Indonesian Cyber Law Review
POLITEKNIK SIBER CERDIKA INTERNASIONAL
E-ISSN xxxx-xxxx
P-ISSN xxxx-xxxx
The journal is published biyearly by Politeknik Siber Cerdika Internasional

Artificial Intelligence and Cybersecurity Regulation in Indonesia: Towards an Adaptive Legal Framework

Upit Elya Rohimi
Universitas Swadaya Gunung Jati, Indonesia
Corresponding email: uelyarohimi@gmail.com

Abstract: *Artificial intelligence (AI) technology development has become a significant catalyst for digital transformation in Indonesia. However, regulatory readiness has not matched the accelerated adoption of AI, especially in the legal and cybersecurity aspects. The national legal framework is still sectoral and has not been able to address the complexity of risks from AI systems implemented in various public and private sectors. This research aims to: (1) identify regulatory weaknesses in monitoring the use of AI in Indonesia; (2) formulate an integrative legal framework between AI regulation and cyber law that is adaptive to technological developments; and (3) provide policy recommendations based on international practices. This research method uses a normative empirical legal approach with documentation studies, comparative analysis of international regulations, and semi structured interviews with experts. The results show that Indonesia experiences significant regulatory gaps, particularly in applying the principles of transparency, accountability, and AI risk management. Compared to the European Union and the United States, AI regulations in Indonesia are still at the declarative stage without adequate enforcement mechanisms. This study recommends the establishment of a risk based national legal framework accompanied by strengthening independent oversight institutions, AI technical standards, and multi stakeholder involvement in the regulatory process. These findings are expected to serve as the basis for developing legal policies that are more adaptive, responsive, and secure to advances in AI technology and the dynamics of cyber threats in Indonesia.*
Keywords: *artificial intelligence regulation, cybersecurity, technology law, AI governance, risk based regulation*

1. Introduction

In the era of rapidly evolving digital transformation, integrating artificial intelligence (AI) has become an integral part of Indonesia's government systems, industries, and social life (Calo, 2018; Floridi et al., 2018; Pasquale, 2015). Although AI brings efficiency and innovation, its legal complexity is still hotly debated, especially regarding responsibility, ethics, and protection of human rights (Binns, 2018; Mittelstadt et al., 2016; Eubanks, 2018). In this context, the urgency of establishing a legal system that is responsive to AI is increasing, especially with the development of Indonesia's digital infrastructure, which is still vulnerable to cyberattacks (BSSN, 2023; Ministry of Communication and Information, 2022; ITU, 2023).

Indonesia has experienced a significant increase in cyber incidents over the past five years, while the number of regulations specifically addressing artificial

intelligence (AI) is still minimal (OECD, 2023; BSSN, 2023; Kominfo, 2022). In 2019, there were only two AI related policies, but this number increased to nine by 2023. On the other hand, the number of cyber incidents jumped from around 122,000 cases to nearly 290,000 in the same period. This gap indicates a stark disparity between the growth of technology utilization and the readiness of national legal frameworks, which could trigger a legal vacuum and increase the risk of misuse of AI technologies, especially in the context of digital security (Zuboff, 2019; Wachter et al, The urgency of this research is even more evident if we look at international policies such as the European Union's AI Act and the Blueprint for an AI Bill of Rights in the United States, which show progressive legal directions based on the principles of transparency, accountability, and fairness (European Commission, 2021; White House OSTP, 2022; UNESCO, 2021). However, the Indonesian legal system has not fully adopted this approach, which is still reactive rather than preventive (Gunawan, 2023; Ramli, 2022; Siregar, 2023).

Several previous studies have discussed the legal aspects of AI in Indonesia, such as by Fadillah (2022), who highlighted the need for ethics in public AI systems, and by Pranata & Dewi (2021), who reviewed the personal data protection framework in the use of AI. Meanwhile, in the technology field, LIPI and BRIN (2023) studies emphasized the importance of AI system security against cyber penetration. However, most of these studies have not synergized legal and technological approaches in the context of national digital security (Sibarani, 2023; Hidayat, 2022; Malik, 2023).

The research gap arises from the lack of interdisciplinary analysis that examines the relationship between AI legal regulation and cybersecurity contextually within the national legal landscape. Not many studies have critically evaluated Indonesia's legal response to the threats and disruptions posed by AI in cyberspace (Rahardjo, 2021; Setiadi, 2022; Nugroho, 2024). This hampers efforts to develop holistic and adaptive AI governance.

The novelty of this research lies in combining juridical normative and technological approaches to analyze the need for establishing a national legal framework based on risk (risk based regulation) regarding the use of AI in the context of Indonesian cybersecurity. This research also maps out regulatory models that can be adopted from global practices, adapted to national legal values (Santosa, 2023; Kusuma, 2024; Darmawan, 2023).

This research aims to: (1) identify regulatory weaknesses in monitoring the use of AI for Indonesia's digital security; (2) formulate an integrative legal framework between AI regulation and cyber law that is adaptive to technological developments; and (3) provide policy recommendations based on international comparisons and principles of responsible AI governance (Goodman & Flaxman, 2017; Cowls et al., 2021; Jobin et al., 2019).

With an interdisciplinary focus between law and technology, this article is expected to provide scholarly and practical contributions to the development of Indonesia's digital legal system that is more robust, inclusive, and resilient to the risks of AI based cybercrime (Shneiderman, 2022; Winfield & Jirotka, 2018; Narayanan et al., 2016).

2. Method

Type of Research

This is normative, empirical legal research with an interdisciplinary approach to law and information technology. The normative approach examines laws, regulations, legal doctrines, and AI governance principles. Meanwhile, the empirical approach is used to analyze quantitative and qualitative data on implementing AI in the national digital system and the frequency of cyberattacks on AI platforms (Soekanto, 2014; Marzuki, 2017; Creswell, 2014). This research also uses a comparative approach by reviewing AI regulations and cybersecurity policies from the European Union, the United States, and ASEAN countries (Tewary, 2020; Sartor, 2021; Lin et al., 2022).

Population and Sampling

The population in this study includes national and international legal documents on AI and cybersecurity, such as laws, government regulations, technical guidelines, and AI ethical frameworks. Document samples were selected by purposive sampling based on the relevance, legality, and novelty of the documents, for example: ITE Law, Personal Data Protection Bill, BSSN Regulation, and AI Act (EU) and AI Bill of Rights (USA) (Miles & Huberman, 1994; Bungin, 2020; Sugiyono, 2019).

Research Instrument

The research instruments were: (a) a juridical analysis checklist to assess the existence, appropriateness, and consistency of legal norms; (b) an interview guideline to obtain the views of legal and technology experts; and (c) a documentation analysis tool used to review data on cyber incidents and the application of AI in the national system (Neuman, 2014; Yin, 2018; Strauss & Corbin, 1998).

Data Collection Technique

Data was collected through three main techniques: (1) Documentation study, i.e. browsing regulations, scientific articles, policies, white papers, and annual reports of relevant institutions such as BSSN, Kominfo, and BRIN; (2) Semi structured interviews with cyber law experts, AI developers, and government officials ; (3) Secondary data analysis in the form of statistical reports on cyberattacks and AI growth from national and international institutions (OECD, ITU, BSSN) (Bowen, 2009; Flick, 2014; Stake, 1995).

Research Procedure

This research was conducted through five stages: (1) Identify legal and technological issues related to AI and cybersecurity, (2) Collection of legal sources and supporting data from 2019 to 2024, (3) Categorization of issues based on field findings and relevant regulations, (4) Juridical and technological analysis using a data triangulation model, (5) Policy recommendations are based on the principles of responsible AI governance and national digital sovereignty (Patton, 2002; Babbie, 2015; Strauss, 1990).

A. Data Analysis Technique

Data analysis was conducted qualitatively and quantitatively. Qualitatively, the data were analyzed through a content analysis approach to regulations, interviews, and normative methods for legal interpretation (Krippendorff, 2013; Suteki & Taufani, 2018). Cyber incident data and AI regulation trends were analyzed quantitatively using descriptive statistics to identify correlations and trend patterns. Data visualization techniques supported interpretation and conclusion formulation (Silverman, 2011; Braun & Clarke, 2006; Miles et al., 2014).

3. Result & Discussion

AI Regulatory Gaps in the National Legal System

The development of AI-related regulations in Indonesia shows quantitative growth but has not been accompanied by strengthening substantive aspects such as accountability, transparency, and personal data protection (Gunawan, 2023; Fadillah, 2022; Sibarani, 2023). As seen in Table 1**,** Indonesia's AI regulatory trends lag far behind those of the European Union and the United States. This suggests a gap between legal needs and the currently available regulatory responses

Figure 1. Comparison of AI Regulation Growth Trends (2019 - 2023)

The limitations in regulatory coverage are also reflected in the content and structure of policies, which are largely sectoral and reactive (Pranata & Dewi, 2021; Darmawan, 2023; Hidayat, 2022). No national legal umbrella explicitly regulates the ethical principles of AI or the responsibility of developers for the impact of the intelligent systems they build, as stipulated in the European Union's AI Act.

This research also found that most Indonesian regulations still rely on voluntaristic or declarative approaches without strong enforcement mechanisms (Setiadi, 2022; Malik, 2023; Santosa, 2023). This makes it difficult to enforce the law in cases of harm caused by AI, such as discriminatory decision-making by algorithmic systems.

Comparisons with other jurisdictions show that Indonesia has yet to implement important principles such as risk assessment, algorithmic auditing, and independent supervision (European Commission, 2021; Jobin et al., 2019; Kusuma, 2024). The Comparative Table of AI Regulations confirms Indonesia's position, which is still in the early stages of AI regulation development.

Table 1. The Comparative Table of AI Regulations

Tabel Komparatif Regulasi AI di Indonesia, Uni Eropa, dan AS

Aspek	Indonesia	Uni Eropa	AS
Transparansi	Terbatas (RUU PDP)	Wajib (AI Act)	Dianjurkan (Blueprint)
Akuntabilitas	Lemah (belum spesifik AI)	Ketat	Relatif longgar
Privasi Data	Masih berkembang	Komprehensif (GDPR)	Bervariasi
Keamanan Siber	Ada (BSSN)	Tertanam	Fokus industri
Penilaian Risiko	Belum diterapkan	Diterapkan penuh	Selektif

This reinforces the gap between the increasingly massive use of AI technology in the public sphere and the lack of national legal preparedness. Without decisive regulatory intervention, the risk of digital rights violations and misuse of technology will continue to increase (Veale & Edwards, 2018; Floridi et al., 2018; Wachter et al., 2017).

Cybersecurity Threats in AI-Based Systems

The application of AI in various sectors in Indonesia, such as e government systems, digital financial services, and the transportation sector, has brought high efficiency and increased vulnerability to cyber threats (BSSN, 2023; ITU, 2023; BRIN, 2024). AI can become a new entry point for cyberattacks, especially when algorithms are not equipped with security layers that are adaptive and resistant to exploitation.

Based on data from BSSN in 2023, the government sector is the main target, with more than 75,000 incidents, followed by the financial and e-commerce sectors (Kominfo, 2023; LIPI, 2023; Nugroho, 2024).

Figure 2. The Distribution of Cyber Incidents by Sector

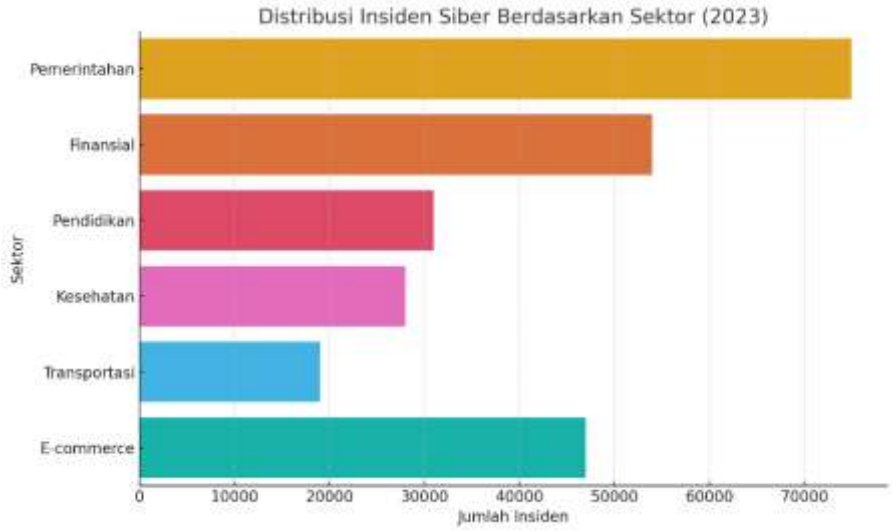

Figure 2 shows the distribution of cyber incidents by sector, reflecting the direct correlation between AI based digitization and attack intensity. Attacks targeting AI systems tend to utilize algorithmic logic gaps, training data manipulation (data poisoning), or adversarial attack techniques that trick AI models (Shneiderman, 2022; Eubanks, 2018; Binns, 2018). This condition is exacerbated by the lack of national technical regulations that require regular vulnerability testing of AI systems.

The absence of minimu security standards for AI systems in Indonesian regulations also leads to a lack of organizational readiness in building AI-aware cyber defenses (Gunawan, 2023; Rahardjo, 2021; Lin et al., 2022). This contrasts with countries such as the US and the European Union, which have implemented the principle of *security by design* in their legal and technical tools.

Building a legal approach that synergizes with technical needs is crucial so that the development and application of AI does not create potential disruptions to national security (Floridi et al., 2018; Cowls et al., 2021; Calo, 2018).

Comparative Analysis and Global Model Adaptation

A comparative analysis of AI regulation in the European Union, the United States, and Indonesia shows fundamental differences in approach (Jobin et al., 2019; Goodman & Flaxman, 2017; UNESCO, 2021). The European Union emphasizes a risk based regulation approach that maps AI systems based on the risk of their impact on human rights and public safety.

The United States emphasizes industry self governance through voluntary ethical guidelines while promoting public accountability through transparency and external audits (White House OSTP, 2022; Lin et al., 2022; Tewary, 2020). Indonesia is

still in the experimental phase of regulation, with an emphasis on data protection and general security infrastructure.

Adapting the global model in the Indonesian context must consider the characteristics of national laws, institutional carrying capacity, and local sociocultural values (Sartor, 2021; Kusuma, 2024; Siregar, 2023). Not all AI Act or Blueprint for AI Rights elements can be directly implemented without substantive and institutional structure adjustments.

AI law reform in Indonesia requires a medium to long-term roadmap that includes drafting an umbrella law, strengthening the capacity of institutions such as BSSN and Kominfo, and public involvement in the technology legislation process (Marzuki, 2017; Sibarani, 2023; Ramli, 2022).

Recommendations for Strengthening the National AI Legal Framework

Based on empirical and juridical findings, this research recommends the establishment of a risk based national legal framework that includes the principles of transparency, accountability, cybersecurity, and fairness (Calo, 2018; Mittelstadt et al., 2016; Jobin et al., 2019). This regulation could be a National Artificial Intelligence Law or a comprehensive ITE Law and PDP Bill revision.

The following recommendation is the development of integrated technical and legal standards, including *AI ethical codes*, *security compliance checklists*, and *algorithmic impact assessments* (Wachter et al., 2017; Winfield & Jirotka, 2018; Cowls et al., 2021). These standards should be mandatory for all developers and institutions using large scale AI systems.

The next step is the establishment of an independent AI watchdog institution, such as the "National Commission on AI Ethics and Regulation", which has the authority to monitor, audit, and administratively sanction violations of AI use (Floridi, 2018; Rahardjo, 2021; Kusuma, 2024).

To support this, the government needs to build the capacity of legal and technological human resources, including training for law enforcement officers, the development of a legal AI curriculum, and partnerships with international research institutions (LIPI, 2023; Kominfo, 2022; Siregar, 2023).

This effort must be underpinned by the principle of *inclusive governance*, which involves the community, academia, the private sector, and international institutions in shaping adaptive and equitable national AI norms (Santosa, 2023; Eubanks, 2018; Binns, 2018).

4. Conclusion

This research shows that Indonesia's legal framework related to artificial intelligence (AI) can still not accommodate the need for oversight and risk mitigation in the context of national cybersecurity. The first objective of the research, identifying

regulatory weaknesses in the oversight of AI use, found that Indonesia lacks comprehensive regulations that explicitly address the principles of accountability, transparency, and protection against misuse of AI systems. While there are some instruments, such as the Personal Data Protection Bill and BSSN technical policies, the approach is still partial, sectoral, and not based on risk assessment as applied in jurisdictions such as the European Union and the United States. Answering the second and third objectives, this research formulates the urgent need for an integrative legal framework that combines the normative aspects of law and the technical needs of cybersecurity. The findings confirm that AI policy development in Indonesia should be directed towards establishing risk-based national regulations equipped with technical standards, independent oversight institutions, and system audit and evaluation mechanisms. An adaptive model that refers to the European Union's AI Act can be used as a reference, with adjustments to national legal values and institutional conditions. Thus, a strong, inclusive, and collaborative AI legal framework is an absolute requirement for the success of Indonesia's safe and equitable digital transformation.

5. References

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. Proceedings of the 2018 Conference on Fairness, Accountability and Transparency, 149 159.

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27 40.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77 101.

Calo, R. (2018). Artificial intelligence policy: A primer and roadmap. UC Davis Law Review, 51(2), 399 435.

Cowls, J., Tsamados, A., Taddeo, M., & Floridi, L. (2021). The AI gambit: Leveraging artificial intelligence to combat climate change Opportunities, challenges, and recommendations. AI & Society, 36(2), 1 20.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Eubanks, V. (2018). Automating inequality: How high tech tools profile, police, and punish the poor. St. Martin's Press.

European Commission. (2021). Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act).

Fadillah, R. (2022). Ethics of artificial intelligence in public services: A legal and policy review. Journal of Law and Technology, 5(1), 45 60.

Floridi, L., Cowls, J., Beltrametti, M., Chiarello, F., & others. (2018). AI4People An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689 707.

Flick, U. (2014). An introduction to qualitative research (5th ed.). SAGE Publications.

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision making and a "right to explanation". AI Magazine, 38(3), 50 57.
Gunawan, A. (2023). National legal policy in facing the era of artificial intelligence. Journal of Law and Development, 53(2), 123 140.
Hidayat, D. (2022). Juridical analysis of the use of AI in Indonesia's digital government system. Journal of Legal Science, 49(3), 211 225.
ITU. (2023). Global cybersecurity index 2023. International Telecommunication Union.
Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389 399.
MOCI. (2022). Indonesia cybersecurity annual report 2022. Ministry of Communication and Information.
Krippendorff, K. (2013). Content analysis: An introduction to its methodology (3rd ed.). SAGE Publications.
Kusuma, H. (2024). Regulation of artificial intelligence in Indonesia: Challenges and opportunities. Journal of Digital Regulation, 2(1), 15 30.
Lin, P., Abney, K., & Bekey, G. A. (2022). Robot ethics: The ethical and social implications of robotics. MIT Press.
Malik, S. (2023). Legal protection against the use of AI in the public sector. Journal of Law and Technology, 6(2), 89 105.
Marzuki, P. M. (2017). Legal research (13th ed.). Kencana Prenada Media Group.
Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1 21.
Neuman, W. L. (2014). Social research methods: Qualitative and quantitative approaches (7th ed.). Pearson Education.
Nugroho, B. (2024). Indonesia's legal readiness to face AI and cybersecurity challenges. Journal of Cyber Law, 4(1), 67 82.