

Cyber Sovereignty and Artificial Intelligence Regulation in Indonesia as A Strategy for Strengthening Legal Frameworks and Public Protection

Shafa Sakinah Abdi^{1*}, Pingki Pratiwi²

^{1,2} Faculty of Law, Universitas Islam Negeri Syarif Hidayatullah, Jakarta, Indonesia.

 : shafasknh@gmail.com

Corresponding Author*



Abstract

Introduction: The rapid development of artificial intelligence (AI) in Indonesia has brought significant transformations in the economic, communication, and public service sectors, while also giving rise to the potential for cybercrimes, such as digital fraud, identity manipulation, and the spread of false content. This phenomenon underscores the urgency of establishing a comprehensive legal framework to close regulatory loopholes that have the potential to threaten legal certainty, accountability, and human rights protection.

Purposes of the Research: This study aims to analyze the urgency and regulatory strategy of AI in Indonesia through an integrated approach that includes regulatory structure, legal substance, and legal system based on the principle of cyber sovereignty.

Methods of the Research: The research uses a normative juridical method by examining primary legal materials, such as national laws and regulations and relevant international legal instruments, as well as secondary legal materials in the form of literature, journals, and opinions of legal experts.

Findings of the Research: Through an integrated approach that includes regulatory structures, legal substances, and legal systems based on the principle of cyber sovereignty, it is found that Indonesia needs adaptive, comprehensive, and sustainable AI regulations to ensure human rights protection, digital security, and responsible use of technology.

Keywords: Artificial Intelligence; Cyber Sovereignty; Legal Regulation.

Submitted: 2026-01-08

Revised: 2026-02-27

Accepted: 2026-02-28

Published: 2026-03-07

How To Cite: Shafa Sakinah Abdi, Pingki Pratiwi. "Cyber Sovereignty and Artificial Intelligence Regulation in Indonesia as A Strategy for Strengthening Legal Frameworks and Public Protection." *TATOHI: Jurnal Ilmu Hukum* 5 no. 12 (2026): 584-596. <https://doi.org/10.47268/tatohi.v5i12.3701>

Copyright ©2026 Author(s)



Creative Commons Attribution-NonCommercial 4.0 International License

INTRODUCTION

The development of artificial intelligence (AI) technology has driven significant transformations in various aspects of human life, including in the legal system.¹ The use of AI brings efficiency, speed, and innovation in data processing and decision-making, so that it is increasingly used in government activities, the business world, and public services.² However, behind these benefits, AI also carries legal consequences that are not simple, especially when this technology is used without clear and responsible regulation, thus demanding an adaptive legal response to the dynamics of technology.

Along with the increasing use of AI, various forms of cybercrime have also emerged that take advantage of the sophistication of this technology.³ AI-based crimes, such as algorithm-

¹ Rohaini et al., "Pemanfaatan Kecerdasan Buatan Di Era Digital: Analisis Dampak, Tantangan, Dan Implikasi Terhadap Regulasi Hukum Di Indonesia," *Jurnal Kajian Hukum Dan Kebijakan Publik* 3, no. 1 (2025): 368-73, <https://doi.org/10.62379/cy6jsr95>.

² Ferti Latowa and I Gede Edi Sunadi, "Pemanfaatan Artificial Intelligence (AI) Sebagai Inovasi Digital Dalam Tata Kelola Pemerintah Daerah," *Journal of Multi Technology* 1, no. 1 (2025): 44-53, <https://doi.org/10.69623/j-multitechno.v1i1.137>.

³ Cindy Tania and Janwan Gidalty, "Strategi Penuntutan Kejahatan Siber Dengan Artificial Intelligence Di Era Digital," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 3, no. 4 (2025): 1387-1401, <https://doi.org/10.51903/j928ts68>.

based digital fraud, the spread of false information, and identity manipulation through deepfake technology, show increasingly complex and hard-to-trace characters.⁴ The adaptive and cross-border nature of crime has caused conventional legal approaches to be less effective, so legal instruments are needed that are able to respond to the new challenges posed by the development of AI. The escalation of digital crime in the Indonesian context is an indication that the use of AI by irresponsible parties has developed significantly. The impact of these crimes is not only in the form of economic losses, but also has implications for human rights violations, especially the right to personal data protection, privacy, and security in cyberspace.⁵ This condition shows that there is a gap between the rapid development of technology and the readiness of the national legal system in providing effective legal protection to the community.

Until now, Indonesia's national legal system does not have a specific regulation that comprehensively regulates artificial intelligence. Existing legal provisions are still general and sectoral, so they have not been able to reach the complexity of legal issues that arise due to the use of AI.⁶ The legal vacuum has an impact on limited legal certainty, weak law enforcement, and increased potential for technology abuse without a clear accountability mechanism. This condition is also reflected in law enforcement and legal governance practices in the professional environment, especially in the context of legal compliance and legal project management, where various problems involving the use of AI often face obstacles in determining the legal basis and subject of accountability.⁷ Both in the corporate environment and at the law enforcement stage, the absence of regulations that specifically regulate artificial intelligence causes the dispute resolution and law enforcement process to not run optimally. This shows that Indonesia's national legal system has not been fully designed to anticipate the rapid and dynamic development of AI technology.⁸

The existence of AI regulations in national law still leaves various conceptual and normative issues that need to be examined more deeply. The uncertainty of the legal framework in responding to the development of AI, both from institutional aspects, normative arrangements, and supervisory systems, shows the need for a systematic and structured legal study. Therefore, an approach that places AI regulation within the framework of a cyber sovereignty-based structure, substance, and legal system becomes relevant for analysis. Therefore, the author is interested in further research on "Cyber Sovereignty and Artificial Intelligence Regulation in Indonesia as a Strategy for Law Strengthening and Community Protection", in order to examine the urgency of establishing AI regulations and formulate strategies to strengthen them in the national legal system.

METHODS OF THE RESEARCH

This study uses a normative juridical approach with the aim of analyzing the urgency of the formation of artificial intelligence (AI) regulations and formulating strategies to

⁴ Adnasohn Aqilla Respati et al., "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban," *Media Hukum Indonesia (MHI)* 2, no. 2 (2024): 586–92, <https://doi.org/10.5281/zenodo.12508126>.

⁵ Kristofer Oscar and Zainal Arifin Hoesein, "Mendorong Regulasi Adaptif Dan Progresif Untuk Menghadapi Penyalahgunaan Artificial Intelligence Di Indonesia," *Journal of Innovative and Creativity* 5, no. 3 (2025): 31501–31511, <https://doi.org/10.31004/joecy.v5i3.4647>.

⁶ Oscar and Hoesein.

⁷ Muhammad Dafi Akbar et al., "Pemanfaatan Dan Permasalahan Artificial Intelligence Dalam Kehidupan Manusia Serta Pengaturannya Secara Hukum," *Media Hukum Indonesia (MHI)* 2, no. 2 (2024): 538–42, <https://doi.org/10.5281/zenodo.12169651>.

⁸ Wahyudi BR, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI," *INNOVATIVE: Journal Of Social Science Research* 5, no. 1 (2025): 3436–50, <https://doi.org/10.31004/innovative.v5i1.17519>.

strengthen regulations in Indonesian national law. The research is theoretical, so it does not use field data, but examines primary legal materials, such as national laws, government regulations, and international legal instruments, as well as secondary legal materials in the form of literature, journals, and legal expert opinions. The analysis is carried out in a normative qualitative manner by interpreting legal norms and the principles of cyber sovereignty, and linking them to AI-based crime problems and regulatory strengthening frameworks through structure, substance, and legal systems. The results of the research are presented in an analytical descriptive manner to answer the formulation of the problem, affirm the urgency of regulation, and formulate adaptive and sustainable legal policy recommendations.

RESULTS AND DISCUSSION

A. Legal Reflection on the Urgency of Establishing *Artificial Intelligence Regulations* in Indonesia

The development of artificial intelligence technology (AI) has taken place rapidly and penetrated various strategic sectors, such as the digital economy, communication systems, financial services, and electronic-based public services.⁹ AI is leveraged for large-scale data analysis, decision-making automation, and improved efficiency of digital services, which significantly drives economic growth and technological innovation. Globally, the OECD report shows that AI adoption is a major factor in the transformation of the digital economy, while in Indonesia the use of AI is expanding as the national digital transformation accelerates.¹⁰ However, behind these benefits, the use of AI also presents significant legal risks if it is not accompanied by adequate regulation. AI technology that is autonomous, adaptive, and algorithm-based opens up space for abuse, both in the form of data manipulation, information engineering, and decision-making that has a direct impact on individual rights.¹¹ The characteristics of AI that are able to mimic human behavior and process data massively make this technology vulnerable to abuse, so it has the potential to cause legal, social, and economic losses.¹² This condition shows that technological developments do not always go hand in hand with the readiness of the legal norms that govern them.

The development of AI in the context of national law in Indonesia poses its own challenges for the legal system which is still basically still oriented to conventional regulatory patterns. Until now, AI regulations are still scattered in several general regulations, such as Law Number 11 of 2008 *Jo.* Law Number 19 of 2016 *Jo.* Law Number 1 of 2024 concerning Information and Electronic Transactions (Law on Information and Electronic Transactions) and Law Number 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law), which have not specifically regulated the characteristics, risks, and legal responsibilities related to AI.¹³ The absence of this special regulation shows that there is an urgent need for the formation of legal policies that are able to

⁹ Imam Zaenudin and Ade Bani Riyan, "Perkembangan Kecerdasan Buatan (AI) Dan Dampaknya Pada Dunia Teknologi," *JITU: Jurnal Informatika Utama* 2, no. 2 (2024): 128–53, <https://doi.org/10.55903/jitu.v2i2.240>.

¹⁰ Azaria Eda Pradana et al., "Tantangan Kecerdasan Buatan Dalam Implikasi Kebijakan Pemerintah Di Indonesia: Studi Literatur," *Jurnal Good Governance* 21, no. 1 (2025): 51–66, <https://doi.org/10.32834/gg.v21i1.889>.

¹¹ BR, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI."

¹² Eka Nanda Ravizki and Lintang Yudhantaka, "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia," *Notaire* 5, no. 3 (2022): 351–76, <https://doi.org/10.20473/ntr.v5i3.39063>.

¹³ Akbar et al., "Pemanfaatan Dan Permasalahan Artificial Intelligence Dalam Kehidupan Manusia Serta Pengaturannya Secara Hukum."

comprehensively respond to the dynamics of AI technology, in order to ensure legal certainty, community protection, and the sustainability of the use of digital technology in Indonesia.

The development of artificial intelligence/AI in Indonesia has brought significant changes in various sectors, including the economy, communications, and public services. This technology increases efficiency, speed of data processing, and innovation of digital services, but at the same time opens up the potential for abuse with legal and social impacts.¹⁴ Forms of AI-based crime include digital fraud that utilizes automated algorithms, identity engineering through *deepfakes*, and the spread of fake content that harms finances, reputations, and lowers public trust in digital systems.¹⁵ This phenomenon confirms that AI is not only a tool for innovation, but also a potential legal risk that must be anticipated through an adequate regulatory framework. Juridically, this is related to the provisions of Law Number 19 of 2016 concerning Information and Electronic Transactions (Electronic Information and Transaction Law), especially Article 27 Paragraph 3 concerning the prohibition of the dissemination of misleading electronic information, and Article 28 Paragraph 1 concerning insult or defamation through electronic media. In addition, Law Number 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law), Article 5 and Article 15 also emphasize the right of data subjects to consent and security of personal data processing, including those generated or used by AI systems.

Empirical data from the Indonesian National Police reinforces the urgency of AI regulation. In the period from 2022 to early 2025, there was a significant increase in cybercrime cases, with the Metro Jaya Police reporting more than 32,000 cases that caused financial and reputational losses to thousands of victims. When compared to the 2019–2021 period, the increase reached around 45%, indicating a noticeable escalation trend.¹⁶ In addition, the 2023 State Cyber and Cryptography Agency report noted that more than 60% of cyber incidents related to the misuse of automated systems, including AI, occurred in the banking and public services sectors.¹⁷ These findings show that AI threats are not just hypothetical risks, but realities that require serious attention from policymakers and law enforcement officials. AI-based crime poses complex legal certainty challenges. AI systems that operate autonomously in data transactions or manipulation raise fundamental questions about the responsible party, whether the developer, the user, or the operator of the system. This condition increases the risk of legal impunity, where victims find it difficult to demand accountability, and law enforcement officials face normative obstacles because there is no juridical definition of AI in national regulations that apply in Article 1 of the Personal Data Protection Law and Article 1 of the Electronic Information and Transaction Law. It is this legal vacuum that confirms the need for special regulations that place legal certainty and accountability as the main foundation.

The social impact of AI abuse is also real and widespread. Digital identity engineering through *deepfakes* or the spread of false information can damage the reputation of

¹⁴ Oscar and Hoesein, "Mendorong Regulasi Adaptif Dan Progresif Untuk Menghadapi Penyalahgunaan Artificial Intelligence Di Indonesia."

¹⁵ Muhammad Syafiq Wafi, Aloysius Wisnubroto, and Yudi Prayudi, "Kejahatan Deepfake Berbasis Artificial Intelligence: Suatu Konsepsi Pada Penggunaan Asas Culpabilitas Sebagai Pembaharuan Pertanggungjawaban Pidana," *Reformasi Hukum* 29, no. 2 (2025): 168–183, <https://doi.org/10.46257/jrh.v29i2.1304>.

¹⁶ Kepolisian Republik Indonesia, "Statistik Kejahatan Siber Nasional Dan Polda Metro Jaya (2022-Awal 2025): Peningkatan Signifikan >32.000 Kasus.," pusiknas.polri.go.id, 2022, <https://pusiknas.polri.go.id>.

¹⁷ Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2023 & Laporan Monitoring Honeynet: >60% Insiden Siber Terkait Sistem Otomatis/AI Di Sektor Perbankan & Layanan Publik," [bssn.go.id](https://www.bssn.go.id), 2023, <https://www.bssn.go.id/laporan-tahunan>.

individuals and institutions. As happened in 2023, where digital identity fraud cases in Jakarta dominated cybercrime statistics according to the Central Statistics Agency of DKI Jakarta Province, with the Metro Jaya Police recording 1,951 reports of online fraud, most of which involved identity theft and caused financial losses of billions of rupiah and significant psychological impact on victims.¹⁸ In the public service sector, the misuse of algorithms can disrupt public access to government services, thereby lowering public trust in state institutions. These facts confirm that the threat of AI not only has a financial impact, but also touches on people's fundamental rights, such as privacy and data security as mandated in Article 4 of the Personal Data Protection Law.¹⁹ Thus, the trend of increasing cases and the impact they cause shows that AI regulation is no longer an option, but an urgent need. The absence of specific regulations has the potential to create a *legal vacuum*, weaken legal certainty, and increase the risk of misuse of digital technology. Therefore, the establishment of comprehensive, adaptive, and principle-based AI regulations on cyber sovereignty is a real legal urgency to ensure user accountability, community protection, and legitimacy of the use of digital technology in Indonesia.

The substance of AI regulation is at the heart of the formation of AI legal policy, as it sets normative boundaries on what is meant by AI and how the technology can be used legally. Until now, Indonesian national law does not have a juridical definition of artificial intelligence, thus creating ambiguity in qualifying a system as AI or just ordinary software.²⁰ The absence of this definition has implications for the difficulty of determining the scope of regulation, compliance standards, and legal consequences of the use of AI technology. Therefore, AI regulations need to explicitly establish juridical definitions and classifications of the use of AI, both based on the level of risk, function, and impact on the public interest.

Formulating the substance of AI regulation, harmonization with international legal standards and instruments is an inseparable step. Various international organizations have formulated AI normative frameworks, such as the OECD Principles on Artificial Intelligence, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and the European Union Artificial Intelligence Act which is based on a risk-based approach²¹. This harmonization is important so that national regulations are not isolated, while ensuring that Indonesia remains competitive and credible in global technology governance. However, harmonization must be carried out selectively by adjusting the characteristics of national law and the strategic interests of the state.

The substance of AI regulation must also integrate ethical and human rights principles as the main normative foundation. The use of AI has the potential to affect the rights to privacy, personal data protection, equality, and non-discrimination, especially when algorithms are used in decision-making that directly impact individuals.²² These principles are in line with Indonesia's constitutional values and are strengthened by the provisions in Law Number 27 of 2022 concerning Personal Data Protection, which affirms the importance

¹⁸ Badan Pusat Statistik Provinsi DKI Jakarta, "Statistik Kriminalitas Provinsi DKI Jakarta 2023," bps.go.id, 2024, <https://jakarta.bps.go.id>.

¹⁹ Muhammad Aiman et al., "Perlindungan Hukum Terhadap Data Pribadi Di Era AI Generatif: Cukupkah UU PDP Mengantisipasi Risiko," *Edu Research* 6, no. 3 (2025): 2988-98, <https://doi.org/10.47827/jer.v6i3.1551>.

²⁰ Martinus Irwanto Ishak, "Kecerdasan Buatan Dan Tantangan Regulasi: Keterbatasan UU ITE Dalam Menjawab Teknologi Canggih," *Djtechno: Jurnal Teknologi Informasi* 6, no. 3 (2025): 1168-75, <https://doi.org/10.46576/djtechno.v6i3.7772>.

²¹ Trisnawati, "Artificial Intelligence Governance and Regulation: A Roadmap to Developing Legal Policies for Artificial Intelligence Deployment," *JGAR: Journal of Governance and Administrative Reform* 5, no. 2 (2024): 185-94, <https://doi.org/10.20473/jgar.v5i2.65194>.

²² Welnof Satria and Sabrina Aulia Rahmah, "Analisis Konseptual Dampak Kecerdasan Buatan Terhadap Privasi Data Pribadi Digital," *Jurnal Multidisiplin Sosial Dan Humaniora* 2, no. 2 (2025): 91-99, <https://doi.org/10.70585/jmsh.v2i2.170>.

of data protection and accountability in information processing. The integration of ethics and human rights is an instrument to prevent AI from being used arbitrarily and harming vulnerable groups. Further, algorithmic transparency and fairness in AI-based decision-making need to be part of the regulatory substance. The shutdown of AI systems risks creating algorithmic biases that are difficult to detect and account.²³ Therefore, regulations need to encourage the principles of *explainability* and *accountability*, especially for AI systems used in strategic sectors such as finance, law enforcement, and public services. This approach aims to ensure that AI-generated decisions can be legally and ethically tested. In closing, regulatory AI should establish effective sanctions and remediation mechanisms against violations of the law or misuse of technology. This mechanism includes administrative, civil, and criminal sanctions, along with recovery procedures for victims who are aggrieved. The existence of clear sanctions shows that AI regulation does not stop at the normative level, but has coercive power to enforce legal certainty and accountability. Thus, the substance of AI regulation functions as a legal instrument that not only directs the use of technology, but also provides concrete legal protection for society.

The phenomenon of artificial intelligence abuse in Indonesia shows the need for more specific legal attention, given the financial losses, privacy violations, and potential algorithmic discrimination that arise due to the vacuum of norms in the national legal system. Existing general provisions, such as the Electronic Information and Transactions Act and the Personal Data Protection Act, do not provide clear juridical definitions or accountability mechanisms for AI developers, users, and systems. This condition poses real legal and social risks, including weakening accountability, declining public trust in digital technology, and increasing potential for AI abuse without effective sanctions. Therefore, the establishment of comprehensive, ethical, and adaptive regulations is very important to fill the legal gap and provide a foundation of legal certainty for the use of technology in Indonesia. This need also opens the way for discussions on strategies to strengthen AI regulations through an integrated approach to the structure, substance, and legal system based on the principles of cyber sovereignty. Regulations that focus only on norms without the support of implementation and supervision mechanisms will find it difficult to enforce accountability and protection of the community, by emphasizing coordination of regulatory agencies, harmonization with international standards, determination of legal responsibilities of relevant parties, and the implementation of audits and monitoring based on national digital infrastructure, AI regulations can be designed more effectively. This framework prepares the foundation for a legal strategy that is able to adapt to the complexity of the use of AI, while maintaining legal certainty and community protection in the era of digital transformation.

B. Strategic Framework for Artificial Intelligence Regulation in Indonesian National Law Based on Structure, Substance, and Cyber Sovereignty

The absence of specific regulations on *artificial intelligence* (AI) in Indonesia's national legal system, as described in the previous discussion, shows a serious gap between technological developments and existing legal regulatory capacity.²⁴ Positive legal instruments that are currently in force, such as Law Number 11 of 2008 concerning

²³ Muh. Akbar Fhad Syahril et al., "Artificial Intelligence Dan Hak Asasi Manusia: Kajian Hukum Tentang Potensi Bahaya Di Indonesia" 11, no. 3 (2024): 359-64, <http://journalstih.amsir.ac.id/index.php/julia/article/view/443>.

²⁴ Friska Monalisa Pangaribuan and Made Cinthya Puspita Shara, "Keterbatasan Pengaturan Artificial Intelligence (AI) Di Indonesia: Dampak Hukum Dan Peran Pemerintah," *Kertha Desa: Journal Ilmu Hukum* 13, no. 8 (2025): 606-18, <https://ojs.unud.ac.id/index.php/kerthadesa/article/view/124973>.

Information and Electronic Transactions and its amendments to Law Number 27 of 2022 concerning Personal Data Protection, are still essentially sectoral and have not been designed to anticipate the characteristics of artificial intelligence that is autonomous, adaptive, and algorithm-based. This condition causes limitations in providing legal certainty, especially in the context of legal accountability, supervision of the use of technology, and the protection of basic rights of citizens in cyberspace, in the perspective of the state of law as affirmed in Article 1 Paragraph 3 of the Constitution of the Republic of Indonesia in 1945, the law has a fundamental function as an instrument of controlling power as well as protecting the interests of the community.²⁵ Therefore, the development of artificial intelligence technology that has the potential to affect the rights to privacy, data security, and social justice cannot be allowed to run without a clear and systematic regulatory framework.²⁶ The strengthening of AI regulations is not only intended to respond to potential violations of the law, but also to ensure that the use of such technology is in line with constitutional values, human rights principles, and Indonesia's national interests in the digital era.

The urgency of strengthening artificial intelligence regulations is also closely related to the need to build accountable and sovereign technology governance. Globally, countries have begun to develop AI legal frameworks that emphasize *precautionary principles*, algorithm transparency, and legal accountability, as reflected in various international instruments.²⁷ Indonesia, as a country with a high level of digital technology adoption, needs to formulate a regulatory strategy that is not only adaptive to global developments, but also contextual with the national legal system and the social realities of its people. Without a structured strategy, AI regulation has the potential to be reactive, partial, and ineffective in its implementation.

Strengthening artificial intelligence regulations in Indonesian national law requires a clear and integrated institutional structure. Until now, the regulation and supervision of digital technology is still spread across various ministries and institutions, such as the Ministry of Communication and Digital, the Ministry of Industry, the Ministry of Higher Education, and the State Cyber and Cryptography Agency. This fragmentation of authority has the potential to cause policy overlap and weak oversight of the use of AI. Therefore, it is necessary to establish or appoint an AI regulatory body that has a coordinating and regulatory mandate, and is functionally connected with technical ministries and law enforcement officials. The establishment of such an institution is in line with the principles of *good governance* and international practice, where AI oversight is placed within a specific and focused institutional framework.

The existence of AI regulatory agencies is not intended to replace the authority of existing institutions, but functions as a central *coordinating body* in policy formulation, standardization, and supervision of the implementation of AI technology, in the context of law enforcement, this institution needs to have a clear coordination mechanism with law enforcement officials, including the Police and Prosecutor's Office, to deal with violations involving digital technology. This coordination ensures that the development and utilization of AI runs in accordance with the principles of accountability, transparency, and

²⁵ Watik Refka Annisa, "Fungsi Hukum Sebagai Instrumen Yang Menjamin Perlindungan Dan Pemenuhan HAM Di Indonesia," *Global Review of Law and Human Rights* 1, no. 1 (2025): 36–48, <https://idereach.com/Journal/index.php/grlhr/article/view/119>.

²⁶ Yudha Sri Wulandari, "Kecerdasan Buatan Dan Perlindungan Data: Analisis Regulasi Yang Adil Untuk Sistem Hukum Indonesia," *Jurnal Ilmu Hukum "THE JURIS"* 9, no. 1 (2025): 24–31, <https://doi.org/10.56301/juris.v9i1.1518>.

²⁷ Wulandari.

legal compliance, while preventing overlapping authority between agencies. In addition to the institutional aspect, the regulatory structure of AI also demands a proportionate division of roles and responsibilities between the government, industry players, and society. The government plays the role of regulator and supervisor, industry as the main actor in the development and application of technology, and the community as a protected subject as well as a user of technology. This division of roles is important to prevent the dominance of purely economic interests in AI development without considering ethical aspects and human rights protection. The principle of *shared responsibility* becomes relevant, where industry players are not only subject to regulations, but also have self-regulation obligations through the application of ethical standards and legal compliance.

The effectiveness of the regulatory structure also depends on a planned and sustainable inter-agency coordination mechanism. This coordination is needed to accelerate the process of policy formulation, data exchange, and cross-sector case handling involving AI. This approach is in line with the practice of harmonizing national regulations to create strong legal certainty and prevent sectoral and partial policies. The implementation of AI regulations will be effective if it is accompanied by a planned and comprehensive socialization strategy to the public and industry players. This socialization includes legal education activities, the involvement of industry associations, and the use of digital platforms as a medium of policy communication, with an equal understanding, all relevant parties can adjust the practice and governance of AI technology in accordance with applicable legal provisions. This approach not only encourages *voluntary compliance*, but also strengthens the public's legal awareness of their rights and obligations, so that the implementation of regulations can run effectively, sustainably, and in line with the principles of accountability and public protection.

The need for a clear juridical definition in AI regulation is also very necessary so that the use of technology can be properly classified within the national legal framework. This definition not only includes the notion of AI as a system or software capable of automated data analysis and decision-making, but also includes the adaptive and algorithmic characteristics inherent in such technology. The determination of juridical definitions is the basis for the application of the law, so that existing norms, such as Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection, can be applied consistently to all forms of AI implementation. In addition, the substance of the regulation needs to regulate the legal responsibilities of the parties involved, both developers, providers, and users of AI systems. These arrangements include the obligation to maintain the security, integrity, and accountability of the algorithm, as well as establish accountability mechanisms when the AI system causes losses or violations of the law. This principle is also in line with the legal responsibility of electronic system operators as stipulated in Articles 7 and 8 of the Electronic Information and Transactions Law, while expanding the scope of regulations to adjust the autonomous and adaptive character of AI technology.

The harmonization of national regulations with international standards is a strategic step to ensure policy consistency and interoperability. As such, the principles set out in the OECD AI Principles (2019), the EU AI Act (2021 draft), and the UNESCO Recommendation on the Ethics of *Artificial Intelligence* (2021) which emphasize transparency, security, inclusivity, and accountability. By adopting these principles, Indonesia can adjust its legal framework to align with global practices while maintaining national cyber sovereignty,

thereby preventing norm conflicts and increasing public trust in the use of AI.²⁸ The substance of the regulation is also obliged to integrate ethical and human rights principles, including privacy protection, data security, anti-discrimination, and algorithm transparency. This provision serves as a moral and legal control against potential misuse of AI technology, such as algorithmic bias, automatic discrimination, and privacy violations. The integration of ethical principles in the context of national law can be strengthened through internal guidelines of regulatory agencies, algorithm audits, as well as public consultation mechanisms to assess social and human rights impacts before the implementation of AI systems.

As part of the substance framework, AI regulations should contain sanctions and remediation mechanisms for any violations or misuse of technology. This mechanism can be in the form of administrative, criminal, or civil sanctions accompanied by recovery procedures for the aggrieved party. These regulations ensure that regulations have real *enforceability*, so that legal certainty and accountability can be effectively enforced. Therefore, the substance of AI regulation is not only an operational guideline for developers and users, but also provides concrete legal protection for society and the state in utilizing AI.²⁹ The supervision and regulation of artificial intelligence in Indonesia must be based on the principle of cyber sovereignty, which emphasizes full control over data, algorithms, and digital applications operating on the country's territory.³⁰

This principle emphasizes that the management of technological infrastructure, including AI systems, must be subject to national laws and national interest priorities, as stipulated in Article 3 of Law Number 11 of 2008 *Jo.* Law 19 of 2016 concerning Information and Electronic Transactions. The cyber sovereignty approach allows the government to ensure that the use of AI does not cause dependence on foreign parties, while maintaining data security and algorithm integrity that has an impact on the public interest and national defense, to ensure compliance with these principles, a mechanism for auditing, certification, and continuous monitoring of AI systems developed and used in Indonesia is needed. Technical certifications can be carried out against AI algorithms and software, while regular audits ensure that the system works in accordance with applicable legal and ethical standards. This mechanism is in line with the international practices recommended in the OECD AI Principles, which emphasize continuous evaluation and accountability in the implementation of autonomous technologies, as well as serving as an instrument for mitigating complex and adaptive technological risks. In addition, a regulatory system based on cyber sovereignty should include a rapid response strategy to law violations and AI abuse. This strategy includes early detection protocols, cross-agency coordination, and efficient investigation and enforcement mechanisms. A quick response not only prevents economic and reputational losses, but also maintains public trust in national digital technology.³¹ This approach is in line with the principles of *accountability* and *resilience* that

²⁸ Cecep Mustafa and Rita Komalasari, "Enhancing Indonesia-EU Relations: Balancing AI Regulation, National Security, and Economic Growth In a Digital Age (Meningkatkan Hubungan Indonesia-Eropa: Menyeimbangkan Regulasi AI, Keamanan Nasional, Dan Pertumbuhan Ekonomi Di Era Digital)," *Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 16, no. 1 (2025): 57-74, <https://vs-jurnal.dpr.go.id/index.php/politika/article/view/4725>.

²⁹ Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177-99, <https://doi.org/10.25072/jwy.v5i2.460>.

³⁰ Tubagus Akbar Satria Primadana, Fokky Fuad, and Sadino Sadino, "Tantangan Regulasi Dan Implementasi Artificial Intelligence (AI) Dalam Pengembangan Alutsista Indonesia: Perspektif Kebijakan Pertahanan," *JIHHP: Jurnal Politik Hukum, Humaniora Dan Politik* 5, no. 6 (2025): 5596-5608, <https://doi.org/10.38035/jihhp.v5i6.5267>.

³¹ Kementerian Komunikasi dan Informatika Republik Indonesia, "Strategi Nasional Kecerdasan Artifisial Republik Indonesia 2020 - 2045" (Jakarta, 2020), p. 45-52.

are the benchmarks for the effectiveness of modern cyber regulations, including those applied in the European Union and Singapore in AI management. This approach suggests that strengthening a regulatory system based on cyber sovereignty does not only rely on technical instruments of supervision, but also requires the support of a robust and accountability-oriented legal framework.³² The UK experience can be used as a comparative reference, where the regulation of artificial intelligence is developed through a *jurisprudence* and sectoral governance approach that allows AI surveillance to run adaptive without ignoring legal certainty. Various industry sectors in the UK that use AI are required to comply with data protection standards, cybersecurity, and algorithmic surveillance mechanisms as part of efforts to maintain the sovereignty and security of the national digital system. The strong legal and academic foundations in AI governance in the UK are reflected in the growing global reference literature, such as *The Oxford Handbook of AI Governance* published by Oxford University Press, which asserts that the effectiveness of AI regulation is highly dependent on the integration between legal systems, ethical principles, and institutional mechanisms.³³ This model confirms that effective AI regulation can be built progressively through an adaptive, precedent-based, and technology-oriented legal system in a sustainable manner.

Therefore, in order for regulations to be carried out optimally, the integration of the legal system with national digital infrastructure is a crucial step. This infrastructure includes a centralized database, a secure communication system, and a cyber-incident monitoring and reporting platform that is inter-agency. This kind of integration allows for effective coordination between regulatory agencies, law enforcement, and other stakeholders, while strengthening the legal certainty and effectiveness of AI surveillance. A regulatory system based on cyber sovereignty not only maintains technological security, but also ensures that the use of AI is aligned with national interests, law, and public protection. Overall, the implementation of an integrated AI regulatory strategy through institutional structures, legal substances, and cyber sovereignty-based systems has real implications for legal certainty, user accountability, and community protection, with inter-agency coordination, clear juridical definitions, supervisory mechanisms, and continuous certification and auditing, legal norms can be enforced systemically and the risk of technology misuse can be minimized. This is because this approach not only ensures national legal compliance, but also builds public trust in digital technology and national regulations so that the use of AI can run effectively, safely, and sustainably.

CONCLUSION

The development of artificial intelligence (AI) in Indonesia in principle provides significant benefits in supporting digital transformation. However, its use also poses various legal challenges, especially the increase in cybercrime such as algorithm-based digital fraud, identity engineering through *deepfake technology*, and the spread of fake content that has the potential to cause financial losses, damage reputations, and reduce public trust in digital systems. The absence of a juridical definition of AI and a clear accountability mechanism has caused the implementation of the provisions of Law Number 19 of 2016 concerning Electronic Information and Transactions and Law Number 27 of 2022

³² Theodore M Lechterman, *The Concept of Accountability in AI Ethics and Governance*, in *The Oxford Handbook of AI Governance* (New York: Oxford University Press, 2024), p. 164–182.

³³ Justin B Bullock et al., *The Oxford Handbook of AI Governance* (New York: Oxford University Press, 2024).

concerning Personal Data Protection to be optimal, making it difficult to realize legal certainty and accountability. In addition, the use of AI without ethical oversight has the potential to violate human rights, especially related to the protection of personal data and the potential for algorithmic discrimination. The strategy to strengthen artificial intelligence regulations in Indonesia is carried out through an integrated approach to the structure, substance, and legal system based on cyber sovereignty. In terms of structure, the strategy includes the establishment of regulatory agencies that coordinate with ministries and law enforcement officials, the division of roles of government, industry, and society, and regulatory socialization mechanisms to ensure compliance and effective implementation. In terms of substance, the strategy includes the establishment of a juridical definition of AI, the regulation of legal responsibilities of developers, users, and AI systems, harmonization with international standards, the integration of ethical and human rights principles, and sanctions and remediation mechanisms for violations. Meanwhile, in terms of the legal system, this strategy emphasizes the application of the principles of cyber sovereignty through surveillance of data, algorithms, and AI applications, continuous audits and certifications, integration of regulations with national digital infrastructure, and rapid response mechanisms to misuse of technology, with the combination of these measures, AI regulations are expected to run comprehensively, adaptively, and accountably, while maintaining legal certainty, public protection, and legitimacy. The use of digital technology in Indonesia

REFERENCES

- Aiman, Muhammad, Desmarani Helfisar, Sopian, Al Ikhlas, and Zaenuddin B Palalas. "Perlindungan Hukum Terhadap Data Pribadi Di Era AI Generatif: Cukupkah UU PDP Mengantisipasi Risiko." *Edu Research* 6, no. 3 (2025): 2988–98. <https://doi.org/10.47827/jer.v6i3.1551>.
- Akbar, Muhammad Dafi, Josua Ferdinand Sihotang, Rendika Purnama, and Taria Hasna. "Pemanfaatan Dan Permasalahan Artificial Intelligence Dalam Kehidupan Manusia Serta Pengaturannya Secara Hukum." *Media Hukum Indonesia (MHI)* 2, no. 2 (2024): 538–42. <https://doi.org/10.5281/zenodo.12169651>.
- Annisa, Watik Refka. "Fungsi Hukum Sebagai Instrumen Yang Menjamin Perlindungan Dan Pemenuhan HAM Di Indonesia." *Global Review of Law and Human Rights* 1, no. 1 (2025): 36–48. <https://idereach.com/Journal/index.php/grlhr/article/view/119>.
- Badan Pusat Statistik Provinsi DKI Jakarta. "Statistik Kriminalitas Provinsi DKI Jakarta 2023." bps.go.id, 2024. <https://jakarta.bps.go.id>.
- Badan Siber dan Sandi Negara. "Lanskap Keamanan Siber Indonesia 2023 & Laporan Monitoring Honeynet: >60% Insiden Siber Terkait Sistem Otomatis/AI Di Sektor Perbankan & Layanan Publik." bssn.go.id, 2023. <https://www.bssn.go.id/laporan-tahunan>.
- BR, Wahyudi. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *INNOVATIVE: Journal Of Social Science Research* 5, no. 1 (2025): 3436–50. <https://doi.org/10.31004/innovative.v5i1.17519>.
- Bullock, Justin B, Yu-Che Chen, Johannes Himmelreich, Valerie M. Hudson, Anton Korinek, Matthew M. Young, and Baobao Zhang. *The Oxford Handbook of AI Governance*. New

York: Oxford University Press, 2024.

- Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99. <https://doi.org/10.25072/jwy.v5i2.460>.
- Ishak, Martinus Irwanto. "Kecerdasan Buatan Dan Tantangan Regulasi: Keterbatasan UU ITE Dalam Menjawab Teknologi Canggih." *Djtechno: Jurnal Teknologi Informasi* 6, no. 3 (2025): 1168–75. <https://doi.org/10.46576/djtechno.v6i3.7772>.
- Kementerian Komunikasi dan Informatika Republik Indonesia. "Strategi Nasional Kecerdasan Artifisial Republik Indonesia 2020 – 2045." Jakarta, 2020.
- Kepolisian Republik Indonesia. "Statistik Kejahatan Siber Nasional Dan Polda Metro Jaya (2022-Awal 2025): Peningkatan Signifikan >32.000 Kasus." pusiknas.polri.go.id, 2022. <https://pusiknas.polri.go.id>.
- Latowa, Ferti, and I Gede Edi Sunadi. "Pemanfaatan Artificial Intelligence (AI) Sebagai Inovasi Digital Dalam Tata Kelola Pemerintah Daerah." *Journal of Multi Technology* 1, no. 1 (2025): 44–53. <https://doi.org/10.69623/j-multitechno.v1i1.137>.
- Lechterman, Theodore M. *The Concept of Accountability in AI Ethics and Governance*, in *The Oxford Handbook of AI Governance*. New York: Oxford University Press, 2024.
- Mustafa, Cecep, and Rita Komalasari. "Enhancing Indonesia-EU Relations: Balancing AI Regulation, National Security, and Economic Growth In a Digital Age (Meningkatkan Hubungan Indonesia-Eropa: Menyeimbangkan Regulasi AI, Keamanan Nasional, Dan Pertumbuhan Ekonomi Di Era Digital)." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 16, no. 1 (2025): 57–74. <https://vs-jurnal.dpr.go.id/index.php/politica/article/view/4725>.
- Oscar, Kristofer, and Zainal Arifin Hoesein. "Mendorong Regulasi Adaptif Dan Progresif Untuk Menghadapi Penyalahgunaan Artificial Intelligence Di Indonesia." *Journal of Innovative and Creativity* 5, no. 3 (2025): 31501–31511. <https://doi.org/10.31004/joecy.v5i3.4647>.
- Pangaribuan, Friska Monalisa, and Made Cinthya Puspita Shara. "Keterbatasan Pengaturan Artificial Intelligence (AI) Di Indonesia: Dampak Hukum Dan Peran Pemerintah." *Kertha Desa: Journal Ilmu Hukum* 13, no. 8 (2025): 606–18. <https://ojs.unud.ac.id/index.php/kerthadesa/article/view/124973>.
- Pradana, Azaria Eda, Augustin Rina Herawati, Ida Hayu Dwimawanti, and Maesaroh. "Tantangan Kecerdasan Buatan Dalam Implikasi Kebijakan Pemerintah Di Indonesia: Studi Literatur." *Jurnal Good Governance* 21, no. 1 (2025): 51–66. <https://doi.org/10.32834/gg.v21i1.889>.
- Primadana, Tubagus Akbar Satria, Fokky Fuad, and Sadino Sadino. "Tantangan Regulasi Dan Implementasi Artificial Intelligence (AI) Dalam Pengembangan Alutsista Indonesia: Perspektif Kebijakan Pertahanan." *JIHHP: Jurnal Politik Hukum, Humaniora Dan Politik* 5, no. 6 (2025): 5596–5608. <https://doi.org/10.38035/jihhp.v5i6.5267>.
- Ravizki, Eka Nanda, and Lintang Yudhantaka. "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia." *Notaire* 5, no. 3 (2022): 351–76. <https://doi.org/10.20473/ntr.v5i3.39063>.

- Respati, Adnasohn Aqilla, Astri Dewi Setyarini, Dodi Parlagutan, Muhammad Rafli, Rayhan Syahbana Mahendra, and Andriyanto Adhi Nugroho. "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban." *Media Hukum Indonesia (MHI)* 2, no. 2 (2024): 586–92. <https://doi.org/10.5281/zenodo.12508126>.
- Rohaini, Yulianti, Nabila Gusriyanti, Aldo Felyo, Lilis Amelia, and Muh Raditya Caesare. "Pemanfaatan Kecerdasan Buatan Di Era Digital: Analisis Dampak, Tantangan, Dan Implikasi Terhadap Regulasi Hukum Di Indonesia." *Jurnal Kajian Hukum Dan Kebijakan Publik* 3, no. 1 (2025): 368–73. <https://doi.org/10.62379/cy6jsr95>.
- Satria, Welnof, and Sabrina Aulia Rahmah. "Analisis Konseptual Dampak Kecerdasan Buatan Terhadap Privasi Data Pribadi Digital." *Jurnal Multidisiplin Sosial Dan Humaniora* 2, no. 2 (2025): 91–99. <https://doi.org/10.70585/jmsh.v2i2.170>.
- Syahril, Muh. Akbar Fhad, A. Darmawansya TL, Murdiono, and Arini Asriyani. "Artificial Intelligence Dan Hak Asasi Manusia: Kajian Hukum Tentang Potensi Bahaya Di Indonesia" 11, no. 3 (2024): 359–64. <http://journalstih.amsir.ac.id/index.php/julia/article/view/443>.
- Tania, Cindy, and Janwan Gidaly. "Strategi Penuntutan Kejahatan Siber Dengan Artificial Intelligence Di Era Digital." *Hakim: Jurnal Ilmu Hukum Dan Sosial* 3, no. 4 (2025): 1387–1401. <https://doi.org/10.51903/j928ts68>.
- Trisnawati. "Artificial Intelligence Governance and Regulation: A Roadmap to Developing Legal Policies for Artificial Intelligence Deployment." *JGAR: Journal of Governance and Administrative Reform* 5, no. 2 (2024): 185–94. <https://doi.org/10.20473/jgar.v5i2.65194>.
- Wafi, Muhammad Syafiq, Aloysius Wisnubroto, and Yudi Prayudi. "Kejahatan Deepfake Berbasis Artificial Intelligence: Suatu Konsepsi Pada Penggunaan Asas Culpabilitas Sebagai Pembaharuan Pertanggungjawaban Pidana." *Reformasi Hukum* 29, no. 2 (2025): 168–183. <https://doi.org/10.46257/jrh.v29i2.1304>.
- Wulandari, Yudha Sri. "Kecerdasan Buatan Dan Perlindungan Data: Analisis Regulasi Yang Adil Untuk Sistem Hukum Indonesia." *Jurnal Ilmu Hukum "THE JURIS"* 9, no. 1 (2025): 24–31. <https://doi.org/10.56301/juris.v9i1.1518>.
- Zaenudin, Imam, and Ade Bani Riyan. "Perkembangan Kecerdasan Buatan (AI) Dan Dampaknya Pada Dunia Teknologi." *JITU: Jurnal Informatika Utama* 2, no. 2 (2024): 128–53. <https://doi.org/10.55903/jitu.v2i2.240>.

Conflict of Interest Statement: The author(s) declares that research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest,

Copyright: © AUTHOR. This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. (CC-BY NC), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

TATOHI: Jurnal Ilmu Hukum is an open access and peer-reviewed journal published by Faculty of Law, Universitas Pattimura, Ambon, Indonesia.

