts. Finally, this study will put forward a set of proposals on legal reform by providing substantial definitions of deepfakes, regulatory measures regarding disinformation, and ethical guidelines toward responsible AI development. Some of the recommendations would strive to balance individual rights protection, such as those of privacy and freedom of expression, against the need to mitigate the risks of AI-generated content.

4. RESULTS AND DISCUSSION

4.1 Current Legal Frameworks in Indonesia

The ITE Law of Indonesia, Law No. 11 of 2008 as amended by Law No. 19 of 2016, is the leading legal framework for regulating digital content in Indonesia, including misinformation. This law criminalizes a wide range of online offenses, such as defamation, hate speech, and the spread of false information. Article 27 prohibits the dissemination of information that can cause damage or insult to others, thus giving a legal avenue for victims of misleading content. Although the law does take care of misinformation, it does not particularly take into consideration deepfake technology, which relies on AI to create highly believable but completely fabricated video and audio content. While deepfakes could fall under general misinformation and defamation provisions, their novelty in manipulating digital content is actually not regulated; hence, there is a lacuna in the law, making enforcement and accountability difficult.

The ITE Law, especially through Articles 27, 28, and 29, was enacted to deal with online crimes like defamation and misinformation. However, all these articles are viewed as multi-interpretable, hence are under appeal for revision to remove ambiguities and provide more clarity to the law [38]. While the law is often applied to regulate false news and defamation, it is still unsure whether deepfakes would fall under its ambit due to the lack of clear provisions related to digital manipulation of content [39]. Moreover, the broad scope of the ITE Law has raised concerns regarding its impact on freedom of expression, as its vague language can be used to limit democratic values [38] . At the same time, the dissemination of false information, including deepfakes, poses serious risks to political and social stability, highlighting the need for a balance between regulation and free speech [40].

With these challenges, legal revisions have to be developed to accommodate the intricacy of deepfake technology. Of course, existing laws cannot satisfactorily represent the technological nuisances that deepfakes creation and dissemination; the call for updated regulations therefore comes into view [41]. Many scholars and policy makers call for government special laws around digital content manipulation that will eventually allow legal frameworks to catch up with the advancing technology [42]. Perhaps a more balanced legal framework will go a long way toward lessening some of the deepfake risks without inhibiting freedom of expression or protecting individuals from harm resulting from AI-generated misinformation.

Indonesia's Personal Data Protection Law, Law No. 27 of 2022, provides protection against the misuse of personal data, especially in the use of digital platforms. The law protects consent, transparency, and accountability in processing personal data. Given that deepfakes are, more often than not, used without permission, personal data protection may also be applied where deepfake content infringes on any person's right to privacy or misappropriates their identity.

Meanwhile, similar to ITE Law, deepfakes are not specifically dealt with under the Personal Data Protection Law either, and it is not very clear how it shall be applied to AI-generated content. This law was more focused on data protection in the traditional contexts of database management and online transactions, thus leaving a gap in the regulation of AI technologies that create deepfakes and other related harms.

A review of international legal frameworks reveals several approaches to addressing the challenges of deepfakes and AI-generated content. For example, in the United States, the Malicious Deep Fake Prohibition Act of 2018 explicitly criminalizes the creation and distribution of deepfakes intended to harm individuals or influence political processes. Similarly, the General Data Protection Regulation by the European Union provides a strong framework on data protection that could be applied to deepfakes using personal data to create deceptive content.

While existing Indonesian legal frameworks address deepfakes, none possesses the required specific detail needed in addressing this emerging challenge. More important is a set of regulatory imperatives due to its very nature and presumed implications for society and individual beings.

4.2 *Ethics Issues Related to AI and Deepfake Technologies*

International ethical frameworks through organizations such as OECD and IEEE emphasize key principles in AI ethics: transparency, accountability, fairness, and the protection of human rights. The same is much relevant in this context, in which AI-generated content has enormous potential to be manipulated with a view to misleading or deceiving viewers and damaging trust in digital platforms.

The country has no comprehensive national framework on AI ethics, and the legal provisions are not broad enough to embrace the ethical issues thrown up by AI technologies. While Indonesia is actively exploring AI development, the country does not incorporate ethical considerations into its laws and regulations. The absence of clear guidelines on ethical usage has created a vacuum in the responsible and ethical handling of AI technologies, including deepfakes.

Another important ethical challenge with deepfakes is the difficulty in source identification and accountability due to manipulated content. Deepfake technology enables seamless replication of a person's image and voice to such an extent that most of this content would appear to viewers as indistinguishable from reality. This is a serious cause for concern in light of eroding levels of trust in digital media and the potential for harm in many contexts, including, but not limited to, politics, media, and personal relationships.

Many challenges arise here, and for the same, much emphasis on the AI ethics frameworks is made on the transparency of the AI systems, including disclosing the use of AI-generated content by both the users and the creators. Equally important is the mechanism for accountability to make those liable who create and/or disseminate any harmful deepfakes.

4.3 *Gaps in Indonesia's Legal System*

The legislation in force does not govern this issue of deepfakes in Indonesia. From the foregoing discussions, a fair amount of protection is derived both from the ITE Law and from the Personal Data Protection Law; however, each of them, in itself, is not relevant to this form of expression as these respective laws never foresaw the peculiar challenge presented by this AI technology named deepfakes. Lacking a definition by law about deepfakes creates a loophole regarding regulation and the punishment of abusing AI in malicious or hazardous creation.

There is a noticeable lack of a comprehensive AI ethics framework in Indonesia. While AI development is growing rapidly in the country, the absence of clear ethical guidelines for AI use leaves room for abuse and misuse of technologies like deepfakes. Without ethical oversight, AI creators and users are not held to the same standards as other technological innovations, which could result in significant harm to individuals, society, and the integrity of the media.

4.4 *Proposed Legal Reforms*

It is suggested that specific Indonesian legislation on making, disseminating, and utilizing deepfakes, including a legal definition of deepfakes, be put in place regarding criminalizing an act of making and disseminating deepfakes with the intent to deceive or cause harm to any person. Drawing on international experiences, such as the Malicious Deep Fake Prohibition Act of the U.S., Indonesia might develop a legal framework that would balance free speech with protection from the negative consequences of AI-generated content.

Indonesia may consider incorporating the principles of AI ethics into its national legal framework. It may provide a national code on AI ethics relating to transparency, accountability, and fairness. Norms of the ethics of AI development need to be brought into statute to make sure that AI technologies, including deepfakes, are responsibly used without causing harm to an individual or society.

Indonesia may be enlightened on the collaboration with international organizations like the OECD and IEEE on how other countries are setting legal and ethical frameworks on AI ethics. It will ensure that Indonesia's legal steps to deal with deepfakes borrow from international standards and contribute to global efforts toward the ethical implications of AI technologies.

5. CONCLUSION

This paper concludes that Indonesia's current legal system is not specific to deal with the challenges thrown up by deepfakes and AI-generated misinformation. Current laws, such as the ITE Law and Personal Data Protection Law, generally guard against online harms but are in essence inadequate in their reach about deepfakes. The study thus calls for specific legislation that squarely addresses the creation and distribution of deepfakes, with explicitly stated penalties and definitions. Furthermore, embedding the principles of ethics in AI into national laws will ensure that AI technologies are developed and applied responsibly to retain public trust in digital media. Finally, collaboration with international bodies and alignment with global ethical standards will further strengthen Indonesia's legal framework and provide a comprehensive approach to mitigating the risks associated with deepfakes and other AI-generated content.

REFERENCES

[1] I. A. Aram and E. A. Juliana, "Digitisation and artificial intelligence in the world of media," 2024.

[2] N. L. Rane, Ö. Kaya, and J. Rane, *Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0*. Deep Science Publishing, 2024.

[3] V. Nadda, P. K. Tyagi, A. Singh, and V. Singh, *Integrating AI-Driven Technologies Into Service Marketing*. IGI Global, 2024.

[4] N. L. Rane, S. K. Mallick, O. Kaya, and J. Rane, "Role of machine learning and deep learning in advancing generative artificial intelligence such as ChatGPT," *Appl. Mach. Learn. Deep Learn. Archit. Tech.*, pp. 96–111, 2024.

[5] B. T. L. S. Shepherd and A. A. Jacob, “A Detailed Investigation on Digital Technology and AI in Social Sectors,” in *Future of Digital Technology and AI in Social Sectors*, IGI Global, 2025, pp. 33–62.

[6] S. Ghodke, “Ethical Implications of Deepfake Technology,” vol. 6, no. 5, pp. 2019–2021, 2024.

[7] M. Momeni, “Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation,” *J. Creat. Commun.*, p. 09732586241277335, 2024.

[8] J. P. Cardenuto *et al.*, “The age of synthetic realities: Challenges and opportunities,” *APSIPA Trans. Signal Inf. Process.*, vol. 12, no. 1, 2023.

[9] M. B. E. Islam, M. Haseeb, H. Batool, N. Ahtasham, and Z. Muhammad, “AI threats to politics, elections, and democracy: a blockchain-based deepfake authenticity verification framework,” *Blockchains*, vol. 2, no. 4, pp. 458–481, 2024.

[10] C. Gilbert and M. A. Gilbert, “The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation,” *Int. Res. J. Adv. Eng. Sci. (ISSN 2455-9024)*, vol. 9, no. 4, pp. 170–181, 2024.

[11] A. V. A. Nasution, S. Suteki, and A. D. Lumbanraja, “Prospek Pemenuhan Right To Be Forgotten Bagi Korban Deepfake Pornography Akibat Penyalahgunaan Artificial Intelligence Di Indonesia,” *Diponegoro Law J.*, vol. 13, no. 2, 2024.

[12] H. Chemerys, “Zaporizhzhia, Ukraine Anyta. Chemeris@ gmail. com Deepfakes As A Problem Of Modernity: A Brief Overview And Current State,” *Науковий журнал Хортицької національної академії.(Серія Педагогіка. Соціальна робота) наук. журн./[редкол. ВВ Нечипоренко (голов. ред.) та ін..]. Запоріжжя Вид-во комунального закладу вищої освіти «Хортицька національна навчально-реабілітаційна академ*, p. 162, 2023.

[13] L. Noor, I. Malahat, and H. Noor, “The Socio-Political Implications of Deepfakes in Developing Countries,” *Available SSRN 4963439*, 2024.

[14] C. T. Noerman and A. L. Ibrahim, “Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara,” *J. USM Law Rev.*, vol. 7, no. 2, 2024.

[15] S. G. Arkaan, A. R. Atmadja, and M. D. Firdaus, “Fake news detection in the 2024 Indonesian general election using Bidirectional Long Short-Term Memory (BI-LSTM) algorithm,” *Fake news Detect. 2024 Indones. Gen. Elect. using Bidirectional Long Short-Term Mem. algorithm*, vol. 21, no. 2, pp. 22–30, 2024.

[16] S. Murugesan, “Application of AI to real-time intelligent attitude control of spacecraft,” in *Proceedings. IEEE International Symposium on Intelligent Control 1989*, 1989, pp. 287–292.

[17] R. Suryawanshi, K. Chatrapathy, A. Al-Khaykan, W. D. Priya, C. V. K. Reddy, and K. V. S. Prasad, “Decomposition of electrical and electronic waste management by using artificial intelligence,” in *2023 Seventh International Conference on Image Information Processing (ICIIP)*, 2023, pp. 411–416.

[18] A. I. Almulhim, A. Al Kafy, M. N. Ferdous, M. A. Fattah, and S. R. Morshed, “Harnessing urban analytics and machine learning for sustainable urban development: A multidimensional framework for modeling environmental impacts of urbanization in Saudi Arabia,” *J. Environ. Manage.*, vol. 357, p. 120705, 2024.

[19] N. Luhmann, “Je vois quelque chose que tu ne vois pas,” *Trivium*, no. 20, pp. 0–6, 2015, doi: 10.4000/trivium.5151.

[20] N. Constantin, R. Nelwin, and A. Christanto, “Artificial Intelligence: Communication, Technology, and Society (a Systematic Literature Review).,” *J. Indones. Sos. Teknol.*, vol. 5, no. 10, 2024.

[21] A. Jagdale, V. Kubde, and R. Kortikar, “DeepFake Image Detection : Fake Image Detection using CNNs and GANs Algorithm,” pp. 1–10, 2024, doi: 10.55041/IJSREM38628.

[22] S. A. Fisher, J. W. Howard, and B. Kira, “Moderating synthetic content: The challenge of generative AI,” *Philos. Technol.*, vol. 37, no. 4, p. 133, 2024.

[23] A. K. Win, M. M. Hein, C. H. Lwin, A. M. Thu, M. M. Thu, and N. Y. Khaing, “A Novel Methodology for Deepfake Detection Using MesoNet and GAN-based Deepfake Creation,” in *2024 5th International Conference on Advanced Information Technologies (ICAIT)*, 2024, pp. 1–6.

[24] D. Ghiurău and D. E. Popescu, “Distinguishing Reality from AI: Approaches for Detecting Synthetic Content,” *Computers*, vol. 14, no. 1, p. 1, 2024.

[25] K. Qureshi, “A Multidisciplinary Threats to Emerging Cybersecurity, Legal and Ethical Threats Posed by Deepfake Technology,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. 9.

[26] Т. В. Епифанова and К. И. Копейкин, “Проблемы законодательного регулирования объектов, созданных с использованием дипфейк-технологии в России и за рубежом,” *Северо-Кавказский юридический вестник*, no. 3, pp. 121–128, 2024.

[27] A. K. Sharma and R. Sharma, “Generative Artificial Intelligence and Legal Frameworks: Identifying Challenges and Proposing Regulatory Reforms,” *Kutafin Law Rev.*, vol. 11, no. 3, pp. 415–451, 2024.

[28] F. Lu, “AI-Generated Content: Legal Challenges & Potential Reforms,” *Lect. Notes Educ. Psychol. Public Media*, vol. 66, pp. 174–181, 2024.

[29] R. H. A. Barreto, C. C. M. Jaborandy, and C. S. Porto, “Ethical Challenges Of Artificial Intelligence In The Light Of Human Rights,” *Interfaces Científicas-Humanas e Sociais*, vol. 12, no. 2, pp. 314–326, 2024.

[30] Y. Deng, “AI and Ethics: Moral Considerations of Automated Rumor Detection Technology,” *Commun. Humanit. Res.*, vol. 47, pp. 123–126, 2024.

[31] P. Kashefi, Y. Kashefi, and A. Ghafouri Mirsaraei, “Shaping the future of AI: balancing innovation and ethics in global regulation,” *Unif. Law Rev.*, vol. 29, no. 3, pp. 524–548, 2024.

[32] M. Sahoo, “Ethics in AI–Critical Skills for the New World,” in *Abu Dhabi International Petroleum Exhibition and Conference*, 2024, p. D021S056R002.

[33] M. A. Fadhlurrahman, S. Riyanta, and A. R. Ras, "The Role of Competitive Intelligence in Strategic Decision-Making: A Literature Review," *Asian J. Eng. Soc. Heal.*, vol. 3, no. 10, pp. 2307–2324, 2024.

[34] A. Todupunuri, "Artificial intelligence ethics: Investigating ethical frameworks, bias mitigation, and transparency in AI systems to ensure responsible deployment and use of AI technologies," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 13, no. 09, pp. 10–15680, 2024.

[35] R. Ejjami, "The Ethical Artificial Intelligence Framework Theory (EAIFT): A New Paradigm for Embedding Ethical Reasoning in AI Systems".

[36] M. H. Hadi and A. A. Jasim, "Legislative and Ethical Foundations for Future Artificial Intelligence," *J. Coll. Basic Educ.*, vol. 30, no. 126, pp. 127–145, 2024.

[37] S. Duggineni, "Journal of Artificial Intelligence & Cloud Computing," *J. Artif. Intell. Cloud Comput.*, vol. 1, no. 4, pp. 1–7, 2024.

[38] I. Rosyadi, "Criminal Liability Against Perpetrators of HOAX Spread in Indonesia," *Int. J. Law Dyn. Rev.*, vol. 1, no. 1, pp. 41–53, 2023.

[39] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *J. Cakrawala Ilm.*, vol. 2, no. 10, pp. 3799–3806, 2023, doi: 10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

[40] R. Manthovani, "Dampak Berita Hoax Terhadap Keamanan Negara Dalam Perspektif Cyberlaw Bela Negara," *J. Magister Ilmu Huk. Huk. dan Kesejaht.*, vol. 8, no. 2, pp. 14–34, 2023.

[41] D. Haspada, A. Mauluddin, D. Z. Santana, and W. Kusnaedi, "Mitigasi Pelanggaran Hukum Penggunaan Media Sosial Melalui Teknologi Informasi," *J. Pengabdi. Tri Bhakti*, vol. 5, no. 2, pp. 94–98, 2023.

[42] A. Afisa, Z. Qodir, A. Habibullah, and U. Sugiharto, "Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia," *J. Soc. Media*, vol. 8, no. 2, pp. 424–444, 2024.