A Comparative Legal Analysis of Deepfake Transparency: Contrasting Indonesia'sAbsence of Law with China's Legislative Approach

Marvell Limiardo, Lewiandy
Tarumanagara University, Jakarta, Indonesia
E-mail: marvell205220042@stu.untar.ac.id, lewiandy@fh.untar.ac.id[2]

Abstract

AI-generated deepfakes pose a clear global threat, undermining public trust and individual dignity through geopolitical disinformation and fraud, a trend now manifesting in Indonesia. This article's objective is to comparatively analyze Indonesia's "vacuum of law" (recht vacuum), which relies on outdated general statutes, against China's proactive "AI Labelling Law". Employing a normative legal research method with a descriptive-analytical approach , the study finds that Indonesia operates in a functional legal vacuum, lacking foundational legal definitions for "AI" or "deepfake" and relying on a "fundamentally unfit" EIT Law that creates a severe "accountability gap". In stark contrast, China's law mandates a comprehensive dual-labeling system (explicit and implicit) with clear obligations for providers and users, enforcing its "cyber sovereignty" doctrine. This research contributes a critical case study of reactive versus proactive regulation, presenting the technical mechanisms of China's law as a potential "technical blueprint" for Indonesia, while also serving as a "cautionary tale" regarding its state-centric ideology.

Keywords: *Deepfake, AI Transparency, Legal Vacuum, Comparative Law*

Introduction

Artificial Intelligence **"AI"**- generated deepfakes have emerged as a clear and present global danger, evolving from a theoretical risk into a scalable tool for malicious deception.[1] Major advancements have been made in key domains pertaining to those fields of computer vision, large language models in regards to AI, as well as speech recognition.[2] The maturity of these fields has catalyzed revolutionary breakthroughs in diverse applications, from autonomous systems and logistics to medical diagnostics and interactive personal assistants.[3] A major consequence of these AI advancements is the creation of images and videos. This has spurred the growth of synthetic media, which is content created

[1]Aftab Arif, et al., "An Overview of Cyber Threats Generated by AI", *International Journal of Multidisciplinary Sciences and Arts*, Volume 3 Issue 4 (2024), hlm. 68.

[2] Eva Hariyanti, et al., "Implementations of Artificial Intelligence in Various Domains of IT Governance: A Systematic Literature Review", *Journal of Information Systems Engineering and Business Intelligence/Journal of Information Systems Engineering and Business Intelligence* , Volume 9 Issue 2 (2023), hlm. 306.

[3]Akhil Cherian Jacob, et al., "Ai Based Virtual Personal Assistant", *International Journal of Innovative Science and Research Technology*, Volume 9 Issue 6 (2024), hlm. 2460.

by AI and Machine Learning techniques.[4] A technology known as "deepfake" has surfaced within the realm of synthetic media.[5] This application is different because it's defined less by its technical complexity and more by the intention behind it. A renowned dictionary had provided a definition where, a deepfake is "A video or sound recording that replaces someone's face or voice with that of someone else, in a way that appears real." [6]

"Deepfake" is thus understood as the malicious application of synthetic media to create hyper-realistic content purely for deception.[7] By fabricating convincing scenarios of real people doing or saying things that never occurred, malicious intent becomes a core component of the term. This inherently deceptive nature makes deepfakes a clear and alarming weapon for misinformation, threatening both personal reputations and public trust. This threat is no longer theoretical but is made practical and scalable by our digital environment.[8] A convincing deepfake requires the AI to learn from a vast amount of personalized data to successfully mimic its target.

The dangers of deepfakes became clear in February 2022, when a fake video of President Volodymyr Zelenskyy informing his troops to raise the white flag was spread during the Russian invasion.[9] This was a prime example of a deepfake being used for its defining, malicious purpose: political disinformation.[10] Michael Grothaus, an author who writes about deepfakes, described a video that showed him robbing a cyclist at gunpoint. He stated that even though the video looked real, the event was completely fabricated.[11] Fransesca also noted that deepfakes are now a problem in court. She pointed to a UK custody case where fake audio was used to make a father sound threatening.[12] This shows why it is so important to verify that all digital evidence in a trial is real. These examples illustrate the alarming potential of deepfakes, and with some reports estimating a 900% annual increase in online deepfake videos, the scale of the thread is rapidly growing.[13]

---

[4] Cihan Orak and Zeynep Turan, "Using Artificial Intelligence in Digital Video Production: A Systematic Review Study", *Journal of Educational Technology and Online Learning*, Volume 7 Issue 3 (2024), hlm. 289.

[5] Pooja Kaushik, et al., "Financial Fraud and Manipulation: The Malicious Use of Deepfakes in Business", *Advances in Business Information Systems and Analytics Book Series*, Volume 1 Issue 1 (2024), hlm. 174.

[6] Cambridge Advanced Learner's Dictionary & Thesaurus, "Deepfake", Cambridge University Press, <https://dictionary.cambridge.org/dictionary/english/deepfake>, accessed on 20 August 2025.

[7] Francesca Palmiotto, "Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective", SSRN (2023),<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384122>, accessed on 20 August 2025

[8] William Easttom, "Deepfake Technology: Emerging Threats and Security Implications", *International Conference on Cyber Warfare and Security*, Volume 20 Issue 1 (2025), hlm. 85.

[9] Atul Alexander, "Crisis and General International Law: Lessons from The Russia-Ukraine Conflict", *Indonesian Journal of International Law*, Volume 21 Issue 1 (2023), hlm. 1-2.

[10] Dylan Desjardins, "Possibilities & Perils of Deepfake Technology", T*he George Washington University Regulatory Studies Center*, Volume 1 Issue 1(2022), hlm. 1.

[11] Francesca, *Op. Cit.*, hlm.4.

[12] *Ibid*.

[13] Accelerated Capability Environment Division, "Innovating to detect deepfakes and protect the public", Gov.UK Press (2025), <https://www.gov.uk/government/case-studies/innovating-to-detect-deepfakes-

Within Indonesia, this global threat has manifested with local urgency. Reports indicate the rising use of deepfakes for political disinformation, public scams, and the creation of non-consensual pornographic content, which leverages the digital footprint of individuals to cause profound reputational and psychological harm.[14] The capacity to fabricate reality with such precision and scale poses a direct threat to individual dignity, public trust, and the very integrity of the information ecosystem.[15]

Confronting the pervasive threat of synthetic media misinformation requires a fundamental intervention. The central challenge is that it is hard to distinguish artificial content from reality, so an effective strategy must begin with reliable AI-detection systems.[16] The UK government has also stated that detecting deepfakes is crucial for public protection. Once detected, the next step is to implement clear and consistent labeling requirements to inform viewers of the content's artificial origin.[17] This framework of detection and disclosure is a foundational step in equipping people to critically evaluate media and in preserving the integrity of information.

In line with the need of transparency, the clear, unambiguous, and verifiable identification of synthetic content, has emerged as the essential first line of legal and ethical defense.[18] Contrasting with Indonesia, the Cyberspace Administrative body of China **"CAC"**, with the issued Measures for the Labelling of AI-generated content **"China's AI Labelling Law"** took transparency as a core principle, aiming to combat the rise of misinformation and deepfakes by ensuring users can clearly identify when content is generated or manipulated by machines.[19] By mandating disclosure, legal frameworks can strengthen the possibility of tracing some if not most of the AI-generated content, thus it will be able to restore a degree of informational equilibrium, and allow viewers to apply necessary skepticism to content that is not authentic.[20]

This article presents a comparative analysis of two diametrically opposed regulatory philosophies for achieving such transparency. On one side stands Indonesia, a jurisdiction

---

and-
protect-the-public>, accessed on 28 October 2025.

[14] Abdillah Satari Rahim, et al., "Identify Cyber Intelligence Threats in Indonesia", *International Journal of Humanities Education and Social Sciences*, Volume 3 Issue 1 (2023), hlm. 432.

[15] Agus Permana, "Indonesia's Cyber Defense Strategy in Mitigating the Risk of Cyber Warfare Threats", *Syntax Idea,* Volume 3 Issue 1 (2021), hlm. 7.

[16] Heike Felzman, et al., "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics*, Volume 26 Issue 6 (2020), hlm. 3337-3339

[17] Accelerated Capability Environment Division, *Op.Cit.*

[18] Ville Aula and Tero Erkillä, *Handbook on Public Policy and Artificial Intelligence*, England: Edward Elgar Publishing (2024), hlm 2-7.

[19] Mimi Zhou and Lu Zhang, "Navigating China's regulatory approach to generative artificial intelligence and large language models", *Cambridge Forum on AI: Law and Governance,* Volume 1 (2025), hlm.2.

[20] Irina A. Filipova, "Legal Regulation of Artificial Intelligence: Experience of China", *Journal of Digital Technologies and Law*, Volume 2 Issue 1 (2024), hlm. 52.

grappling with a "vacuum of law" (*recht vacuum*),[21] where a novel and potent technological threat is being met with outdated, general-purpose legal instruments that are ill-suited for the task.[22] On the other side is China, a jurisdiction that has responded with a swift, prescriptive, and comprehensive legislative mandate, reflecting a philosophy of proactive state control over the digital information ecosystem.[23] This juxtaposition frames the analysis not merely as a comparison of two national legal systems, but as a critical case study on the broader global debate between reactive, analogical legal traditions and proactive, state-centric governance models in the regulation of emerging technologies.[24]

Method

The study is a type of normative legal research, which utilizes legal sources like regulations, legal principles, theories, and expert opinions. The analysis is descriptive, meaning it aims to describe the research subject and object to connect legal regulations with the issues being studied. Furthermore, this research will analyze the regulatory differences regarding AI-generated deepfakes between Indonesia and China. The approaches used are the normative (statute) approach and the comparative approach. The normative approach involves examining all relevant regulations, while the comparative approach analyzes legal comparisons between countries. In this study, the author will compare Indonesia and China on their AI-generated deepfake regulations. The study will use an inductive analysis approach where the text will be defined through an inductive reasoning as progressing from specific observations to broader generalizations, such as using specific findings to derive a general understanding. In this case, the author will use this inductive method to examine regulatory differences. By first analyzing specific frameworks, policies, and case studies from both Indonesia and the China, this research will identify key challenges and divergences in their approaches.

Discussion

1. Anatomy of a Regulatory Void in Indonesia: Digital Lawlessness

Indonesia's approach to AI-generated deepfakes constitutes a functional legal vacuum (*recht vacuum*), creating a digital "state of nature" where deception can proliferate with

[21] Chandra Maharani, et al., "Legal Vacuum Regarding Licensing Regulations for Constructing Flats in the Regions", *Jurnal Pranata Hukum*, Volume 19 Issue 1 (2024), hlm. 29.

[22] Muhammad Najiib Al Fithri and Ery Agus Priyono, "Issues and Possibilities in Regulating Artificial Intelligence (AI) Related To Copyright in Indonesia", *International Journal of Social Science and Human Research*, Volume 7 Issue 6 (2024), hlm. 4152-4152.

[23] Baiyang Xiao, "Agile and Iterative Governance: China's Regulatory Response to AI", *Social Science Research Network*, (2025), hlm. 1.

[24] Topo Santoso, "Comparative Law in the Faculty of Law, University of Indonesia: Course Content and Teaching Methods", *Asian Journal of Comparative Law*, Volume 14 (2019), hlm. 15.

impunity.[25] This void is defined by the absence of a dedicated, binding legal framework for AI and a critical definitional gap in primary legislation. While policy documents like the National AI Strategy 2020-2045 issued by the Indonesian Agency in regards to both the Assessment and Application of Technology[26] **"IAAAT"** and Ministry of Communications and Informatics **"MOCI"** Circular Letter No. 9 of 2023 exist,[27] they are non-binding ethical guidelines, not enforceable law. Crucially, there is no formal legal definition for "AI" or "deepfake" in any statute, a foundational obstacle that creates ambiguity for law enforcement and cripples the state's ability to regulate synthetic media effectively.

In this regulatory void, the legal system defaults to applying pre-existing general statutes, principally Law No. 11 of 2008 in regards to both Electronic Information as well as Electronic Transactions **"Informatics Law"** However, this law is fundamentally unfit for regulating deepfake technology.[28] An article-by-article critique reveals its shortcomings: Article 27(1) on immorality is too narrow for non-sexual deepfakes and focuses on distribution, not creation; Articles 27(3) & 27A on defamation face high evidentiary hurdles in proving criminal intent (*mens rea*); and Article 28(1) on misinformation is limited to cases causing "consumer losses," rendering it ineffective against political or social manipulation. The UU ITE was designed for a different technological era, and applying it to generative AI is an exercise in inadequate legal analogy.

The law's inadequacy is compounded by the legal fiction of classifying AI as an "electronic agent."[29] This concept was designed for deterministic systems, like an e-commerce checkout, where actions are predictable and directly controlled by an operator. Generative AI, however, is autonomous and produces novel, often unforeseeable outputs. Equating a deepfake model with a simple "electronic agent" is a category error that obscures the complex chain of agency between the model's developer, its operator, and the end-user. This misclassification creates a severe accountability gap, making it nearly impossible to properly allocate legal responsibility for harmful AI-generated content.

Ultimately, this legal vacuum is a symptom of Indonesia's reactive regulatory culture, which consistently applies outdated legal frameworks to new technological harms after they

[25] Aabid Majeed Sheikh, et al., "Thomas Hobbes' views on Philosophy, State of Nature and International Relations", *International Journal of Humanities and Education Development*, Volume 2 Issue 1 (2020), hlm. 40.

[26] Satria Ardhi, "AI Tidak Terlepas dari Berbagai Aktivitas Masyarakat, Kominfo Siap Luncurkan Panduan Etik Penggunaan AI", Gadjah Mada University Press (2023), < https://ugm.ac.id/id/berita/ai-tidak-terlepas-dari-berbagai-aktivitas-masyarakat-kominfo-siap-luncurkan-panduan-etik-penggunaan-ai/>, accessed on 1 November 2025.

[27] Winnie Yamashita Rolindrawan, "Regulation of Artificial Intelligence in Indonesia", SSEK Press (2024), <https://ssek.com/blog/indonesia-law-update-regulation-of-artificial-intelligence/>, accessed on 2 November 2025.

[28] Abdul Aziz Pamungkas, et al., "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity", *Pena Justicia*, Volume 24 Issue 2 (2025), hlm. 4570.

[29hlm] Meirza Aulia Chairani, et al., "The Urgency of Developing Law as A Legal Basis for The Implementation of Artificial Intelligence in Indonesia", *Journal of Law and Justice*, Volume 7 Issue 1 (2022), hlm. 37

emerge.[30] This approach is ill-equipped for the exponential pace of digital disruption and contrasts sharply with a proactive model that anticipates future challenges. The deepfake phenomenon demands a forward-looking, specific, and technically informed legal response. Instead, Indonesia has responded with tools from a pre-generative AI era.[31] The failure to mandate deepfake transparency is a critical case study illustrating the urgent need for the Indonesian legal system to transition from a reactive to a proactive model of governance capable of shaping, rather than merely reacting to, technological innovation.

2. Blueprint for Reform: China's Architecture of Mandated Transparency

In stark contrast to Indonesia's regulatory inertia, China has responded to synthetic media with decisive action through its China's AI Labelling Law effective September 1, 2025.[32] This regulation was issued by China's CAC, the Ministry for Industrial and Informative Technology of China, The Ministry of Public Security of China, and China's State Administration of Radio and Television.[33] This regulation is a direct implementation of China's state doctrine of "cyber sovereignty," which purports the state's absolute right to govern the internet within its borders, prioritizing national security and social stability. With this new regulation, China is giving relevant entities about six months to prepare for compliance after its effective date on September 1, 2025.[34]

The core of the regulation is a mandatory dual-labeling system designed for both public awareness and state traceability.[35] First, it requires explicit labeling, which will be added to AI-generated content or in other interactive scenes as per deemed necessary through the forms of text, sound, or image which should be easily perceived by users,[36] as such:

1. Text - Add text or general symbol labels at appropriate positions at the beginning, end, or middle of the text, or add prominent labels at the interface of interactive scenes or around the text.

[30] Alzet Rama, et al., "Legal gaps in indonesia's electronic information and transactions law in addressing deepfake technology: challenges and regulatory recommendations", *Indonesian Journal of School Counseling*, Volume 10 Issue 2 (2025), hlm. 203.

[31] Adnasohn Aqilla Respati, "Reformulasi Undang-Undang ITE terhadap *Artificial Intelligence* Dibandingkan dengan Uni Eropa dan China AI Act Regulation", *Jurnal USM Law Review*, Volume 7 Issue 3 (2024) hlm. 1740.

[32] Matt Shenan, *China's AI Regulations and How They Get Made*, United States: Carnegie Endowment For International Peace (2023), hlm. 4.

[33] Qingle Hu and Wei Liu, "The Regulation of Artificial Intelligence in China", *International Conference on Social Sciences and Humanities and Arts*, Volume 3 (2024), hlm. 683.

[34] Rogier Creemers, "The Regulation of Generative AI in China", *Social Science Research Network*, (2024), hlm. 2.

[35] Bing Chen and Jiaying Chen, "China's Legal Practices Concerning Challenges of Artificial General Intelligence", *Multidisciplinary Digital Publishing Institute*, Volume 13 Issue 60, hlm. 5.

[36] Barbara Li, "China Releases 'AI Plus' Plan, rolls out AI Labelling Law", The International Association of Privacy Professionals Press (2023), < https://iapp.org/news/a/china-releases-ai-plus-plan-rolls-out-ai-labeling-law>, accessed on 2 November 2025.

2. Audio - Add voice or audio rhythm labels at appropriate positions at the beginning, end, or middle of the audio, or add prominent labels at the interface of interactive scenes.
3. Images - Add prominent labels at proper positions on images.
4. Videos - Add prominent labels at appropriate positions on the starting screen of the video and the periphery of the video and add prominent labels at appropriate positions at the end and in the middle of the video.
5. Virtual Scenes - Add prominent labels at appropriate positions on the starting screen and during the continuous service of the virtual scene.
6. Other Scenarios - Add prominent labels according to their own application characteristics.

Second, it mandates implicit labeling,[37] which will be assessed by adopting several technical measures within the file's or content's internal data and these labels should be easily perceived by users. China's AI Labelling Law requires providers of AI to add implicit labels to the file's metadata without impacting user's use of such contents.[38]

Critically, China's AI Labelling Law had laid out the obligations of service providers of AI in their regulation. All service providers must provide methods and examples for labelling AI-generated content in the user service agreement and remind users to carefully read and understand the labelling requirements.[39] If requested by the user, the service provider may provide AI-generated content without an explicit label, provided that the user's labelling obligations and liabilities are specified in the user service agreement, and the service provider must keep logs of the recipient's information and other relevant information for no less than six month.[40] AI providers whose main business is to offer online content services will then be required to verify AI-generated content as well as to ensure that appropriate labels are given and respected. In these cases, information on the nature of AI-generated content, the name or code of the dissemination platform, content number, and other

[37] Yan Luo and Xuezi Dan, "China Releases New Labeling Requirements for AI-Generated Content", The Covington Press (2025), <https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/>, accessed on 2 November 2025.

[38] Chuck Hollis, et al., "China's proposed AI Labelling Regulations: Key points", Norton Rose Fullbright Press (2024), <https://www.nortonrosefulbright.com/en/knowledge/publications/c1211a61/chinas-proposed-ai-labelling-regulations-key-points>, accessed on 1 November 2025.

[39] Lauren Hurcombe, et al., "China released new measures for labelling AI-generated and synthetic content", DLA Piper Press (2025), <https://www.technologyslegaledge.com/2025/03/china-released-new-measures-for-labelling-ai-generated-and-synthetic-content/>, accessed on 31 October 2025.

[40] Arlo Kipfer, "China's New AI Labeling Rules: What Every China Business Needs to Know", Harris Sliwoski Firm Press (2025), <https://harris-sliwoski.com/chinalawblog/chinas-new-ai-labeling-rules-what-every-china-business-needs-to-know/>, accessed on 2 November 2025.

dissemination information should be added to the file's metadata.[41] Network information content dissemination service providers should also provide necessary labelling functions and remind users to declare the AI-generated content.

The obligations for users of such providers are also regulated with China's AI Labelling Law as users will be required to send a declaration that such AI-generated content, pertaining to the regulation mandating such labeling function provided by the service provider, are applied when publishing such content. This created a dual-layered approach as the users, which is the critical figure at play when it comes to spreading misinformation, specifically those that have been AI-generated are required to disclose such label when publishing such content.

As one of the world's first comprehensive and mandatory national framework for synthetic media transparency, China's law presents a paradox.[42] Its detailed, dual-labeling approach offers a potential technical blueprint for other nations, like Indonesia, seeking to combat deepfakes.[43] However, the model's underlying philosophy of state control makes it difficult for liberal democracies to replicate. The law is deeply interwoven with a state-centric ideology of cyber sovereignty that prioritizes security over individual freedoms. While its technical mechanisms may be adapted globally, its holistic model, integrating transparency with a powerful apparatus of state surveillance, serves as both a source of technical inspiration and a cautionary tale about the profound political choices inherent in designing such regulations.

3. Bridging the Regulatory Chasm: The Critical Need for Deepfake Transparency in Indonesia

Indonesia's pursuit of Organization for Economic Co-operation and Development [**"OECD"**] membership by 2027 signals a strategic commitment to align its national policies with the high-level standards set by this influential organization, which is widely regarded as a global benchmark for advanced economic governance.[44] In the realm of digital policy, the OECD has been a definitive leader, establishing the first intergovernmental AI Principles in 2019. These principles represent a broad international consensus and were further strengthened in July 2024 by integrating the Global Partnership on Artificial Intelligence

[41] Silvia Lacovcich, "Chinese platforms to label AI-generated content under new law", National Technology News (2025), <https://nationaltechnology.co.uk/Chinese_platforms_to_label_aii_generated_content_under_new_law.php>, accessed on 1 November 2025.

[42] Ann O'Dea, "All AI-generated online content must now be labelled under Chinese law", Silicon Republic Press (2025), <https://www.siliconrepublic.com/machines/all-ai-generated-online-content-must-now-be-labelled-under-chinese-law-wechat-weibo>, accessed on 1 November 2025.

[43] Emmie Hine and Luciano Floridi, "New deepfake regulations in China are a tool for social stability, but ay what cost?", *Journal of Nature Machine Intelligence* (2022), pp. 608-610.

[44] Arisa Ema, et al., "The HAIP Reporting Framework: Feedback on a quiet revolution in AI Transparency", *OECD Press* (2025), <https://oecd.ai/en/wonk/the-haip-reporting-framework-feedback-on-a-quiet-revolution-in-ai-transparency>, accessed 2 November 2025.

"GPAI". A cornerstone of this global framework is transparency and explainability.[45] This principle obligates AI actors to foster a general understanding of an AI's capabilities, to make stakeholders clearly aware when they are interacting with an AI system, and to provide plain-language explanations of the data and logic behind an AI's output. This last point is crucial, as it is designed to ensure that any individual adversely affected by an AI-driven decision has a meaningful basis to challenge that outcome.[46]

These principles are not merely theoretical; the global AI policy discussion has decisively moved from defining these concepts to the practical challenge of implementation. The shared objective is to foster "trustworthy AI" that is human-centered, maximizes benefits, and protects individual rights. "Trustworthy AI" has become the global benchmark because it fundamentally shifts the goal of AI development from pure technical capability to positive human and societal outcomes. It's a framework designed to ensure AI systems are human-centric, ethical, and reliable, built on core pillars like transparency, fairness, accountability, and robustness.[47] This standard is essential for one primary reason: public trust. Without the assurance of trustworthiness, society will reject the adoption of AI in critical areas like medicine, law, and finance. This framework, therefore, serves a dual purpose: it proactively mitigates significant societal harms like automated bias or disinformation, and it translates abstract ethical goals into a clear, actionable set of requirements for policymakers and developers to implement and enforce.[48]

However, efforts to apply the OECD AI Principles are currently scattered, with tools and information often being sparse and disconnected from broader policy. To solve this, the OECD is creating a common framework to compare and share these tools. This will be supported by a regularly updated, interactive database on OECD.AI, providing policymakers and AI actors with the concrete tools needed to ensure their systems abide by all the core principles, including transparency, explainability, fairness, and accountability.

Conclusion

The legal comparison reveals a stark contrast in regulatory philosophy and preparedness. Indonesia is caught in a functional "*recht vacuum*", attempting to govern sophisticated AI-driven deception with a "fundamentally unfit" and outdated EIT Law.[49] This reactive approach, has created a severe accountability gap and left the public exposed to political disinformation and fraud. Conversely, China's AI Labelling Law provides a

[45] Tommaso Giardini and Nora Fischer, "AI Transparency and Explainibility: Operationalising the OECD AI Principle 1.3", Digital Policy Alert (2024), < https://digitalpolicyalert.org/ai-rules/oecd-principle-1-3>, accessed on 1 November 2025.

[46] Sónia Pedro Sebastião and David Ferreira-Mendes Dias, "AI Transparency: A Conceptual, Normative, and Practical Frame Analysis", *Journal Cogitatio*, Volume 13 (2025), hlm. 3.

[47]OECD, "OECD Employment Outlook 2023", *OECD Press* (2023), <https://www.oecd.org/en/publications/oecd-employment-outlook-2023_08785bba-en.html>, accessed on 2 November 2025.

[48]Alice Gomstyn, et al., "What is trustworthy AI?", *IBM Press* (2025), <https://www.ibm.com/think/topics/trustworthy-ai>, accessed on 2 November 2025

[49] Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP", *Jurnal Ilmiah Hukum dan Hak Asasi Manusia* (2024), hlm. 76.

decisive, proactive, and comprehensive framework. By mandating a dual-labeling system (both explicit and implicit) and defining clear obligations for service providers and users , China has created a robust, albeit state-controlled, architecture for transparency.

Based on this analysis, Indonesia should consider the transition from its reactive regulatory culture to a proactive one by enacting a specific, binding law to govern generative AI. The first step is purely foundational: the legislature must introduce formal legal definitions for "Artificial Intelligence" and "deepfake" into statute. This act alone would close the critical ambiguity that currently cripples the ability of law enforcement to regulate synthetic media. This new law must abandon the flawed "electronic agent" analogy and establish a clear, modern chain of legal responsibility for harm, distinguishing between AI developers, platform operators, and end-users.

Furthermore, Indonesia should adopt the technical architecture of China's law as a blueprint for mandated transparency. This framework should require a dual-labeling system: explicit labeling (e.g., clear text or watermarks) to ensure public awareness , and implicit labeling (e.g., technical metadata) to ensure traceability for enforcement. By adapting these mechanisms without importing the underlying state-centric ideology , Indonesia can create an effective legal defense that enhances public trust and restores informational integrity against the escalating threat of deepfakes.

Bibliography

Accelerated Capability Environment Division. "Innovating to detect deepfakes and protect the public". Gov.UK Press (2025). <https://www.gov.uk/government/case-studies/

innovating-to-detect-deepfakes-and-protect-the-public>.

Alexander, Atul. "Crisis and General International Law: Lessons from The Russia-Ukraine Conflict". Indonesian Journal of International Law. Volume 21 Issue 1 (2023).

Ann O'Dea. "All AI-generated online content must now be labelled under Chinese law". Silicon Republic Press (2025). <https://www.siliconrepublic.com/machines/all-ai-

generated-online-content-must-now-be-labelled-under-chinese-law-wechat-weibo>.

Ardhi, Satria. "AI Tidak Terlepas dari Berbagai Aktivitas Masyarakat, Kominfo Siap Luncurkan Panduan Etik Penggunaan AI". Gadjah Mada University Press (2023). < https://ugm.ac.id/id/berita/ai-tidak-terlepas-dari-berbagai-aktivitas-masyarakat-kominfo-siap-luncurkan-panduan-etik-penggunaan-ai/>.

Arif, Aftab. et al.. "An Overview of Cyber Threats Generated by AI". International Journal of Multidisciplinary Sciences and Arts. Volume 3 Issue 4 (2024).

Arvitto, Rafi Satrya. "Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP". Jurnal Ilmiah Hukum dan Hak Asasi Manusia (2024).

Bing Chen and Jiaying Chen. "China's Legal Practices Concerning Challenges of Artificial General Intelligence". Multidisciplinary Digital Publishing Institute. Volume 13 Issue 60 (2024).

Cambridge Advanced Learner's Dictionary & Thesaurus. "Deepfake". Cambridge University Press. <https://dictionary.cambridge.org/dictionary/english/deepfake>.

Chairani, Meirza Aulia. et al.. "The Urgency of Developing Law as A Legal Basis for The Implementation of Artificial Intelligence in Indonesia". Journal of Law and Justice. Volume 7 Issue 1 (2022).

Cihan Orak and Zeynep Turan. "Using Artificial Intelligence in Digital Video Production: A Systematic Review Study". Journal of Educational Technology and Online Learning. Volume 7 Issue 3 (2024).

Creemers, Rogier. "The Regulation of Generative AI in China". Social Science Research Network. (2024).

Desjardins, Dylan. "Possibilities & Perils of Deepfake Technology". The George Washington University Regulatory Studies Center. Volume 1 Issue 1(2022).

Easttom, William. "Deepfake Technology: Emerging Threats and Security Implications". International Conference on Cyber Warfare and Security. Volume 20 Issue 1 (2025).

Ema, Arisa. et al.. "The HAIP Reporting Framework: Feedback on a quiet revolution in AI Transparency". OECD Press (2025). <https://oecd.ai/en/wonk/the-haip-reporting-

framework-feedback-on-a-quiet-revolution-in-ai-transparency>.

Emmie Hine and Luciano Floridi. "New deepfake regulations in China are a tool for social stability, but ay what cost?". Journal of Nature Machine Intelligence (2022).

Felzman, Heike. et al.. "Towards Transparency by Design for Artificial Intelligence". Science and Engineering Ethics. Volume 26 Issue 6 (2020).

Filipova, Irina A.."Legal Regulation of Artificial Intelligence: Experience of China". Journal of Digital Technologies and Law.Volume 2 Issue 1 (2024).

Gomstyn, Alice. et al.. "What is trustworthy AI?". IBM Press (2025). <https://www.ibm.com/think/topics/trustworthy-ai>.

Hariyanti, Eva. et al.. "Implementations of Artificial Intelligence in Various Domains of IT Governance: A Systematic Literature Review". Journal of Information Systems Engineering and Business Intelligence/Journal of Information Systems Engineering and Business Intelligence. Volume 9 Issue 2 (2023).

Hollis, Chuck. et al.. "China's proposed AI Labelling Regulations: Key points". Norton Rose Fullbright Press (2024). <https://www.nortonrosefulbright.com/en/knowledge/

publications/c1211a61/chinas-proposed-ai-labelling-regulations-key-points>.

Hurcombe, Lauren. et al.. "China released new measures for labelling AI-generated and synthetic content". DLA Piper Press (2025). <https://www.technologyslegaledge.com/2025/03/china-released-new-measures-for-labelling-ai-generated-and-synthetic-content/>.

Jacob, Akhil Cherian. et al.. "Ai Based Virtual Personal Assistant". International Journal of Innovative Science and Research Technology. Volume 9 Issue 6 (2024).

Kaushik, Pooja. et al.. "Financial Fraud and Manipulation: The Malicious Use of Deepfakes in Business". Advances in Business Information Systems and Analytics Book Series. Volume 1 Issue 1 (2024).

Kipfer, Arlo. "China's New AI Labeling Rules: What Every China Business Needs to Know". Harris Sliwoski Firm Press (2025). <https://harris-sliwoski.com/chinalawblog/chinas-new-ai-labeling-rules-what-every-china-business-needs-to-know/>.

Lacovcich, Silvia. "Chinese platforms to label AI-generated content under new law". National Technology News (2025). <https://nationaltechnology.co.uk/Chinese_

platforms_to_label_aii_generated_content_under_new_law.php>.

Li, Barbara. "China Releases 'AI Plus' Plan, rolls out AI Labelling Law". The International Association of Privacy Professionals Press (2023). < https://iapp.org/news/a/china-releases-ai-plus-plan-rolls-out-ai-labeling-law>.

Magramo, Kathleen. "British Engineering Giant Arup Revealed as $25 million deepfake scam victim". CNN (2024). <https://edition.cnn.com/2024/05/16/tech/arup-deepfake- scam-loss-hong-kong-intl-hnk>.

Maharani, Chandra. et al.. "Legal Vacuum Regarding Licensing Regulations for Constructing Flats in the Regions". Jurnal Pranata Hukum. Volume 19 Issue 1 (2024).

Marçal Mora-Cantallops. et al.. "Traceability for Trustworthy AI: A Review of Models and Tools". Multidisciplinary Digital Publishing Institute (2021).

Mimi Zhou and Lu Zhang. "Navigating China's regulatory approach to generative artificial intelligence and large language models". Cambridge Forum on AI: Law and Governance. Volume 1 (2025).

Muhaimin. Metode Penelitian Hukum. (Nusa Tenggara Barat: Mataram University Press, 2020).

Muhammad Najiib Al Fithri and Ery Agus Priyono. "Issues and Possibilities in Regulating Artificial Intelligence (AI) Related To Copyright in Indonesia". International Journal of Social Science and Human Research. Volume 7 Issue 6 (2024).

OECD. "OECD Employment Outlook 2023". OECD Press (2023). <https://www.oecd.org/en/publications/oecd-employment-outlook-2023_08785bba-en.html>.

Palmiotto, Francesa. "Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective". SSRN (2023). <https://papers.ssrn.com/sol3/

papers.cfm?abstract_id=4384122>.

Pamungkas, Abdul Aziz. et al.. "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity". Pena Justicia. Volume 24 Issue 2 (2025).

Permana, Agus. "Indonesia's Cyber Defense Strategy in Mitigating the Risk of Cyber Warfare Threats". Syntax Idea. Volume 3 Issue 1 (2021).

Qingle Hu and Wei Liu. "The Regulation of Artificial Intelligence in China". International Conference on Social Sciences and Humanities and Arts. Volume 3 (2024).

Rahim, Abdillah Satari. et al.. "Identify Cyber Intelligence Threats in Indonesia". International Journal of Humanities Education and Social Sciences. Volume 3 Issue 1 (2023).

Rama, Alzet. et al.. "Legal gaps in indonesia's electronic information and transactions law in addressing deepfake technology: challenges and regulatory recommendations". Indonesian Journal of School Counseling. Volume 10 Issue 2 (2025).

Respati, Adnasohn Aqilla. "Reformulasi Undang-Undang ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation". Journal USM Law Review. Volume 7 Issue 3 (2024).

Rolindrawan, Winnie Yamashita. "Regulation of Artificial Intelligence in Indonesia". SSEK Press (2024). <https://ssek.com/blog/indonesia-law-update-regulation-of-artificial-

intelligence/>.

Santoso, Topo.. "Comparative Law in the Faculty of Law, University of Indonesia: Course Content and Teaching Methods". Asian Journal of Comparative Law. Volume 14 (2019).

Shenan, Matt. China's AI Regulations and How They Get Made. United States: Carnegie Endowment For International Peace (2023).

Sheikh, Aabid Majeed. et al.. "Thomas Hobbes' views on Philosophy, State of Nature and International Relations". International Journal of Humanities and Education Development. Volume 2 Issue 1 (2020).

Sónia Pedro Sebastião and David Ferreira-Mendes Dias. "AI Transparency: A Conceptual, Normative, and Practical Frame Analysis". Journal Cogitatio, Volume 13 (2025).

Tommaso Giardini and Nora Fischer. "AI Transparency and Explainability: Operationalising the OECD AI Principle 1.3". Digital Policy Alert (2024). < https://digitalpolicyalert.org/ai-rules/oecd-principle-1-3>.

Ville Aula and Tero Erkillä. Handbook on Public Policy and Artificial Intelligence. England: Edward Elgar Publishing (2024).

Xiao, Baiyang. "Agile and Iterative Governance: China's Regulatory Response to AI". Social Science Research Network. (2025).

Yan Luo and Xuezi Dan. "China Releases New Labeling Requirements for AI-Generated Content". The Covington Press (2025). <https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/>.