

HUMAN RIGHTS PROTECTION IN ARTIFICIAL INTELLIGENCE GOVERNANCE: COMPARATIVE LESSONS FOR INDONESIA'S REGULATORY FRAMEWORK

¹Adhika Mahindra Satya, ²Radian Salman, ²Rosa Ristawati, ³Haryono, ⁴Ahmad Shabudin Ariffin

¹Master of Law Study Program, Faculty of Law, Universitas Airlangga, Surabaya, Indonesia

²Faculty of Law, Universitas Airlangga, Surabaya, Indonesia

³Faculty of Economics and Business, Universitas Tanjungpura, Pontianak, Indonesia

⁴Faculty of Business and Management Sciences, Universiti Islam Antarabangsa Tuanku Syed Sirajuddin (UniSIRAJ),
Perlis, Malaysia

*Corresponding author: adhika.mahin.satya-2024@fh.unair.ac.id

Abstract

The rapid development of artificial intelligence (AI) has raised significant concerns regarding the protection of human rights, particularly in relation to privacy, non-discrimination, accountability, and legal certainty. This study examines regulatory gaps in Indonesia's AI governance from a human rights perspective and proposes regulatory recommendations through a comparative analysis of legal frameworks in the European Union (EU), China, and the United States (U.S.). Employing doctrinal legal research, this study applies statutory, conceptual, comparative, and case-based approaches. The findings reveal that, although Indonesia has adopted several legal instruments relevant to digital technologies, including the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, and various ethical guidelines, these instruments were not specifically designed to address the distinctive risks associated with AI systems. In particular, the absence of clear AI-specific definitions, risk-classification mechanisms, algorithmic transparency and audit requirements, mandatory human oversight, and rules on synthetic-content labeling creates substantial regulatory gaps that may undermine effective human rights protection. Comparative analysis indicates that Indonesia could draw on the EU AI Act's risk-based regulatory framework, human oversight requirements, and transparency obligations; China's approach to algorithm governance and synthetic-content labeling; and the U.S. sectoral model, particularly the Colorado AI Act and state privacy laws addressing transparency and discriminatory outcomes in automated decision-making. This study argues that Indonesia should establish a dedicated AI regulatory framework incorporating clear legal definitions, risk-based classification, algorithmic auditing, meaningful human oversight, transparency requirements, and synthetic-content labeling. Such a framework is essential to ensure that the development and deployment of AI systems remain consistent with human rights protection and legal certainty within Indonesia's national legal order.

Keywords: *Artificial Intelligence; Human Rights; AI Regulation; Algorithmic Governance; Indonesia.*

Received: 24 June 2025; Revised: 25 April 2026; Accepted: 27 April 2026; Available online: 30 April 2026; Published: 30 April 2026.

How to Cite: Satya, Adhika Mahindra, Radian Salman, Rosa Ristawati, Haryono Haryono, and Ahmad Shabudin Ariffin. "Human Rights Protection in Artificial Intelligence Governance: Comparative Lessons for Indonesia's Regulatory Framework." *Diponegoro Law Review* 11, no. 1 (2026): 68–93. <https://doi.org/10.14710/dilrev.11.1.2026.68-93>.

Copyright © Diponegoro Law Review. Published by Faculty of Law, Universitas Diponegoro. This is an open access article under the CC-BY-NC-SA License. (<https://creativecommons.org/licenses/by-nc-sa/4.0/>)

1. Introduction

Artificial Intelligence (AI) is technology that enables machines to exhibit intelligent behavior by solving environmental problems and taking actions to achieve specific goals with a certain

degree of autonomy.¹ AI is characterized by the application of diverse intelligent technologies in the fields of science and engineering, facilitating the development of intelligent machines and computing systems to accomplish real-world objectives.² The current general understanding of AI systems is that they are autonomous systems that learn from their surroundings and change their models of change based on changes in their changing environment.³ AI has the capability to complete tasks previously impossible for humans, such as processing various types of data. AI also enhances daily life through devices equipped with personal assistants on mobile phones or by powering the development of autonomous vehicles.⁴

However, even though AI brings many benefits to human life, advances in AI also present complex challenges for human life, especially in its position as a non-legal entity or an entity that is not legally responsible, involving various stakeholders, such as providers, developers, and hardware suppliers.⁵ Issues such as transparency, algorithmic bias, human rights, privacy rights, unfairness, weak cybersecurity, liability bias in cases of harm, and others are significant challenges of the implementation of AI.⁶ An illustrative instance of human rights infringements stemming from the implementation of AI in access to justice is the utilization of online court proceedings through the WeChat application within Chinese judicial systems.⁷

The state is responsible for the actualization and preservation of the human rights of all citizens, which includes the protection of privacy and individual information, as articulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. This article elucidates that, within the framework of data security amidst technological progress, the state must safeguard and ensure the rights of individuals. This includes human rights, data protection, and privacy rights. Legal protection constitutes an endeavor to safeguard the dignity and honor inherent to humanity while simultaneously acknowledging the human rights attributed to each legal subject. This protection is afforded through legal provisions designed to avert criminal acts, with Pancasila and the principle of the rule of law serving as its fundamental founding principles.⁸

To date, Indonesia lacks specific, comprehensive legislation governing artificial intelligence. However, regulations governing the use of artificial intelligence are not entirely outside the legal framework. The use of AI-based technology remains governed by Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 and Law No. 1 of 2024, as well as Law No. 27 of 2022 on Personal Data Protection. These regulations govern electronic systems, electronic agents, data processing, and personal data protection that are functionally related to the operation of AI systems. Through these provisions, Indonesian positive law has established general obligations regarding system security, data protection, and

¹ Hussein A. Abbass, "Social Integration of Artificial Intelligence: Functions, Automation Allocation Logic and Human-Autonomy Trust," *Cognitive Computation* 11, no. 2 (April 2019): 159–71, <https://doi.org/10.1007/s12559-018-9619-0>.

² Hyeyoung Hah and Deana Shevit Goldin, "How Clinicians Perceive Artificial Intelligence-Assisted Technologies in Diagnostic Decision Making: Mixed Methods Approach," *Journal of Medical Internet Research* 23, no. 12 (December 2021): 1–19, <https://doi.org/10.2196/33540>.

³ Tetyana (Tanya) Krupiy, "A Vulnerability Analysis: Theorising the Impact of Artificial Intelligence Decision-Making Processes on Individuals, Society and Human Diversity from a Social Justice Perspective," *Computer Law & Security Review* 38 (September 2020): 1–25, <https://doi.org/10.1016/j.clsr.2020.105429>.

⁴ David Lorge Parnas, "The Real Risks of Artificial Intelligence," *Communications of the ACM* 60, no. 10 (September 2017): 27–31, <https://doi.org/10.1145/3132724>.

⁵ Miriam Buiten, Alexandre De Streel, and Martin Peitz, "The Law and Economics of AI Liability," *Computer Law & Security Review* 48 (April 2023): 1–20, <https://doi.org/10.1016/j.clsr.2023.105794>.

⁶ Rowena Rodrigues, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities," *Journal of Responsible Technology* 4 (December 2020): 1–12, <https://doi.org/10.1016/j.jrt.2020.100005>.

⁷ Nataliia Martsenko, "Artificial Intelligence and Human Rights: A Scientific Review of Impacts and Interactions," *Studia Prawnoustrojowe*, no. 58 (December 2022): 326–38, <https://doi.org/10.31648/sp.8245>.

⁸ Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia (Sebuah Studi Tentang Prinsip-prinsipnya, Penanganannya oleh Pengadilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara)*, 1st ed. (Surabaya: Bina Ilmu, 1987).

accountability for electronic activities. However, existing regulations have not been specifically designed to anticipate the characteristics, risks, and complexities of AI technology.

The Indonesian government has also adopted several policy instruments and guidelines for AI governance. These instruments include the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics, the 2020-2045 Indonesian National Artificial Intelligence Strategy, and the Guidelines for Responsible and Trusted Artificial Intelligence in the Financial Technology Industry published by the Financial Services Authority (OJK). These policy documents and guidelines contain general principles such as transparency, accountability, system security, responsible innovation, and personal data protection. The soft-law nature of these instruments means they are not legally binding and lack enforceable sanctions, limiting their capacity to provide operational guidance for addressing complex AI risks, including automated decision-making, algorithmic accountability, and human rights protection.

The limitations of the existing legal framework are evident in addressing the human rights risks posed by AI. Current regulations lack explicit AI-specific definitions, risk classification mechanisms, transparency and impact assessment obligations, human oversight requirements, and algorithmic audit standards, rendering them insufficient to anticipate systemic risks arising from automated decision-making, algorithmic bias, large-scale data processing, and AI-generated content. Human rights and the right to privacy are fundamental reasons for formulating specific laws on AI in Indonesia, given that this technology has the potential to cause unpredictable ethical and social impacts under certain conditions.⁹ The ethical dimension is closely linked to the development and use of AI, making morally grounded regulation essential to ensure justice and legal certainty.¹⁰ The existing regulatory gap has the potential to weaken the preventive protection of the right to privacy, the principle of non-discrimination, legal certainty, and accountability mechanisms in the use of AI technology.

The increasing deployment of artificial intelligence generates legal risks that require adaptive legal responses to rapid social and technological change. Roscoe Pound's theory of *law as a tool of social engineering*, defined by Satjipto Raharjo as a conscious effort to use legal instruments to design or change the social order, places the law as a strategic means of directing the development of society.¹¹ This theoretical perspective emphasizes that law not only functions repressively after violations occur, but also plays a preventive role by shaping a regulatory framework responsive to technological dynamics. The adaptive function of law becomes relevant in the context of AI, enabling technological innovation to align with human rights values.

Previous research by M. Wildan Mufti et al. emphasizes the need to implement AI technology legislation in Indonesia, using Pound's social engineering theory to analyze the function of law as a social control tool in regulating the appropriate use of AI.¹² Another study by Ardina Khoirun Nisa discusses the development of AI and its implications for the Indonesian legal system, employing a normative juridical approach, and assesses its adequacy in anticipating AI-related issues.¹³ The originality of this research lies in its analysis, which prioritizes the protection of human rights as the primary criterion for assessing the adequacy of Indonesia's legal framework for regulating AI. This research not only maps existing regulations but also systematically identifies normative gaps and structural limitations in Indonesian positive law that have not adequately addressed the specific risks posed by AI. The novelty of this research is

⁹ Patricia Gomes Rêgo De Almeida, Carlos Denner Dos Santos, and Josivania Silva Farias, "Artificial Intelligence Regulation: A Framework for Governance," *Ethics and Information Technology* 23, no. 3 (September 2021): 505–25, <https://doi.org/10.1007/s10676-021-09593-z>.

¹⁰ Aries Saputro and Radian Salman, "Legal and Moral Principles as Guidelines for Carrying Out Official Duties," *Yuridika* 39, no. 2 (May 2024): 127–52, <https://doi.org/10.20473/ydk.v39i2.50496>.

¹¹ Satjipto Rahardjo, *Ilmu Hukum*, 6th ed. (Bandung: PT Citra Aditya Bakti, 2006).

¹² M. Wildan Mufti et al., "Urgensi Pembentukan Peraturan Perundang-undangan Teknologi Berbasis Artificial Intelligence," *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 11 (June 2024): 137–41, <https://doi.org/10.5281/zenodo.11422903>.

¹³ Ardina Khoirun Nisa, "The Prospect of AI Law in Indonesian Legal System: Present and Future Challenges," *The Indonesian Journal of International Clinical Legal Education* 6, no. 1 (March 2024): 25–48, <https://doi.org/10.15294/iccle.v6i1.4686>.

reinforced through a comparative law approach that examines artificial intelligence regulatory models in the European Union (EU), China, and the United States (U.S) to yield comparative insights relevant to the development of a human rights-oriented AI regulatory framework in Indonesia.

2. Method

Using a doctrinal legal research method, this study applies four approaches: the statute, conceptual, comparative law, and case approaches. These four approaches are used in an integrated manner to assess the adequacy of the legal framework for regulating AI and its implications for human rights protection in Indonesia. Through the statutory approach, this study examines positive laws related to the use of AI, including Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments through Law Number 19 of 2016 and Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, as well as related sectoral regulations and policies, such as the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics and Guidelines for Responsible and Trusted Artificial Intelligence in the Financial Technology Industry. This approach assesses the extent to which applicable legal norms respond to the risk of AI-related human rights violations. A conceptual approach is used to examine legal protection theories, human rights principles, and the concepts of algorithmic accountability and human oversight as the basis for a doctrinal analysis of the need to update and strengthen AI regulations. A comparative legal approach is applied by analyzing AI regulatory models in the EU, China, and the U.S. to identify principles, mechanisms, and human rights protection standards relevant to application in the Indonesian legal system. A case approach is used by examining concrete examples of personal data violations related to the use of technology, including Karanganyar District Court Decision Number 5/Pid.Sus/2023/PN Krg and Tangerang District Court Decision Number 77/Pid. Sus/2024/PN Tng, to demonstrate the gap between applicable legal norms and human rights protection practices in the context of AI.

Data for this study comprise primary and secondary legal materials. Primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law Number 11 of 2008 concerning Electronic Information and Transactions, along with its amendments through Law Number 19 of 2016 and Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, as well as sectoral regulations and policies related to AI. Secondary legal materials include law textbooks, national and international scientific journals, legal doctrines, policy reports, and previous research results relevant to the regulation of AI and the protection of human rights. Data were gathered through library research to identify, classify, and analyze laws and regulations, journals, scientific articles, and other literature relevant to the research problem. This research adopts the descriptive-analytical method to objectively describe the conditions of AI regulation in the Indonesian legal system. Furthermore, it analyzes these conditions through a legal theory framework, human rights principles, and a doctrinal approach to formulate recommendations for strengthening AI regulations in line with the principles of the rule of law and human rights protection standards.

3. Results and Discussion

3.1. Limitations of Indonesia's Legal Framework in Addressing Artificial Intelligence from a Human Rights Perspective

3.1.1. Artificial Intelligence Risk Transformation and Its Challenges to Human Rights Protection

The development of AI brings not only significant benefits but also poses serious risks to the fulfillment and protection of human rights.¹⁴ AI's ability to autonomously process data, learn

¹⁴ Jesslyn Jesslyn and Raja Ritonga, "Pengaruh Artificial Intelligence (AI) terhadap Hak Asasi Manusia," *Jurnal Res Justitia: Jurnal Ilmu Hukum* 5, no. 1 (January 2025): 35–49, <https://doi.org/10.46306/rj.v5i1.135>.

patterns, and make decisions within complex socio-technical networks enables algorithmic outputs to directly and significantly affect human lives, often with diminishing human oversight.¹⁵ This condition raises profound ethical and social concerns, as automated decision-making increasingly operates beyond direct human control.¹⁶ Advances in AI also have substantial economic and social impacts, including potential unemployment, intensified surveillance of workers, widening wealth disparities, and growing uncertainty about privacy and individual control over personal data.¹⁷ Moreover, AI technologies may undermine democratic values by facilitating the spread of manipulative information, reinforcing authoritarian tendencies, increasing the risk of conflict, and constraining human autonomy in both the digital and physical spheres.¹⁸

Human rights are regarded as one of the most essential notions in jurisprudence. Human rights are fundamental entitlements that must be protected and advanced to uphold the dignity and liberty of all people.¹⁹ The state is obliged to guarantee these rights in order to protect the dignity and freedom of individuals as stipulated in Article 28, letter I, paragraph (4) of the 1945 Constitution of the Republic of Indonesia, which reads: "The protection, promotion, enforcement, and fulfillment of human rights is the responsibility of the state, especially the government."

Current regulations fail to address the risks posed by AI to human rights. The ability of AI to process, combine, or manipulate personal data without adequate oversight creates risks of privacy and data security violations. The spread of AI-generated content, such as deepfakes and false information, is rapid, while positive regulations have yet to provide practical tools to limit these harmful effects.²⁰

Current legal framework is limited to the Electronic Information and Transactions Law, the Personal Data Protection Law, the AI Ethics Circular Letter from the Ministry of Communication and Information Technology, and ethical guidelines published by the OJK. These instruments provide an initial normative basis for the use of digital technology, but do not currently cover the complexity of AI risks. Existing regulations have not addressed the consequences of AI, including algorithmic impact assessments, system transparency, and the accountability of AI developers and users. Therefore, regulations are needed to govern this technology responsibly and in accordance with human rights principles.

3.1.2. Limitations of the Indonesian Legal Framework in Regulating Artificial Intelligence Risks

Indonesia faces regulatory limitations in addressing AI risks, as the rapid development of AI technology has not been adequately anticipated by the existing legal framework.²¹ The national

¹⁵ Carmen Oana Mihaila and Mircea Mihaila, "Artificial Intelligence - The Era of Social Inequalities. In Regulating the Future, We Need to Look at the Risks," *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, May 20, 2024, 39–63, <https://doi.org/10.62768/ADJURIS/2024/1/03>.

¹⁶ Michael Pizzi, Mila Romanoff, and Tim Engelhardt, "AI for Humanitarian Action: Human Rights and Ethics," *International Review of the Red Cross* 102, no. 913 (April 2020): 145–80, <https://doi.org/10.1017/S1816383121000011>.

¹⁷ Sinta Dewi and Mohammad Wildan Hidayat, "Protection of Data Privacy in The Era of Artificial Intelligence in The Financial Sector in Indonesia," *Journal of Central Banking Law and Institutions* 1, no. 2 (May 2022): 353–66, <https://doi.org/10.21098/jcli.v1i2.18>.

¹⁸ Bernd Carsten Stahl et al., "Exploring Ethics and Human Rights in Artificial Intelligence – A Delphi Study," *Technological Forecasting and Social Change* 191 (June 2023): 1–17, <https://doi.org/10.1016/j.techfore.2023.122502>.

¹⁹ Roman I. Blahuta et al., "Enhancing Human Rights Protections in Ukrainian Law Enforcement: National Compliance with EU Standards," *Yuridika* 39, no. 1 (January 2024): 1–30, <https://doi.org/10.20473/ydk.v39i1.45461>.

²⁰ Christopher Whyte, "Deepfake News: AI-Enabled Disinformation as a Multi-Level Public Policy Challenge," *Journal of Cyber Policy* 5, no. 2 (May 2020): 199–217, <https://doi.org/10.1080/23738871.2020.1797135>.

²¹ Jeroen K. G. Hopster and Matthijs M. Maas, "The Technology Triad: Disruptive AI, Regulatory Gaps and Value Change," *AI and Ethics* 4, no. 4 (November 2024): 1051–69, <https://doi.org/10.1007/s43681-023-00305-5>.

legal framework currently associated with artificial intelligence consists of Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 28 of 2014 concerning Copyright. These laws contain provisions on electronic information, electronic transactions, personal data protection, and intellectual property rights.

Non-binding technical instruments are also present in the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics and the Responsible and Trusted Artificial Intelligence (AI) Code of Conduct Guidelines in the Financial Technology Industry, published by the OJK. Both guidelines contain general ethical principles, including responsibility, transparency, security, and personal data protection. The soft-law nature of these guidelines means there are no explicit legal obligations and no definite enforcement mechanisms to ensure effective human rights protection.

AI is not a single homogeneous technology. Different types of AI, such as generative AI and decision-making or agent-based AI, entail distinct legal risks and regulatory consequences.²² Generative AI primarily raises legal issues related to the creation and dissemination of synthetic content, including deepfakes, disinformation, intellectual property concerns, and privacy violations arising from automated content generation.²³ In contrast, decision-making or agent-based AI systems are more closely associated with risks arising from automated profiling, algorithmic discrimination, opaque decision-making processes, and the erosion of individual autonomy and due process.²⁴ Indonesia's current legal framework, which indirectly regulates AI through general provisions on electronic systems and personal data protection, does not distinguish between these categories of AI or their respective risk profiles. As a result, the application of uniform legal norms within the existing framework remains insufficient to address the diverse, AI-specific human rights risks posed by different forms of AI.

The limitations of this legal framework are evident in the lack of explicit definitions and classifications of AI, of specific regulations on algorithmic impact assessment, of transparency and clarity requirements for automated decisions, and of accountability standards for developers and users of AI. Existing positive norms still focus on acts, such as illegal access, data manipulation, and general violations of personal data.²⁵ Meanwhile, specific risks associated with AI, such as automated profiling, deepfakes, large-scale data manipulation, and high-risk automated decision-making, remain inadequately regulated under the existing legal framework.²⁶ These weaknesses indicate the dominance of a repressive approach in the existing legal framework. Preventive protections that should be in place through algorithmic audit obligations, data governance standards, and AI system oversight have not obtained a clear normative basis. As a result, the existing legal framework has not comprehensively anticipated specific AI-related risks, particularly those arising from automated decision-making and algorithmic governance.

²² Lily Ballot Jones, Julia Thornton, and Daswin De Silva, "Limitations of Risk-Based Artificial Intelligence Regulation: A Structuration Theory Approach," *Discover Artificial Intelligence* 5, no. 14 (February 2025): 1–13, <https://doi.org/10.1007/s44163-025-00233-9>.

²³ Furizal et al., "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review," *Social Sciences & Humanities Open* 12 (2025): 1–25, <https://doi.org/10.1016/j.ssaho.2025.101882>.

²⁴ Dubravka Cecez-Kecmanovic, "Ethics in the World of Automated Algorithmic Decision-Making – A Posthumanist Perspective," *Information and Organization* 35, no. 3 (September 2025): 1–16, <https://doi.org/10.1016/j.infoandorg.2025.100587>.

²⁵ Adnasohn Aqilla Respati, "Reformulasi UU ITE terhadap Artificial Intelligence dibandingkan dengan Uni Eropa dan China AI Act Regulation," *JURNAL USM LAW REVIEW* 7, no. 3 (December 2024): 1737–58, <https://doi.org/10.26623/julr.v7i3.10578>.

²⁶ Natalia Díaz-Rodríguez et al., "Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation," *Information Fusion* 99 (November 2023): 101896, <https://doi.org/10.1016/j.inffus.2023.101896>.

3.1.3. Analysis of Court Decisions and Regulatory Limitations in the Supervision of Artificial Intelligence Technology

Court decisions clearly illustrate how positive law governs issues related to personal data and technology.²⁷ The Karanganyar District Court Decision Number 5/Pid.Sus/2023/PN Krg and the Tangerang District Court Decision Number 77/Pid.Sus/2024/PN Tng show that judges can impose criminal sanctions for the theft or misuse of personal data under Law Number 27 of 2022 concerning Personal Data Protection and the provisions of the ITE Law. These decisions confirm that Indonesian law provides a clear legal basis for prosecuting perpetrators of personal data violations.²⁸

An analysis of the two decisions reveals limitations on how the law interprets the role of advanced technologies, particularly AI. The courts treated the cases as conventional personal data violations, without considering the possibility of AI involvement in the collection, processing, or dissemination of data. The judges did not explicitly address critical aspects, such as automated systems, large-scale web scraping, or AI-based impersonation techniques in their legal reasoning.²⁹

This situation reflects the limitations of the legal framework in overseeing AI technology. In addition, law enforcement agencies in Indonesia do not fully understand the specific challenges associated with AI due to the lack of clear legal guidelines.³⁰ The judiciary plays a repressive role after a violation has occurred, while the preventive dimension related to the obligations of AI system developers and operators lacks a normative basis. The lack of AI-specific substantive norms means that courts have no basis for specifically assessing the systemic risks inherent in the use of AI.³¹

3.1.4. Legal Protection Theory and Its Relevance to the Regulatory Limitations of Artificial Intelligence

The legal protection theory proposed by Philipus M. Hadjon provides a conceptual framework for assessing the extent to which the legal system can protect human rights in the context of the use of AI. This concept distinguishes between preventive protection and repressive protection. Preventive legal protection aims to protect citizens from rights violations by providing oversight mechanisms, channels for objection, and binding norms before violations occur. Meanwhile, repressive legal protections address violations that have already occurred through administrative, civil, or criminal sanctions.³²

The application of this theory to the regulation of AI in Indonesia broadly indicates the dominance of repressive legal protection. Current laws focus more on responding to data

²⁷ Agus Siagian and Dony Alexander, "Penerapan Hukum Pidana terhadap Pelaku Tindak Pidana Siber di Indonesia: Analisis Putusan Pengadilan," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan* 4, no. 9 (2025): 2641–56, <https://doi.org/10.54443/sibatik.v4i9.3360>.

²⁸ Mochamad Januar Rizki, *Menelaah 3 Putusan Perkara Pelanggaran PDP, Minimnya Literasi dan Tantangannya*, January 6, 2025, <https://www.hukumonline.com/berita/a/menelaah-3-putusan-perkara-pelanggaran-pdp--minimnya-literasi-dan-tantangannya-lt677bd1211839d/>, accessed on May 20, 2025.

²⁹ Denis Kolodin et al., "Artificial Intelligence in E-Commerce: Legal Aspects," *Proceedings of the III International Scientific Congress Society of Ambient Intelligence 2020 (ISC-SAI 2020)* 129 (2020): 96–102, <https://doi.org/10.2991/aebmr.k.200318.012>.

³⁰ Lusi Zafriana, "Integrasi Kecerdasan Buatan dalam Penegakan Hukum: Peluang Inovasi dan Tantangan Keadilan Prosedural di Indonesia," *Jurnal Penelitian Ilmu Sosial dan Eksakta* 5, no. 1 (September 2025): 24–36, <https://doi.org/10.47134/trilogi.v5i1.1688>.

³¹ Anggil Syahra Putri Mecca, Wahab Aznul Hidayat, and Hadi Tuasikal, "Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) dalam Sistem Peradilan Pidana di Indonesia," *Jurnal Sosial Teknologi* 5, no. 6 (June 2025): 1730–46, <https://doi.org/10.59188/jurnalsostech.v5i6.32207>.

³² Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia (Sebuah Studi tentang Prinsip-prinsipnya, Penanganannya oleh Pengadilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi)*, Special Edition First Printing (Malang: Peradaban, 2007).

breaches or cybercrimes after they occur.³³ Legislators have not codified AI-specific rules requiring risk assessments, system transparency obligations, or continuous monitoring mechanisms.³⁴ As a result, state institutions protect human rights primarily after violations cause harm, rather than at the prevention stage.

A study by M. Syamsuri Harun and Men Wih Widiyanto, entitled “Criminal Liability for the Theft of Personal Data Using Artificial Intelligence Technology (Case Study of Decision No. 5/Pid.Sus/2023/PN Krg), shows that AI plays a role in strengthening the perpetrator's ability to access, process, and exploit data, for example, through automation, profiling, and exploitation of system vulnerabilities. The study shows that AI plays a role in strengthening the perpetrator's ability to access, process, and exploit data, for example, through automation, profiling, and exploitation of system vulnerabilities. Criminal liability remains directed at the human perpetrator who controls the system. Positive law lacks supervisory mechanisms and explicit AI-specific obligations governing the management of the use of AI in the processing of personal data. This confirms that Indonesia's legal framework is not fully equipped to address the risks posed by AI, including automated decision-making, profiling, and data-driven risks.³⁵

3.1.5. Consequences of Regulatory Limitations in Artificial Intelligence Governance on Human Rights Protection

The limitations of existing legal frameworks in addressing AI risks have direct consequences for the fulfillment of human rights, particularly in terms of equality, privacy, individual freedom, and the protection of human dignity.³⁶ AI systems can collect, analyze, and categorize personal data on a large scale through processes that are often not fully understood, recognized, or controllable by individuals as data subjects.³⁷ This capability creates vulnerabilities that cannot be adequately addressed by existing laws, which were not designed to regulate AI-specific risks by Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 and Law No. 1 of 2024, as well as non-binding instruments such as the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics and the Responsible and Trusted Artificial Intelligence Code of Conduct Guidelines in the Financial Technology Industry published by the OJK. The operation of AI that is not within legal boundaries has the potential to produce discriminatory evaluations and decisions that arise from algorithmic bias and non-transparent system design.³⁸ These impacts threaten the basic principles of equality and justice, which are the foundation for the fulfillment of human rights.³⁹

The deployment of AI technology, under limited ethical and legal frameworks, poses a substantial risk of infringing upon fundamental human rights, liberties, and the sanctity of personal

³³ Oky Syalendro, Arief Fahmi Lubis, and R Yusak Andri Ende Putra, “Cyber Crime Crimes in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases,” *AURELIA: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia* 4, no. 1 (December 2024): 335–47, <https://doi.org/10.57235/aurelia.v4i1.3708>.

³⁴ Ghuftron Rosadi Hidayah, Ha. Djazim Ma'shum, and Muhammad Awaluddin, “Studi Komparatif Perlindungan Data Pribadi dalam UU ITE 2024 dan UU PDP 2022,” *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora* 4, no. 4 (August 2025): 61–70, <https://doi.org/10.55606/jurish.v4i4.6341>.

³⁵ M. Syamsuri Harun and Men Wih Widiyanto, “Criminal Liability for the Theft of Personal Data Using Artificial Intelligence Technology (Case Study of Decision No. 5/Pid.Sus/2023/PN Krg),” *International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy* 1, no. 1 (July 2025): 168–76, <https://doi.org/10.56861/nalarnagara.v1i1.196>.

³⁶ Sue Anne Teo, “Artificial Intelligence and Its ‘Slow Violence’ to Human Rights,” *AI and Ethics* 5, no. 3 (June 2025): 2265–80, <https://doi.org/10.1007/s43681-024-00547-x>.

³⁷ Markus Kattinig et al., “Assessing Trustworthy AI: Technical and Legal Perspectives of Fairness in AI,” *Computer Law & Security Review* 55 (November 2024): 1–18, <https://doi.org/10.1016/j.clsr.2024.106053>.

³⁸ Miriam C Buiten, “Towards Intelligent Regulation of Artificial Intelligence,” *European Journal of Risk Regulation* 10, no. 1 (March 2019): 41–59, <https://doi.org/10.1017/err.2019.8>.

³⁹ Denis Coitinho and André Luiz Olivier Da Silva, “Algorithmic Injustice and Human Rights,” *Filosofia Unisinos* 25, no. 1 (March 2024): 1–17, <https://doi.org/10.4013/fsu.2024.251.09>.

privacy.⁴⁰ AI's ability to identify patterns, profile individuals, and predict behavior from data collected across various sources creates opportunities for invasive monitoring.⁴¹ This situation threatens the right to privacy, which is a fundamental right and part of human dignity. The lack of explicit AI-specific normative boundaries leaves individuals vulnerable, as their daily activities are monitored and processed by automated systems without effective human oversight.⁴²

Another consequence of the regulatory gaps regarding the legality of content generated by AI is the threat to intellectual property rights.⁴³ Generative models can produce text, images, or other works with uncertain copyright status or legal responsibility for the impact of such content.⁴⁴ As Law Number 28 of 2014 concerning Copyright only recognizes humans as creators, there are no regulations determining the legal status of works produced by AI systems and the parties responsible for potential legal violations.⁴⁵ This ambiguity raises important questions about the future of intellectual property protection in a digital ecosystem increasingly dominated by generative technology.

Moral rights, privacy rights, and freedom as fundamental human values should protect human dignity.⁴⁶ Human creativity and cultural dynamics can lead technological development in unexpected directions.⁴⁷ The concept of affordances explains this condition: the possibility of different outcomes arising from a technology's design and from the ways humans interact with it.⁴⁸ Insufficiently regulated use of AI poses significant risks to human dignity and freedom. Therefore, strong regulations are needed to manage and minimize the impact of technology and ensure that the use of AI remains consistent with human rights principles.⁴⁹ The state has an obligation to protect the rights to freedom and privacy as stipulated in Article 28G of the 1945 Constitution of the Republic of Indonesia, which states: "Every person shall have the right to protection of their personal self, family, honor, dignity, and property under their control, as well as the right to feel secure and protected from the threat of fear of doing or not doing something that is a human right." The limitations of existing legal frameworks in governing AI risk undermine human dignity and neglect the fundamental rights that the state and the law must guarantee.⁵⁰

⁴⁰ Nehaluddin Ahmad, Aqilah Walin Ali, and Mohammad Hilmy Baihaqy Bin Yussof, "The Challenges of Human Rights in the Era of Artificial Intelligence," *UUM Journal of Legal Studies* 16, no. 1 (January 2025): 150–69, <https://doi.org/10.32890/uujls2025.16.1.9>.

⁴¹ Kishor Avhad et al., "Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring," *International Journal of Advanced Research in Science, Communication and Technology* 4, no. 2 (August 2024): 528–34, <https://doi.org/10.48175/IJARSCT-19681>.

⁴² Ozlem Ozmen Garibay et al., "Six Human-Centered Artificial Intelligence Grand Challenges," *International Journal of Human-Computer Interaction* 39, no. 3 (February 2023): 391–437, <https://doi.org/10.1080/10447318.2022.2153320>.

⁴³ Urbanisasi and Agusman, "Perlindungan Hukum terhadap Karya Kecerdasan Buatan (AI): Tantangan dan Peluang bagi Sistem HAKI Indonesia: Penelitian," *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan* 4, no. 2 (November 2025): 11575–80, <https://doi.org/10.31004/jerkin.v4i2.3709>.

⁴⁴ Yang Lin and Taorui Guan, "From Safe Harbours to AI Harbours: Reimagining DMCA Immunity for the Generative AI Era," *Journal of Intellectual Property Law & Practice* 20, no. 9 (September 2025): 605–16, <https://doi.org/10.1093/jiplp/jpaf043>.

⁴⁵ Muhammad Akmal Mukhasibi and Selamat Widodo, "Analisis Prinsip Ownership Hak Cipta Terhadap Karya Hasil Artificial Intelligence (AI) Dalam Perspektif Hukum Positif," *Jurnal Penelitian Serambi Hukum* 18, no. 02 (July 2025): 297–307, <https://doi.org/10.59582/sh.v18i02.1337>.

⁴⁶ Deepti Yadav, "Human Rights Protection," *International Journal For Multidisciplinary Research* 7, no. 4 (July 2025): 1–20, <https://doi.org/10.36948/ijfmr.2025.v07i04.51897>.

⁴⁷ Vincent Blok, "The Role of Human Creativity in Human-Technology Relations," *Philosophy & Technology* 35, no. 59 (September 2022): 1–19, <https://doi.org/10.1007/s13347-022-00559-7>.

⁴⁸ Steven Livingston and Mathias Risse, "The Future Impact of Artificial Intelligence on Humans and Human Rights," *Ethics & International Affairs* 33, no. 02 (2019): 141–58, <https://doi.org/10.1017/S089267941900011X>.

⁴⁹ Loso Judijanto and Rabith Madah Khulaili Harsya, "Etika dan Hukum dalam Penggunaan Artificial Intelligence terhadap Privasi Digital di Indonesia," *Sanskara Hukum Dan HAM* 3, no. 03 (April 2025): 141–49, <https://doi.org/10.58812/shh.v3i03.543>.

⁵⁰ Hari Sutra Disemadi and Lu Sudirman, "Reassessing Legal Recognition of AI: Human Dignity and the Challenge of AI as a Legal Subject in Indonesia," *Masalah-Masalah Hukum* 54, no. 1 (March 2025): 1–12, <https://doi.org/10.14710/mmh.54.1.2025.1-12>.

3.2. A Comparison of Artificial Intelligence Regulatory Frameworks in Indonesia and the European Union, China, and the United States

3.2.1. Artificial Intelligence Regulations in Indonesia

Regulations on AI in Indonesia remain limited, and the current legal framework is insufficiently specific and comprehensive to be codified in a separate regulation. Regulations on aspects related to AI still depend on the interpretation and application of existing laws and regulations, particularly Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 on Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, and the second amendment through Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as Law Number 27 of 2022 concerning Personal Data Protection. This constellation shows that AI regulation remains scattered across various sectoral laws, without a single legal framework explicitly and systematically designed to address the characteristics of AI technology and its implications for human rights.

The Electronic Information and Transactions Law (ITE Law) does not explicitly define AI.⁵¹ The regulation only recognizes the concept of “electronic agent” or “device in an electronic system that autonomously performs predetermined actions on electronic information” as defined in Article 1 point 8 of Law Number 11 of 2008, which reads: “An Electronic Agent is a device of an Electronic System that is made to act on certain Electronic Information automatically, which is organized by a Person.” The first amendment to the ITE Law in 2016 and the second amendment in 2024 focus more on adjusting provisions regarding responsibility, strengthening law enforcement instruments, and protecting against the misuse of electronic systems. The enactment of Law No. 1 of 2024 as the second amendment to Law No. 11 of 2008 significantly improves the legal framework for electronic transactions, but it does not directly address AI-specific issues, particularly the design, development, and supervision of AI systems that have the potential to violate human rights.

Considering the evidence above, the characterization of AI in Indonesia, described simply as an “electronic agent,” appears too broad and, for regulatory purposes, needs to capture the complexity of AI technology.⁵² Research by A.A. Shchitova entitled “Definition of Artificial Intelligence for Legal Regulation,” reinforces this view by arguing that, in many jurisdictions, the concept of AI is based on misunderstandings about its nature and function. The findings show that an imprecise understanding of AI can hinder the development of effective regulations.⁵³ Based on this analysis, the formulation of norms in the Indonesian legal system, including the legislative process, does not fully reflect an adequate understanding of the definition and characteristics of AI.

Law No. 27 of 2022 on Personal Data Protection provides an important foundation for protecting the right to privacy and individual control over personal data. This regulation complements several other policy instruments related to AI, including the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics and the Guidelines for a Responsible and Trustworthy Artificial Intelligence Code of Ethics in the Financial Technology Industry compiled by the OJK. These instruments contain ethical principles such as transparency, accountability, prudence, and consumer and

⁵¹ Happy Sturaya Quratuainniza and Ema Nurkhaerani, “Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia,” *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 4, no. 1 (December 2025): 71–87, <https://doi.org/10.59246/aladalah.v4i1.1694>.

⁵² Ferdinand Lisaldy, Ismail, and Dewi Iryani, “Lex AI Sebagai Tata Kelola Kecerdasan Buatan Sui Generis di Indonesia,” *Technology and Economics Law Journal* 3, no. 1 (November 2024): 429–44, <https://doi.org/10.21143/TELJ.vol3.no1.1051>.

⁵³ A.A. Shchitova, “Definition of Artificial Intelligence for Legal Regulation,” *Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)* 156 (2020): 616–20, <https://doi.org/10.2991/aebmr.k.201205.104>.

personal data protection. However, their legal character remains that of guidelines and does not constitute a clear, AI-specific obligation under the law.⁵⁴

The Indonesian government has also developed the 2020-2045 Indonesian National Artificial Intelligence Strategy as a national policy direction that sets out areas of focus, priority areas, and development and utilization initiatives for AI.⁵⁵ This document serves as a reference for ministries, institutions, local governments, and other stakeholders to carry out activities in the field of AI. The national strategy contains principles in ethics, governance, talent development, data infrastructure, research, and industrial innovation.⁵⁶ However, it remains a policy document and lacks the binding force of a law that directly stipulates the rights, obligations, and mechanisms of legal accountability for the use of AI.

This fragmented regulatory configuration shows that Indonesia has only reached the stage of indirect regulation of AI through the Electronic Information and Transaction Law and its two amendments, the Personal Data Protection Law, and various sectoral ethical guidelines and national policy documents. This framework lacks norms specifically designed to regulate AI. There are no explicit AI-specific provisions that define AI, no regulations governing the technical characteristics and behavior of AI systems, and no risk classification that distinguishes between low, medium, and high-risk AI use. Current regulations face limitations in setting standards for governance, accountability mechanisms, or transparency obligations in automated decision-making processes, including limitations on obligations for algorithmic impact assessments, algorithmic bias audits, or effective human oversight. The lack of AI-specific sanctions for the misuse of AI further widens the gap between technological developments and available legal instruments.⁵⁷ These conditions are insufficient to manage AI-related challenges, particularly due to the lack of explicit AI-specific regulatory mechanisms, including risks of algorithmic discrimination, privacy violations, manipulation of personal data, and uncertainty about legal accountability for decisions made by AI systems.⁵⁸

3.2.2. Regulation of Artificial Intelligence in the European Union

The human rights protection framework in the EU provides a strong foundation for the development of AI regulation. The 1950 European Convention on Human Rights establishes the right to privacy as a fundamental right that all member states must guarantee.⁵⁹ Scholars and policymakers began to recognize the protection of personal data as an essential element of human rights in the 1970s, marking a shift toward broader informational rights. The 2000 Charter of Fundamental Rights of the European Union, which became legally binding in 2009, explicitly

⁵⁴ Muhammad Naufal Aulia, "Kebijakan Etika dalam Pengembangan dan Penggunaan Kecerdasan Buatan di Indonesia," *Fakultas Teknologi Maju dan Multidisiplin Universitas Airlangga* (Surabaya), May 26, 2025, <https://ftmm.unair.ac.id/kebijakan-etika-dalam-pengembangan-dan-penggunaan-kecerdasan-buatan-di-indonesia/>, accessed on December 6, 2025.

⁵⁵ Edo Aryanto, Hijriatul Mabruk, and Wiryawan Narendroputro, "Artificial Intelligence Implementation Strategy to Make It Happen Smart Government Indonesia Gold 2045," *International Journal of Science and Society* 5, no. 5 (October 2023): 172–97, <https://doi.org/10.54783/ijssoc.v5i5.877>.

⁵⁶ Andrian Putra, *Roadmap AI: Indonesia Menuju Era Kecerdasan Buatan*, August 29, 2025, <https://msbu.co.id/blog/roadmap-ai-indonesia-menuju-era-kecerdasan-buatan>, accessed on December 6, 2025.

⁵⁷ Anggada Perkasa, Andini Pratiwi Siregar, and Venia Utami Keliat, "The Urgency of Establishing Legal Instruments Against Potential Artificial Intelligence (AI) Crimes," *Jurnal Ilmu Hukum Prima* 8, no. 1 (April 2025): 91–97.

⁵⁸ Issa Saidi, "The Legal Vacuum in Global AI Governance: Issues and Opportunities," *Science of Law* 2025, no. 2 (June 2025): 252–55, <https://doi.org/10.55284/vz4j8696>.

⁵⁹ Michaela Padden and Andreas Öjehag-Pettersson, "Protected How? Problem Representations of Risk in the General Data Protection Regulation (GDPR)," *Critical Policy Studies* 15, no. 4 (October 2021): 486–503, <https://doi.org/10.1080/19460171.2021.1927776>.

affirms the right to the protection of personal data as part of the fundamental rights guaranteed by the EU.⁶⁰

The General Data Protection Regulation (GDPR) was a pivotal legislative framework in the 2010s and applies to all EU member states.⁶¹ The Council of Europe's Convention 108+ on Data Protection, which was adopted in 2018, and the EU's 2016 GDPR reinforce the principle that personal data protection is a crucial component in advancing human rights. The GDPR serves as the primary legal instrument establishing the rights of data subjects, including the right of access, the right to obtain information, the right to challenge data processing, data portability, explicit consent and its withdrawal, data correction, the right to request the erasure of their data, and the right to compensation.⁶² The GDPR also has extraterritorial jurisdiction, protecting every individual within the EU regardless of nationality, and regulating cross-border data transfers to non-EU countries when controllers outside the EU process the personal data of EU citizens.⁶³

Protecting the private data of individuals constitutes a fundamental human right, which is obligatory and deserving of protection, as articulated in Article 8 of the European Union Charter of Fundamental Rights. Including personal data protection alongside other rights and freedoms within the framework of the EU's human rights marks a significant advancement for the protection of individuals' rights across the EU. However, it can be argued that the Charter's right to personal data protection does not meet the criteria for a human right and is considered an ordinary consumer right.⁶⁴ The right to personal data protection is also stipulated in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). Following the GDPR, collecting, processing, and analyzing personal data of individuals necessitates a rigorous adherence to fundamental rights aimed at preventing discrimination and underscoring the imperative for transparent information dissemination.⁶⁵

The European Union Regulation on AI (Regulation (EU) 2024/1689) employs a risk-based and rights-protective methodology, thereby instituting an extensive policy framework within the EU concerning AI that exerts a collective influence. This regulation marks a pioneering legal framework for AI, establishing safety principles, transparency, non-discrimination, traceability, and environmental sustainability.⁶⁶ The EU AI Act maps the risks of using AI into three tiers: high risk, low or minimal risk, and unacceptable risk.⁶⁷

The EU AI Act establishes a binding set of provisions to guarantee the protection of human rights. Article 5 prohibits AI practices that threaten human dignity and fundamental rights, including subconscious manipulation, exploitation of vulnerable groups, social scoring systems, and the use of real-time biometric recognition in public spaces without clear restrictions. Article 6(1) establishes a classification of high-risk AI systems covering critical sectors such as the judiciary, employment, education, health, critical infrastructure, and public administration. Article 9(2) requires providers of high-risk AI systems to establish, implement, and maintain a continuous

⁶⁰ Frederik J. Zuiderveen Borgesius, "Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence," *The International Journal of Human Rights* 24, no. 10 (November 2020): 1572–93, <https://doi.org/10.1080/13642987.2020.1743976>.

⁶¹ David Erdos, "Assessing UK Data Protection Reform in Transnational Context: What New Direction?," *SSRN Electronic Journal*, Paper No. 28/2021, 2021, 1–28, <https://doi.org/10.2139/ssrn.3940308>.

⁶² Oskar Josef Gstrein and Andrej Janko Zwitter, "Extraterritorial Application of the GDPR: Promoting European Values or Power?," *Internet Policy Review* 10, no. 3 (September 2021): 1–30, <https://doi.org/10.14763/2021.3.1576>.

⁶³ Bo Zhao and Weiquan Chen, "Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Extraterritorial Application in China," *US-China Law Review* 16, no. 3 (March 2019): 97–113, <https://doi.org/10.17265/1548-6605/2019.03.002>.

⁶⁴ Bart Custers and Gianclaudio Malgieri, "Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data," *Computer Law & Security Review* 45 (July 2022): 1–11, <https://doi.org/10.1016/j.clsr.2022.105683>.

⁶⁵ Runshan Fu, Yan Huang, and Param Vir Singh, "AI and Algorithmic Bias: Source, Detection, Mitigation and Implications," *SSRN Electronic Journal*, 2020, 1–35, <https://doi.org/10.2139/ssrn.3681517>.

⁶⁶ Celso Cancela-Outeda, "The EU's AI Act: A Framework for Collaborative Governance," *Internet of Things* 27 (October 2024): 1–11, <https://doi.org/10.1016/j.iot.2024.101291>.

⁶⁷ Giusella Finocchiaro, "The Regulation of Artificial Intelligence," *AI & SOCIETY* 39, no. 4 (August 2024): 1961–68, <https://doi.org/10.1007/s00146-023-01650-z>.

risk management system throughout the system's lifecycle, from design and development to deployment and post-market monitoring. Article 10 sets out data governance standards to ensure data quality, integrity, and representativeness, thereby minimizing algorithmic bias. The integration of these four provisions shows that the EU aims to identify human rights risks before developers deploy AI on a wide scale.

The accountability structure is reinforced by Article 13, which requires providers to give users adequate information for conscious and responsible technology use. Article 14 establishes a human oversight mechanism to ensure that automated decisions remain under human control. Article 16 requires high-risk AI providers to meet technical and administrative standards, including technical documentation, post-market monitoring, and internal audit capabilities. Article 29 sets out obligations for users or deployers to conduct impact assessments, perform operational oversight, and protect vulnerable groups. Articles 50(1) to 50(4) regulate the obligation to label synthetic content and deepfakes as a form of protection against misinformation, public manipulation, and privacy violations. Labelling is adding information or marks to content to indicate who created it or where it originated. This can also indicate that AI created the content and where it came from.⁶⁸ Article 71 imposes severe administrative sanctions for violations that threaten public safety or fundamental rights. Collectively, these provisions demonstrate the systematic integration of human rights principles into AI regulation, including transparency, accountability, and prudence.

The EU regulatory framework emphasizes that AI must be subject to human values and must not pose a threat to fundamental rights. This approach provides a concrete example of how countries can build regulatory structures that are responsive to technological developments while safeguarding human rights. Indonesia still faces significant regulatory gaps in governing AI, particularly due to limitations in AI-specific definitions, risk classification mechanisms, data governance standards, human oversight obligations, and sanctions tailored to AI-related risks. Indonesia can adopt relevant articles of the AI Act with necessary adjustments, including provisions on high-risk practices, risk classification, transparency obligations, data governance, human oversight, provider and user obligations, and administrative sanctions. This adoption has the potential to provide a strong foundation for building an AI legal framework that protects human rights and ensures the safe and responsible use of technology in Indonesia.

3.2.3. Regulation of Artificial Intelligence in China

China has been a major player in AI research and development in recent years, making significant progress in market infrastructure, regulatory frameworks, and technological research, supported by a highly structured, systematic regulatory framework and national strategies aligned with its AI priorities.⁶⁹ China's national strategy on AI views digital technology as an important instrument to enhance the country's capacity in industry, education, security, and public administration.⁷⁰ The central government and local authorities in major cities such as Beijing, Shanghai, and Shenzhen use AI for transportation optimization, public services, law enforcement, and data management, enabling rapid and widespread technology integration into people's lives.⁷¹ In conjunction with central government initiatives, many major urban centers have instituted policies to promote AI development and research, including through the 2017 National

⁶⁸ Mimi Zou and Lu Zhang, "Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models," *Cambridge Forum on AI: Law and Governance* 1 (2025): 1–16, <https://doi.org/10.1017/cfl.2024.4>.

⁶⁹ Anton Saveliev and Denis Zhurenkov, "Artificial Intelligence and Social Responsibility: The Case of the Artificial Intelligence Strategies in the United States, Russia, and China," *Kybernetes* 50, no. 3 (March 2021): 656–75, <https://doi.org/10.1108/K-01-2020-0060>.

⁷⁰ Shaleen Khanal, Hongzhou Zhang, and Araz Taeihagh, "Development of New Generation of Artificial Intelligence in China: When Beijing's Global Ambitions Meet Local Realities," *Journal of Contemporary China* 34, no. 151 (January 2025): 19–42, <https://doi.org/10.1080/10670564.2024.2333492>.

⁷¹ Tan Yigitcanlar et al., "Unlocking Artificial Intelligence Adoption in Local Governments: Best Practice Lessons from Real-World Implementations," *Smart Cities* 7, no. 4 (June 2024): 1576–625, <https://doi.org/10.3390/smartcities7040064>.

Strategy on AI Development promulgated by the State Council, which has attracted significant global interest by articulating a comprehensive vision for achieving global leadership in AI.⁷²

China's regulatory framework prioritizes national security, social order, and data protection in its regulation of AI. The 2021 Personal Information Protection Law (PIPL) is the most important legal instrument in regulating the processing of personal data, including the use of data for training AI models.⁷³ Article 13 requires explicit consent before data processing, Article 24 prohibits algorithmic discrimination that results in unfair treatment of individuals based on personal characteristics, Article 28 provides exceptional protection for sensitive data, and Article 58 requires businesses to conduct data security impact assessments to ensure there are no systemic risks to privacy rights and public safety. The 2017 Cybersecurity Law complements this framework through Articles 41 to 43, which establish the right of individuals to be informed of data collection purposes, to give consent, and to request correction of inaccurate data or deletion of unlawfully collected data. This framework serves as the basis for protecting human rights in the digital domain, despite operating within a strict state-controlled space.

More specific artificial intelligence regulations appear in the 2022 Provisions on the Administration of Algorithm Recommendation Services, which govern the use of recommendation algorithms on large-scale digital platforms. Article 7 requires providers to implement algorithmic audit mechanisms, maintain model security, and protect personal data. Articles 8 and 9 mandate periodic risk assessments to prevent dependency, addictive behavior, or biases that could harm certain groups. These provisions reflect regulatory concern for protecting user rights in automated decision-making. Article 16 strengthens user rights by requiring providers to give clear information about algorithmic use and allowing users to refuse personalized recommendations. Articles 17 to 19 extend protection to vulnerable groups, including children and the elderly, by requiring providers to ensure that recommendation services do not cause harmful or detrimental effects. The integration of these provisions demonstrates sustained attention to transparency, anti-discrimination, and the protection of vulnerable groups in algorithmic technology governance.

New regulations related to generative AI appear in the 2023 Interim Measures for the Administration of Generative Artificial Intelligence Services.⁷⁴ Article 4 requires providers to ensure that AI-generated content complies with the state's moral and ethical values and does not threaten national security. Article 7 mandates the use of lawful and accurate training data, Article 11 establishes a mechanism for filtering and correcting content that may be discriminatory or contain false information, and Article 12 requires providers to protect user privacy, including limiting the use of sensitive data in model training. These regulations demonstrate that the Chinese government considers data accuracy, content security, and privacy protection essential to the governance of generative AI technology.

Generative AI can copy and create works similar to human-made works, such as photos, films, audio, and text, creating increasing interdependence between human society and artificial systems through extended interaction and advanced generative capabilities. At the same time, this development presents significant human rights challenges, including data breaches and the dissemination of false or misleading information.⁷⁵ China's generative AI regulations establish state-centered regulatory oversight by setting minimum criteria for integrating generative AI into the data development and legal governance cycle.⁷⁶ Providers of generative AI services capable of influencing public opinion or triggering social action are required to undergo security

⁷² Jeremy Knox, "Artificial Intelligence and Education in China," *Learning, Media and Technology* 45, no. 3 (July 2020): 298–311, <https://doi.org/10.1080/17439884.2020.1754236>.

⁷³ Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity* 8, no. 1 (January 2022): 1–12, <https://doi.org/10.1093/cybsec/tyac011>.

⁷⁴ Sara Migliorini, "China's Interim Measures on Generative AI: Origin, Content and Significance," *Computer Law & Security Review* 53 (July 2024): 1–7, <https://doi.org/10.1016/j.clsr.2024.105985>.

⁷⁵ Xinxin Li, "Research on Data Risks and Regulations of Generative Artificial Intelligence," *Journal of Theory and Practice of Management Science* 5, no. 4 (2025): 20–24, [https://doi.org/10.53469/jtpms.2025.05\(4\).05](https://doi.org/10.53469/jtpms.2025.05(4).05).

⁷⁶ Yuzhuo Shi, "Study on Security Risks and Legal Regulations of Generative Artificial Intelligence," *Science of Law Journal* 2, no. 11 (2023): 17–23, <https://doi.org/10.23977/law.2023.021104>.

evaluations and comply with algorithm registration and recording requirements, as stipulated in Article 17 of the Algorithm Recommendation Guidelines.

The Cyberspace Administration of China (CAC) recently issued the Final Rules on Labeling of Content Generated by AI and the mandatory national standard GB 45438-2025 Cyber Security Technology-Methods for Labeling Content Generated by AI (hereinafter referred to as the Labeling Rules). The Rules took effect on September 1, 2025, as stated in the Notice on Issuing Measures for AI Generation and Identification of Synthetic Content.⁷⁷ The Chinese government imposes strict oversight and licensing requirements that obligate AI content providers and developers to add explicit labels (clearly visible to end users) or both implicit labels (embedded in content metadata) to the synthetic content they produce.⁷⁸

China's legal framework shows that the country prioritizes national security, social stability, and control over technological risks. Human rights protection remains incorporated through prohibitions on algorithmic discrimination, personal data protection rules, transparency obligations, and safeguards for vulnerable groups. However, the government implements these protections within the boundaries of state policy. This divergence in regulatory orientation indicates that Indonesia cannot adopt China's model in its entirety due to differences in constitutional values and governance models. Several provisions, such as synthetic content labeling, algorithmic audit obligations, risk assessments, and discrimination bans, can nevertheless significantly strengthen human rights protection in Indonesia's forthcoming artificial intelligence regulations. The implementation of these provisions is highly relevant to the Indonesian context.

The development of clear guidelines on content labeling constitutes a fundamental step prior to the dissemination of content generated or modified by AI in the public sphere. Labeling mechanisms should incorporate easily recognizable visual indicators and integrated metadata to ensure transparency and public access to information.⁷⁹ The rapid advancement of AI has facilitated the proliferation of deepfakes, disinformation, and other forms of visual manipulation that threaten the rights to information, privacy, and public safety. Labeling systems also support law enforcement and forensic investigations by enabling the traceability of synthetic content. In this regard, the labeling practices implemented by the People's Republic of China on social media platforms such as TikTok and WeChat may serve as a practical reference for Indonesia in developing AI content labeling mechanisms to strengthen transparency, accountability, and human rights protection.⁸⁰

3.2.4. Artificial Intelligence Regulations in the United States

The U.S. adopts a sectoral approach to regulating AI, which does not rely on a single comprehensive federal statute governing AI as an integrated legal regime.⁸¹ Instead, federal agencies develop policies within their respective sectoral authorities, shaping AI governance

⁷⁷ Yan Luo and Xuezi Dan, *China Releases New Labeling Requirements for AI-Generated Content*, March 18, 2025, <https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/>, accessed on May 5, 2025.

⁷⁸ Xiangwei He and Lijuan Fang, "Regulatory Challenges in Synthetic Media Governance: Policy Frameworks for AI-Generated Content Across Image, Video, and Social Platforms," *Journal of Robotic Process Automation, AI Integration, and Workflow Optimization* 9, no. 12 (December 2024): 36–54.

⁷⁹ Jasper David Brüns and Martin Meißner, "Do You Create Your Content Yourself? Using Generative Artificial Intelligence for Social Media Content Creation Diminishes Perceived Brand Authenticity," *Journal of Retailing and Consumer Services* 79 (July 2024): 1–15, <https://doi.org/10.1016/j.jretconser.2024.103790>.

⁸⁰ Farhan Arda Nugraha and Natisha Andarningtyas, *Platform Media Sosial di China Wajib Beri Label untuk Konten Buatan AI*, September 3, 2025, <https://www.antaranews.com/berita/5085161/platform-media-sosial-di-china-wajib-beri-label-untuk-konten-buatan-ai>, accessed on December 6, 2025.

⁸¹ Sandeep Reddy, "Global Harmonization of Artificial Intelligence-Enabled Software as a Medical Device Regulation: Addressing Challenges and Unifying Standards," *Mayo Clinic Proceedings: Digital Health* 3, no. 1 (March 2025): 1–13, <https://doi.org/10.1016/j.mcpdig.2024.100191>.

through a combination of voluntary frameworks, data privacy regulations, and state laws.⁸² This federal structure allows states to independently enact AI regulations, as demonstrated by the Colorado AI Act enacted in 2024. Such a decentralized regulatory model reflects an approach that prioritizes technological flexibility, market innovation, and the distribution of regulatory authority within the U.S. government.

The voluntary framework plays a central role through the AI Risk Management Framework (AI RMF) published by the National Institute of Standards and Technology (NIST). This framework guides AI developers and providers in identifying, assessing, and mitigating risks throughout the system lifecycle. The AI RMF emphasizes privacy protection, anti-discrimination, transparency, and security as key ethical principles in AI design.⁸³ The federal government reinforced the implementation of the AI RMF through Memoranda M-25-21 and M-25-22, which direct government agencies to apply AI responsibly and maintain public trust through consistent governance.⁸⁴

State legislatures in the U.S. expanded privacy protections through the 2018 California Consumer Privacy Act (CCPA), the first comprehensive privacy law in the country. The CCPA grants consumers the right to access, correct, and delete their personal data, as well as the right to opt out of the sale or sharing of their personal data with third parties.⁸⁵ Section 1798.100 requires businesses to notify consumers of the categories of data collected and the purposes of processing, while Section 1798.120 provides individuals with the right to opt out of the sale or sharing of data, directly affecting the use of personal data in automated decision-making systems. The California Privacy Rights Act (CPRA) of 2020 further updated and expanded the CCPA by introducing additional consumer rights, including the right to correct inaccurate personal information and to restrict the use and disclosure of sensitive personal information.⁸⁶ Section 1798.185 mandates the formulation of implementing regulations governing automated decision-making technology, including notification obligations, the right to understand the general logic of automated systems, and the right to object to automated decisions with significant impacts. Although these provisions are still under development, they demonstrate a regulatory direction increasingly responsive to AI-related risks.

Colorado has enacted the most progressive AI regulations in the U.S. through the Colorado AI Act, also known as Senate Bill 24-205 (SB 24-205). The act is the first state-level legal instrument to explicitly regulate high-risk AI systems and impose comprehensive obligations on both AI developers and deployers.⁸⁷ Section 6-1-1702 establishes definitions and fundamental principles, including definitions of algorithmic discrimination, developers' due diligence obligations, and technical documentation on training data, model limitations, and foreseeable discrimination risks. Section 6-1-1703 imposes extensive obligations on operators of high-risk AI systems, requiring them to implement risk-management policies, conduct ongoing monitoring, and perform impact assessments before and during system use. This section also requires

⁸² Bambang Slamet Eko Sugistiyoko and Aulia Rahman Hakim, "Eksistensi Manusia sebagai Subjek Hukum di Era Kecerdasan Buatan: Kajian Hukum dan Etika untuk Reformasi Regulasi di Indonesia," *Yustitiabelen* 11, no. 2 (July 2025): 116–38, <https://doi.org/10.36563/yustitiabelen.v11i2.1719>.

⁸³ Nandhini Swaminathan and David Danks, "Governing Ethical Gaps in Distributed AI Development," *Digital Society* 3, no. 1 (May 2024): 7, <https://doi.org/10.1007/s44206-024-00088-0>.

⁸⁴ Yi Peng and Yong Tang, "Artificial Intelligence in International Immigration Management: A Comparative Legal Analysis of the United States, Canada, and the European Union," *Critical Humanistic Social Theory* 2, no. 2 (May 2025): 1–7, <https://doi.org/10.62177/chst.v2i2.413>.

⁸⁵ Vasiliki Rahimzadeh, "A Policy and Practice Review of Consumer Protections and Their Application to Hospital-Sourced Data Aggregation and Analytics by Third-Party Companies," *Frontiers in Big Data* 3 (February 2021): 1–7, <https://doi.org/10.3389/fdata.2020.603044>.

⁸⁶ Lars Hornuf, Sonja Mangold, and Yayun Yang, "Data Protection Law in Germany, the United States, and China," in *Data Privacy and Crowdsourcing*, by Lars Hornuf, Sonja Mangold, and Yayun Yang, Advanced Studies in Diginomics and Digitalization (Cham: Springer Nature Switzerland, 2023), 19–79, https://doi.org/10.1007/978-3-031-32064-4_3.

⁸⁷ Mayur Jariwala, "A Comparative Analysis of the EU AI Act and the Colorado AI Act: Regulatory Approaches to Artificial Intelligence Governance," *International Journal of Computer Applications* 186, no. 38 (September 2024): 23–29, <https://doi.org/10.5120/ijca2024923954>.

deployers to notify individuals before an automated decision affects their education, employment, credit, public services, health, housing, or insurance. Section 6-1-1704 requires AI system providers to disclose to consumers that they are interacting with an AI system, unless the circumstances already make this evident. Sections 6-1-1705 and 6-1-1706 regulate enforcement mechanisms, legal exceptions, and the authority of the Colorado Attorney General to ensure compliance. The regulatory structure of SB 24-205 demonstrates an approach explicitly oriented toward protecting human rights, particularly in non-discrimination, algorithmic transparency, access to information, and appeal mechanisms. The obligation to provide notification before deployers make an automated decision reflects the human-in-the-loop principle, which normatively strengthens the protection of individual autonomy.⁸⁸

Federal legislative initiatives are also proposed through S. 2691, the AI Labeling Act of 2023, a bill that establishes labeling requirements for synthetic content generated or modified by AI. The bill requires technology providers to display clear and legible disclosures, including through metadata, on images, videos, audio, or text created by AI. This provision aims to protect the public from disinformation, deepfakes, and other forms of digital manipulation that threaten the right to information and human dignity.⁸⁹ Strengthened protection of human rights is also evident in the American Data Privacy and Protection Act (ADPPA) of 2022, a federal bill that includes the principles of non-discrimination and personal data protection. Section 207 of the ADPPA prohibits the use or dissemination of data that results in unfair treatment based on race, gender, religion, national origin, or disability, and requires specific organizations to conduct discriminatory impact assessments on algorithms. Although not yet passed, the ADPPA signals the legislative direction of federal policy toward AI governance, with a focus on protecting human rights.⁹⁰

This fragmented regulatory model demonstrates that the U.S. is developing AI governance through a combination of complementary regulatory instruments, including voluntary frameworks, sectoral regulations, state privacy laws, and emerging federal initiatives. This regulatory structure establishes human rights-relevant protection mechanisms, particularly regarding privacy, non-discrimination, transparency, and algorithmic accountability. Indonesia can draw on these regulatory elements, with adjustments to its constitutional and legal framework, by adapting principles of automated decision-making transparency reflected in the CPRA, impact assessment, and risk oversight mechanisms under the Colorado AI Act 2024, and synthetic content labeling requirements proposed in the AI Labeling Act 2023. Integrating these elements can strengthen human rights protection in Indonesia by ensuring that the use of AI remains transparent, non-discriminatory, and accountable under the rule of law.

3.2.5. Comparative Analysis of Artificial Intelligence Regulations in Indonesia with the European Union, China, and the United States

A comparison of AI policies in Indonesia, the EU, China, and the U.S. shows fundamental differences in their approaches to regulating AI. Indonesia's AI governance is in its infancy, and its legal framework has yet to adopt dedicated and comprehensive AI-specific legislation. Existing regulations rely solely on the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, and several non-binding ethical guidelines. The lack of explicit AI-specific definitions, risk classification mechanisms, algorithmic audit requirements, human oversight obligations, and synthetic content labeling standards reveals significant regulatory gaps in Indonesia's current legal framework. This situation directly weakens the protection of privacy rights, non-discrimination, and legal certainty under the current regulatory framework regarding responsibility for automated decisions and AI-generated content.

⁸⁸ Bibars Amangeldy et al., "AI-Powered Building Ecosystems: A Narrative Mapping Review on the Integration of Digital Twins and LLMs for Proactive Comfort, IEQ, and Energy Management," *Sensors* 25, no. 17 (August 2025): 5265, <https://doi.org/10.3390/s25175265>.

⁸⁹ Sandra Höltervennhoff et al., "Security Benefits and Side Effects of Labeling AI-Generated Images," version 1, preprint, arXiv, 2025, <https://doi.org/10.48550/ARXIV.2505.22845>.

⁹⁰ Evangelos Razis and James C. Cooper, "The Federalist's Dilemma: State AI Regulation & Pathways Forward," preprint, SSRN, 2025, <https://doi.org/10.2139/ssrn.5283472>.

The EU has developed the most comprehensive regulatory framework through the EU AI Act, which places human rights protection at its core. This regulation governs the definition of AI, risk categories, the obligations of developers and users of high-risk systems, and mechanisms for labeling synthetic content. China adopts a different approach by emphasizing national security and social stability through regulations on algorithms, generative AI, recommendation services, and synthetic content labeling obligations. The U.S. has adopted a fragmented approach, with the federal government developing voluntary frameworks such as the AI Risk Management Framework (AI RMF). In contrast, states such as Colorado have passed the Colorado AI Act, or Senate Bill 24-205 (SB 24-205), which imposes obligations for transparency, impact assessment, the prevention of algorithmic discrimination, and notification to individuals before deployers implement automated decisions. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) further strengthen consumer protection in the use of data and automated decision-making systems.

The comparison shows that, unlike the EU, China, and the U.S., Indonesia remains the only jurisdiction without a dedicated and comprehensive AI-specific regulatory framework. The EU model provides an example of risk-based and human-rights-oriented regulation. The Chinese model demonstrates the importance of technical mechanisms such as algorithm labeling and auditing, while the U.S. model shows how transparency, accountability, and consumer protection develop through a combination of federal and state frameworks. These three models offer clear guidance for Indonesia in formulating AI regulations to address challenges such as algorithmic discrimination, privacy violations, digital disinformation, and legal uncertainty arising from the use of AI technology.

3.3. Recommendations

The comparison results show that Indonesia needs to develop a comprehensive legal framework to regulate AI because Law Number 11 of 2008 concerning Electronic Information and Transactions, along with its two amendments through Law Number 19 of 2016 and Law Number 1 of 2024, Law No. 27 of 2022 concerning Personal Data Protection, the Ministry of Communication and Information Technology's AI Ethics Circular Letter, and the Guidelines for a Responsible and Trustworthy Artificial Intelligence Code of Ethics in the Financial Technology Industry published by the OJK, fail to adequately address AI-specific regulatory needs arising from AI adoption. The existing legal framework lacks explicit AI-specific provisions, such as definitions of AI, risk classification, mechanisms for algorithmic transparency, labeling of synthetic content, or impact assessment obligations to prevent discrimination and privacy violations.

Indonesia needs to formulate a law on AI to address regulatory gaps and limitations in interpreting AI in accordance with the regulatory framework established in Law No. 12 of 2011. This law defines AI and sets the scope of regulation, principles, objectives, and the obligations of developers and users of the system. The law also needs to adopt key elements from the EU AI Act and the Colorado AI Act, including risk classification, risk assessment obligations, human oversight, algorithmic audits, and a prohibition on discriminatory practices in automated decision-making. These provisions are important to ensure that the use of AI is safe and in line with human rights principles.

The government needs to draft implementing regulations to regulate technical aspects such as dataset documentation, model testing, post-operational monitoring, synthetic content labeling, and supervision procedures. The government also needs to establish an AI supervisory authority within the existing institutional framework tasked with certification, auditing, dispute resolution, and administrative law enforcement. The existence of such an authority will strengthen oversight mechanisms and ensure the accountability of AI developers, providers, and users. These recommendations provide a roadmap for developing a structured and responsive AI regulatory system in Indonesia. By drafting a specific AI law, establishing implementing regulations, and forming a supervisory agency, Indonesia can improve the protection of human rights in a more structured and consistent manner and ensure that AI technology is used responsibly within the national legal ecosystem.

4. Conclusion

This study analyzes the regulatory gaps in Indonesia's artificial intelligence governance from a human rights perspective, compares relevant regulatory approaches adopted in the European Union, China, and the United States, and formulates regulatory recommendations that may be adapted to the Indonesian legal system. Based on doctrinal legal analysis of legislation, legal doctrines, judicial decisions, and relevant international regulatory frameworks, the study finds that the rapid development and deployment of artificial intelligence create substantial risks to the protection of human rights, particularly the rights to privacy, non-discrimination, freedom of expression, and legal certainty. The existing Indonesian legal framework, including Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments through Law Number 19 of 2016 and Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, the Circular Letter of the Ministry of Communication and Information Technology concerning Artificial Intelligence Ethics, and the Artificial Intelligence Code of Conduct Guidelines issued by the Financial Services Authority, has not yet provided a comprehensive regulatory framework specifically designed to address the distinctive characteristics and risks of AI systems. In particular, the absence of an explicit legal definition of artificial intelligence, a risk-based classification mechanism, obligations concerning algorithmic transparency and auditing, requirements for human oversight, mechanisms for assessing algorithmic impacts, and standards for labeling synthetic content demonstrates that Indonesia's current regulatory framework remains insufficient to respond effectively to the human rights implications of AI.

The comparative analysis further demonstrates that several regulatory approaches developed in other jurisdictions may provide relevant normative references for Indonesia. The European Union, through the Artificial Intelligence Act, adopts a risk-based regulatory model that emphasizes the protection of fundamental rights through the classification of AI systems according to levels of risk, technical documentation requirements, conformity and impact assessments, transparency obligations, human oversight, and specific requirements concerning AI-generated and synthetic content. China provides additional regulatory references through its governance of recommendation algorithms, generative artificial intelligence, deep synthesis technologies, security assessments, and mandatory labeling mechanisms for AI-generated content. Meanwhile, developments in the United States, particularly through the Colorado AI Act and privacy legislation such as the California Consumer Privacy Act and the California Privacy Rights Act, demonstrate an approach that emphasizes transparency in automated decision-making, the prevention of algorithmic discrimination, impact assessments, and consumer protection. Although these jurisdictions adopt different regulatory philosophies and institutional structures, their respective frameworks demonstrate a common recognition that AI governance requires legal mechanisms capable of identifying technological risks, allocating accountability, ensuring transparency, and providing safeguards against adverse impacts on individual rights.

In light of these findings, Indonesia needs a more specific and comprehensive legal framework governing artificial intelligence. Such regulation should, at a minimum, establish a clear legal definition and regulatory scope of AI, introduce a risk-based classification of AI systems with particular attention to high-risk applications, impose transparency and accountability obligations for automated decision-making, require algorithmic impact assessments to identify and mitigate discriminatory or systemic effects, establish mandatory labeling requirements for synthetic and AI-generated content, and ensure meaningful human oversight over decisions that may affect individual rights. The regulatory framework should also clearly define the responsibilities of AI developers, deployers, providers, and users, while establishing an independent or designated supervisory authority with adequate powers to conduct certification, auditing, monitoring, and administrative enforcement. These mechanisms are necessary not merely to respond to violations after they occur, but also to provide preventive legal protection against foreseeable risks arising from the development and use of AI technologies.

Accordingly, Indonesia should prioritize the formulation of a specific law on artificial intelligence as the primary legal instrument for ensuring the respect, protection, and fulfillment of human rights in the development and deployment of AI systems. Such legislation should not merely regulate technological innovation, but should establish a rights-based governance

framework that combines preventive safeguards, clearly defined accountability mechanisms, effective institutional supervision, and accessible remedies for individuals affected by AI-driven decisions. A coherent, risk-based, and human-rights-oriented regulatory framework is therefore essential to provide legal certainty, strengthen accountability, and ensure that technological advancement in Indonesia remains consistent with constitutional principles, the rule of law, and the protection of human dignity.

Funding Information

None

Conflicts of Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

References

- Abbass, Hussein A. "Social Integration of Artificial Intelligence: Functions, Automation Allocation Logic and Human-Autonomy Trust." *Cognitive Computation* 11, no. 2 (April 2019): 159–71. <https://doi.org/10.1007/s12559-018-9619-0>.
- Ahmad, Nehaluddin, Aqilah Walin Ali, and Mohammad Hilmy Baihaqy Bin Yussof. "The Challenges of Human Rights in the Era of Artificial Intelligence." *UUM Journal of Legal Studies* 16, no. 1 (January 2025): 150–69. <https://doi.org/10.32890/uumjls2025.16.1.9>.
- Amangeldy, Bibars, Nurdaulet Tasmurzayev, Timur Imankulov, Zhanel Baigarayeva, Nurdaulet Izmailov, Tolebi Riza, Abdulaziz Abdulkarimov, Miras Mukazhan, and Bakdaulet Zhumagulov. "AI-Powered Building Ecosystems: A Narrative Mapping Review on the Integration of Digital Twins and LLMs for Proactive Comfort, IEQ, and Energy Management." *Sensors* 25, no. 17 (August 2025): 5265. <https://doi.org/10.3390/s25175265>.
- Aryanto, Edo, Hijriatul Mabruk, and Wiryawan Narendroputro. "Artificial Intelligence Implementation Strategy to Make It Happen Smart Government Indonesia Gold 2045." *International Journal of Science and Society* 5, no. 5 (October 2023): 172–97. <https://doi.org/10.54783/ijssoc.v5i5.877>.
- Aulia, Muhammad Naufal. "Kebijakan Etika dalam Pengembangan dan Penggunaan Kecerdasan Buatan di Indonesia." *Fakultas Teknologi Maju Dan Multidisiplin Universitas Airlangga* (Surabaya), May 26, 2025. <https://ftmm.unair.ac.id/kebijakan-etika-dalam-pengembangan-dan-penggunaan-kecerdasan-buatan-di-indonesia/>.
- Ballot Jones, Lily, Julia Thornton, and Daswin De Silva. "Limitations of Risk-Based Artificial Intelligence Regulation: A Structuration Theory Approach." *Discover Artificial Intelligence* 5, no. 14 (February 2025): 1–13. <https://doi.org/10.1007/s44163-025-00233-9>.
- Blahuta, Roman I., Olha O. Barabash, Vasyl P. Zakharov, Mariia Yu. Kovalska, and Kateryna R. Dobkina. "Enhancing Human Rights Protections in Ukrainian Law Enforcement: National Compliance with EU Standards." *Yuridika* 39, no. 1 (January 2024): 1–30. <https://doi.org/10.20473/ydk.v39i1.45461>.
- Blok, Vincent. "The Role of Human Creativity in Human-Technology Relations." *Philosophy & Technology* 35, no. 59 (September 2022): 1–19. <https://doi.org/10.1007/s13347-022-00559-7>.
- Bo Zhao and Weiquan Chen. "Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Extraterritorial Application in China." *US-China Law Review* 16, no. 3 (March 2019): 97–113. <https://doi.org/10.17265/1548-6605/2019.03.002>.
- Brüns, Jasper David, and Martin Meißner. "Do You Create Your Content Yourself? Using Generative Artificial Intelligence for Social Media Content Creation Diminishes Perceived

- Brand Authenticity.” *Journal of Retailing and Consumer Services* 79 (July 2024): 1–15. <https://doi.org/10.1016/j.jretconser.2024.103790>.
- Buiten, Miriam C. “Towards Intelligent Regulation of Artificial Intelligence.” *European Journal of Risk Regulation* 10, no. 1 (March 2019): 41–59. <https://doi.org/10.1017/err.2019.8>.
- Buiten, Miriam, Alexandre De Streel, and Martin Peitz. “The Law and Economics of AI Liability.” *Computer Law & Security Review* 48 (April 2023): 1–20. <https://doi.org/10.1016/j.clsr.2023.105794>.
- Cancela-Outeda, Celso. “The EU’s AI Act: A Framework for Collaborative Governance.” *Internet of Things* 27 (October 2024): 1–11. <https://doi.org/10.1016/j.iot.2024.101291>.
- Cecez-Kecmanovic, Dubravka. “Ethics in the World of Automated Algorithmic Decision-Making – A Posthumanist Perspective.” *Information and Organization* 35, no. 3 (September 2025): 1–16. <https://doi.org/10.1016/j.infoandorg.2025.100587>.
- Chen, Bing, and Jiaying Chen. “China’s Legal Practices Concerning Challenges of Artificial General Intelligence.” *Laws* 13, no. 5 (September 2024): 1–14. <https://doi.org/10.3390/laws13050060>.
- Coitinho, Denis, and André Luiz Olivier Da Silva. “Algorithmic Injustice and Human Rights.” *Filosofia Unisinos* 25, no. 1 (March 2024): 1–17. <https://doi.org/10.4013/fsu.2024.251.09>.
- Creemers, Rogier. “China’s Emerging Data Protection Framework.” *Journal of Cybersecurity* 8, no. 1 (January 2022): 1–12. <https://doi.org/10.1093/cybsec/tyac011>.
- Custers, Bart, and Gianclaudio Malgieri. “Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data.” *Computer Law & Security Review* 45 (July 2022): 1–11. <https://doi.org/10.1016/j.clsr.2022.105683>.
- De Almeida, Patricia Gomes Rêgo, Carlos Denner Dos Santos, and Josivania Silva Farias. “Artificial Intelligence Regulation: A Framework for Governance.” *Ethics and Information Technology* 23, no. 3 (September 2021): 505–25. <https://doi.org/10.1007/s10676-021-09593-z>.
- Dewi, Sinta, and Mohammad Wildan Hidayat. “Protection of Data Privacy in The Era of Artificial Intelligence in The Financial Sector in Indonesia.” *Journal of Central Banking Law and Institutions* 1, no. 2 (May 2022): 353–66. <https://doi.org/10.21098/jcli.v1i2.18>.
- Díaz-Rodríguez, Natalia, Javier Del Ser, Mark Coeckelbergh, Marcos López De Prado, Enrique Herrera-Viedma, and Francisco Herrera. “Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation.” *Information Fusion* 99 (November 2023): 101896. <https://doi.org/10.1016/j.inffus.2023.101896>.
- Disemadi, Hari Sutra, and Lu Sudirman. “Reassessing Legal Recognition of AI: Human Dignity and the Challenge of AI as a Legal Subject in Indonesia.” *Masalah-Masalah Hukum* 54, no. 1 (March 2025): 1–12. <https://doi.org/10.14710/mmh.54.1.2025.1-12>.
- Erdos, David. “Assessing UK Data Protection Reform in Transnational Context: What New Direction?” *SSRN Electronic Journal*, Paper No. 28/2021, 2021, 1–28. <https://doi.org/10.2139/ssrn.3940308>.
- Finocchiaro, Giusella. “The Regulation of Artificial Intelligence.” *AI & SOCIETY* 39, no. 4 (August 2024): 1961–68. <https://doi.org/10.1007/s00146-023-01650-z>.
- Fu, Runshan, Yan Huang, and Param Vir Singh. “AI and Algorithmic Bias: Source, Detection, Mitigation and Implications.” *SSRN Electronic Journal*, 2020, 1–35. <https://doi.org/10.2139/ssrn.3681517>.
- Furizal, Alfian Ma’arif, Hari Maghfiroh, Iswanto Suwarno, Denis Prayogi, Kariyamin, Syahrani Lonang, and Abdel-Nasser Sharkawy. “Social, Legal, and Ethical Implications of AI-

- Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review." *Social Sciences & Humanities Open* 12 (2025): 1–25. <https://doi.org/10.1016/j.ssaho.2025.101882>.
- Ghufron Rosadi Hidayah, Ha. Djazim Ma'shum, and Muhammad Awaluddin. "Studi Komparatif Perlindungan Data Pribadi dalam UU ITE 2024 dan UU PDP 2022." *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora* 4, no. 4 (August 2025): 61–70. <https://doi.org/10.55606/jurrish.v4i4.6341>.
- Gstrein, Oskar Josef, and Andrej Janko Zwitter. "Extraterritorial Application of the GDPR: Promoting European Values or Power?" *Internet Policy Review* 10, no. 3 (September 2021): 1–30. <https://doi.org/10.14763/2021.3.1576>.
- Hadjon, Philipus M. *Perlindungan Hukum bagi Rakyat di Indonesia (Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara)*. 1st ed. Surabaya: Bina Ilmu, 1987.
- . *Perlindungan Hukum bagi Rakyat di Indonesia (Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi)*. Special Edition First Printing. Malang: Peradaban, 2007.
- Hah, Hyeyoung, and Deana Shevit Goldin. "How Clinicians Perceive Artificial Intelligence–Assisted Technologies in Diagnostic Decision Making: Mixed Methods Approach." *Journal of Medical Internet Research* 23, no. 12 (December 2021): 1–19. <https://doi.org/10.2196/33540>.
- Harun, M. Syamsuri, and Men Wih Widiyanto. "Criminal Liability for the Theft of Personal Data Using Artificial Intelligence Technology (Case Study of Decision No. 5/Pid.Sus/2023/PN Krg)." *International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy* 1, no. 1 (July 2025): 168–76. <https://doi.org/10.56861/nalarnagara.v1i1.196>.
- He, Xiangwei, and Lijuan Fang. "Regulatory Challenges in Synthetic Media Governance: Policy Frameworks for AI-Generated Content Across Image, Video, and Social Platforms." *Journal of Robotic Process Automation, AI Integration, and Workflow Optimization* 9, no. 12 (December 2024): 36–54.
- Hölttervennhoff, Sandra, Jonas Ricker, Maike M. Raphael, Charlotte Schwedes, Rebecca Weil, Asja Fischer, Thorsten Holz, Lea Schönherr, and Sascha Fahl. "Security Benefits and Side Effects of Labeling AI-Generated Images." Version 1. Preprint, arXiv, 2025. <https://doi.org/10.48550/ARXIV.2505.22845>.
- Hopster, Jeroen K. G., and Matthijs M. Maas. "The Technology Triad: Disruptive AI, Regulatory Gaps and Value Change." *AI and Ethics* 4, no. 4 (November 2024): 1051–69. <https://doi.org/10.1007/s43681-023-00305-5>.
- Hornuf, Lars, Sonja Mangold, and Yayun Yang. "Data Protection Law in Germany, the United States, and China." In *Data Privacy and Crowdsourcing*, by Lars Hornuf, Sonja Mangold, and Yayun Yang, 19–79. Advanced Studies in Diginomics and Digitalization. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-32064-4_3.
- Jariwala, Mayur. "A Comparative Analysis of the EU AI Act and the Colorado AI Act: Regulatory Approaches to Artificial Intelligence Governance." *International Journal of Computer Applications* 186, no. 38 (September 2024): 23–29. <https://doi.org/10.5120/ijca2024923954>.
- Jesslyn, Jesslyn, and Raja Ritonga. "Pengaruh Artificial Intelligence (AI) Terhadap Hak Asasi Manusia." *Jurnal Res Justitia: Jurnal Ilmu Hukum* 5, no. 1 (January 2025): 35–49. <https://doi.org/10.46306/rj.v5i1.135>.

- Judijanto, Loso, and Rabith Madah Khulaili Harsya. "Etika dan Hukum dalam Penggunaan Artificial Intelligence terhadap Privasi Digital di Indonesia." *Sanskara Hukum Dan HAM* 3, no. 03 (April 2025): 141–49. <https://doi.org/10.58812/shh.v3i03.543>.
- Kattnig, Markus, Alessa Angerschmid, Thomas Reichel, and Roman Kern. "Assessing Trustworthy AI: Technical and Legal Perspectives of Fairness in AI." *Computer Law & Security Review* 55 (November 2024): 1–18. <https://doi.org/10.1016/j.clsr.2024.106053>.
- Khanal, Shaleen, Hongzhou Zhang, and Araz Taeihagh. "Development of New Generation of Artificial Intelligence in China: When Beijing's Global Ambitions Meet Local Realities." *Journal of Contemporary China* 34, no. 151 (January 2025): 19–42. <https://doi.org/10.1080/10670564.2024.2333492>.
- Kishor Avhad, Vishal Jadhav, Sahil Kurhade, and Prof. M. V. Raut. "Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring." *International Journal of Advanced Research in Science, Communication and Technology* 4, no. 2 (August 2024): 528–34. <https://doi.org/10.48175/IJARST-19681>.
- Knox, Jeremy. "Artificial Intelligence and Education in China." *Learning, Media and Technology* 45, no. 3 (July 2020): 298–311. <https://doi.org/10.1080/17439884.2020.1754236>.
- Kolodin, Denis, Oksana Telychko, Viktor Rekun, Maxym Tkalych, and Vladyslav Yamkovyi. "Artificial Intelligence in E-Commerce: Legal Aspects." *Proceedings of the III International Scientific Congress Society of Ambient Intelligence 2020 (ISC-SAI 2020)* 129 (2020): 96–102. <https://doi.org/10.2991/aebmr.k.200318.012>.
- Krupiy, Tetyana (Tanya). "A Vulnerability Analysis: Theorising the Impact of Artificial Intelligence Decision-Making Processes on Individuals, Society and Human Diversity from a Social Justice Perspective." *Computer Law & Security Review* 38 (September 2020): 1–25. <https://doi.org/10.1016/j.clsr.2020.105429>.
- Li, Xinxin. "Research on Data Risks and Regulations of Generative Artificial Intelligence." *Journal of Theory and Practice of Management Science* 5, no. 4 (2025): 20–24. [https://doi.org/10.53469/jtpms.2025.05\(4\).05](https://doi.org/10.53469/jtpms.2025.05(4).05).
- Lin, Yang, and Taorui Guan. "From Safe Harbours to AI Harbours: Reimagining DMCA Immunity for the Generative AI Era." *Journal of Intellectual Property Law & Practice* 20, no. 9 (September 2025): 605–16. <https://doi.org/10.1093/jiplp/jpaf043>.
- Lisaldy, Ferdinand, Ismail, and Dewi Iryani. "Lex AI sebagai Tata Kelola Kecerdasan Buatan Sui Generis di Indonesia." *Technology and Economics Law Journal* 3, no. 1 (November 2024): 429–44. <https://doi.org/10.21143/TELJ.vol3.no1.1051>.
- Livingston, Steven, and Mathias Risse. "The Future Impact of Artificial Intelligence on Humans and Human Rights." *Ethics & International Affairs* 33, no. 02 (2019): 141–58. <https://doi.org/10.1017/S089267941900011X>.
- Luo, Yan, and Xuezi Dan. *China Releases New Labeling Requirements for AI-Generated Content*. March 18, 2025. <https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/>.
- Martsenko, Nataliia. "Artificial Intelligence and Human Rights: A Scientific Review of Impacts and Interactions." *Studia Prawnoustrojowe*, no. 58 (December 2022): 326–38. <https://doi.org/10.31648/sp.8245>.
- Mecca, Anggil Syahra Putri, Wahab Aznul Hidayat, and Hadi Tuasikal. "Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) dalam Sistem Peradilan Pidana di Indonesia." *Jurnal Sosial Teknologi* 5, no. 6 (June 2025): 1730–46. <https://doi.org/10.59188/jurnalsostech.v5i6.32207>.

- Migliorini, Sara. "China's Interim Measures on Generative AI: Origin, Content and Significance." *Computer Law & Security Review* 53 (July 2024): 1–7. <https://doi.org/10.1016/j.clsr.2024.105985>.
- Mihaila, Carmen Oana, and Mircea Mihaila. "Artificial Intelligence - The Era of Social Inequalities. In Regulating the Future, We Need to Look at the Risks." *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, May 20, 2024, 39–63. <https://doi.org/10.62768/ADJURIS/2024/1/03>.
- Mufti, M. Wildan, M. Hiroshi Ikhsan, Rafif Sani, and M. Fauzan. "Urgensi Pembentukan Peraturan Perundang-undangan Teknologi Berbasis Artificial Intelligence." *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 11 (June 2024): 137–41. <https://doi.org/10.5281/zenodo.11422903>.
- Mukhasibi, Muhammad Akmal, and Selamat Widodo. "Analisis Prinsip Ownership Hak Cipta terhadap Karya Hasil Artificial Intelligence (AI) dalam Perspektif Hukum Positif." *Jurnal Penelitian Serambi Hukum* 18, no. 02 (July 2025): 297–307. <https://doi.org/10.59582/sh.v18i02.1337>.
- Nisa, Ardina Khoirun. "The Prospect of AI Law in Indonesian Legal System: Present and Future Challenges." *The Indonesian Journal of International Clinical Legal Education* 6, no. 1 (March 2024): 25–48. <https://doi.org/10.15294/iccle.v6i1.4686>.
- Nugraha, Farhan Arda, and Natisha Andarningtyas. *Platform Media Sosial di China Wajib Beri Label untuk Konten Buatan AI*. September 3, 2025. <https://www.antaranews.com/berita/5085161/platform-media-sosial-di-china-wajib-beri-label-untuk-konten-buatan-ai>.
- Ozmen Garibay, Ozlem, Brent Winslow, Salvatore Andolina, Margherita Antona, Anja Bodenschatz, Constantinos Coursaris, Gregory Falco, et al. "Six Human-Centered Artificial Intelligence Grand Challenges." *International Journal of Human–Computer Interaction* 39, no. 3 (February 2023): 391–437. <https://doi.org/10.1080/10447318.2022.2153320>.
- Padden, Michaela, and Andreas Öjehag-Pettersson. "Protected How? Problem Representations of Risk in the General Data Protection Regulation (GDPR)." *Critical Policy Studies* 15, no. 4 (October 2021): 486–503. <https://doi.org/10.1080/19460171.2021.1927776>.
- Parnas, David Lorge. "The Real Risks of Artificial Intelligence." *Communications of the ACM* 60, no. 10 (September 2017): 27–31. <https://doi.org/10.1145/3132724>.
- Perkasa, Anggada, Andini Pratiwi Siregar, and Venia Utami Keliat. "The Urgency of Establishing Legal Instruments Against Potential Artificial Intelligence (AI) Crimes." *Jurnal Ilmu Hukum Prima* 8, no. 1 (April 2025): 91–97.
- Pizzi, Michael, Mila Romanoff, and Tim Engelhardt. "AI for Humanitarian Action: Human Rights and Ethics." *International Review of the Red Cross* 102, no. 913 (April 2020): 145–80. <https://doi.org/10.1017/S1816383121000011>.
- Putra, Andrian. *Roadmap AI: Indonesia Menuju Era Kecerdasan Buatan*. August 29, 2025. <https://msbu.co.id/blog/roadmap-ai-indonesia-menuju-era-kecerdasan-buatan>.
- Quratuainniza, Happy Sturaya, and Ema Nurkhaerani. "Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia." *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 4, no. 1 (December 2025): 71–87. <https://doi.org/10.59246/aladalah.v4i1.1694>.
- Rahardjo, Satjipto. *Ilmu Hukum*. 6th ed. Bandung: PT Citra Aditya Bakti, 2006.
- Rahimzadeh, Vasiliki. "A Policy and Practice Review of Consumer Protections and Their Application to Hospital-Sourced Data Aggregation and Analytics by Third-Party Companies." *Frontiers in Big Data* 3 (February 2021): 1–7. <https://doi.org/10.3389/fdata.2020.603044>.

- Razis, Evangelos, and James C. Cooper. "The Federalist's Dilemma: State AI Regulation & Pathways Forward." Preprint, SSRN, 2025. <https://doi.org/10.2139/ssrn.5283472>.
- Reddy, Sandeep. "Global Harmonization of Artificial Intelligence-Enabled Software as a Medical Device Regulation: Addressing Challenges and Unifying Standards." *Mayo Clinic Proceedings: Digital Health* 3, no. 1 (March 2025): 1–13. <https://doi.org/10.1016/j.mcpdig.2024.100191>.
- Respati, Adnasohn Aqilla. "Reformulasi UU ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation." *JURNAL USM LAW REVIEW* 7, no. 3 (December 2024): 1737–58. <https://doi.org/10.26623/julr.v7i3.10578>.
- Rizki, Mochamad Januar. *Menelaah 3 Putusan Perkara Pelanggaran PDP, Minimnya Literasi dan Tantangannya*. January 6, 2025. <https://www.hukumonline.com/berita/a/menelaah-3-putusan-perkara-pelanggaran-pdp--minimnya-literasi-dan-tantangannya-lt677bd1211839d/>.
- Rodrigues, Rowena. "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities." *Journal of Responsible Technology* 4 (December 2020): 1–12. <https://doi.org/10.1016/j.jrt.2020.100005>.
- Saidi, Issa. "The Legal Vacuum in Global AI Governance: Issues and Opportunities." *Science of Law* 2025, no. 2 (June 2025): 252–55. <https://doi.org/10.55284/vz4j8696>.
- Saputro, Aries and Radian Salman. "Legal and Moral Principles as Guidelines for Carrying Out Official Duties." *Yuridika* 39, no. 2 (May 2024): 127–52. <https://doi.org/10.20473/lydk.v39i2.50496>.
- Saveliev, Anton, and Denis Zhurenkov. "Artificial Intelligence and Social Responsibility: The Case of the Artificial Intelligence Strategies in the United States, Russia, and China." *Kybernetes* 50, no. 3 (March 2021): 656–75. <https://doi.org/10.1108/K-01-2020-0060>.
- Shchitova, A. A. "Definition of Artificial Intelligence for Legal Regulation." *Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)*, December 7, 2020, 616–20. <https://doi.org/10.2991/aebmr.k.201205.104>.
- Shi, Yuzhuo. "Study on Security Risks and Legal Regulations of Generative Artificial Intelligence." *Science of Law Journal* 2, no. 11 (2023): 17–23. <https://doi.org/10.23977/law.2023.021104>.
- Siagian, Agus, and Dony Alexander. "Penerapan Hukum Pidana terhadap Pelaku Tindak Pidana Siber di Indonesia: Analisis Putusan Pengadilan." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 4, no. 9 (2025): 2641–56. <https://doi.org/10.54443/sibatik.v4i9.3360>.
- Stahl, Bernd Carsten, Laurence Brooks, Tally Hatzakis, Nicole Santiago, and David Wright. "Exploring Ethics and Human Rights in Artificial Intelligence – A Delphi Study." *Technological Forecasting and Social Change* 191 (June 2023): 1–17. <https://doi.org/10.1016/j.techfore.2023.122502>.
- Sugistiyoko, Bambang Slamet Eko, and Aulia Rahman Hakim. "Eksistensi Manusia sebagai Subjek Hukum di Era Kecerdasan Buatan: Kajian Hukum dan Etika untuk Reformasi Regulasi di Indonesia." *Yustitiabelen* 11, no. 2 (July 2025): 116–38. <https://doi.org/10.36563/yustitiabelen.v11i2.1719>.
- Swaminathan, Nandhini, and David Danks. "Governing Ethical Gaps in Distributed AI Development." *Digital Society* 3, no. 1 (May 2024): 7. <https://doi.org/10.1007/s44206-024-00088-0>.
- Syalendro, Oky, Arief Fahmi Lubis, and R Yusak Andri Ende Putra. "Cyber Crime Crimes in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases." *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia* 4, no. 1 (December 2024): 335–47. <https://doi.org/10.57235/aurelia.v4i1.3708>.

- Teo, Sue Anne. "Artificial Intelligence and Its 'Slow Violence' to Human Rights." *AI and Ethics* 5, no. 3 (June 2025): 2265–80. <https://doi.org/10.1007/s43681-024-00547-x>.
- Urbanisasi and Agusman. "Perlindungan Hukum terhadap Karya Kecerdasan Buatan (AI): Tantangan dan Peluang bagi Sistem HAKI Indonesia: Penelitian." *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan* 4, no. 2 (November 2025): 11575–80. <https://doi.org/10.31004/jerkin.v4i2.3709>.
- Whyte, Christopher. "Deepfake News: AI-Enabled Disinformation as a Multi-Level Public Policy Challenge." *Journal of Cyber Policy* 5, no. 2 (May 2020): 199–217. <https://doi.org/10.1080/23738871.2020.1797135>.
- Yadav, Deepti. "Human Rights Protection." *International Journal For Multidisciplinary Research* 7, no. 4 (July 2025): 1–20. <https://doi.org/10.36948/ijfmr.2025.v07i04.51897>.
- Yi Peng and Yong Tang. "Artificial Intelligence in International Immigration Management: A Comparative Legal Analysis of the United States, Canada, and the European Union." *Critical Humanistic Social Theory* 2, no. 2 (May 2025): 1–7. <https://doi.org/10.62177/chst.v2i2.413>.
- Yigitcanlar, Tan, Anne David, Wenda Li, Clinton Fookes, Simon Elias Bibri, and Xinyue Ye. "Unlocking Artificial Intelligence Adoption in Local Governments: Best Practice Lessons from Real-World Implementations." *Smart Cities* 7, no. 4 (June 2024): 1576–625. <https://doi.org/10.3390/smartcities7040064>.
- Zafriana, Lusi. "Integrasi Kecerdasan Buatan Dalam Penegakan Hukum: Peluang Inovasi dan Tantangan Keadilan Prosedural di Indonesia." *Jurnal Penelitian Ilmu Sosial Dan Eksakta* 5, no. 1 (September 2025): 24–36. <https://doi.org/10.47134/trilogi.v5i1.1688>.
- Zou, Mimi, and Lu Zhang. "Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models." *Cambridge Forum on AI: Law and Governance* 1 (2025): 1–16. <https://doi.org/10.1017/cfl.2024.4>.
- Zuiderveen Borgesius, Frederik J. "Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence." *The International Journal of Human Rights* 24, no. 10 (November 2020): 1572–93. <https://doi.org/10.1080/13642987.2020.1743976>.