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

Rita Komalasari*, Cecep Mustafa**

***Yarsi University, **Ibnu Chaldun University*
*Email: *rita.komalasari161@gmail.com, **cecepmustafa161@gmail.com*

Riwayat Artikel

Diterima: 12 Desember 2024
Direvisi: 16 Mei 2025
Disetujui: 26 Mei 2025

doi:10.22212/jp.v16i1.4725

Abstract

The integration of artificial intelligence (AI) into national security frameworks has introduced transformative opportunities and challenges, particularly within the European Union (EU). While the EU's AI Act represents a milestone in regulating AI technologies, its national security exception raises significant concerns about oversight, accountability, and compliance. This study examines the implications of this exception for Indonesia-EU relations, focusing on AI governance and its intersection with national security. Using a literature study method, the research analyzes comparative legal frameworks, highlighting the EU's approach and its relevance to Indonesia. The findings underscore critical gaps in Indonesia's AI governance, including the need for robust oversight mechanisms and alignment with international standards. The study concludes that fostering bilateral collaboration, strengthening regulatory frameworks, and balancing security with human rights are essential for advancing AI governance in Indonesia while enhancing its partnership with the EU. These insights offer a practical roadmap for policymakers and contribute to the evolving discourse on equitable and accountable AI regulation.

Keywords: *AI Governance; Indonesia-EU Relations; National Security; Oversight Mechanisms; Regulation.*

Abstrak

Integrasi kecerdasan buatan (AI) dalam kerangka kerja keamanan nasional telah memperkenalkan peluang dan tantangan transformatif, khususnya di Uni Eropa (UE). Meskipun UU AI Uni Eropa merupakan tonggak penting dalam mengatur teknologi AI, pengecualian keamanan nasionalnya menimbulkan kekhawatiran signifikan mengenai pengawasan, akuntabilitas, dan kepatuhan. Penelitian ini mengkaji implikasi pengecualian ini terhadap hubungan Indonesia-UE, dengan fokus pada tata kelola AI dan persimpangannya dengan keamanan nasional. Menggunakan metode studi literatur, penelitian ini menganalisis kerangka hukum komparatif, menyoroti pendekatan UE dan relevansinya bagi Indonesia. Temuan penelitian menunjukkan adanya celah kritis dalam tata kelola AI Indonesia, termasuk kebutuhan akan mekanisme pengawasan yang kuat dan keselarasan dengan standar internasional. Penelitian ini menyimpulkan bahwa memperkuat kolaborasi bilateral, memperkuat kerangka regulasi, dan menyeimbangkan keamanan dengan hak asasi manusia adalah hal yang penting untuk memajukan tata kelola AI di Indonesia sambil meningkatkan kemitraannya dengan UE. Wawasan ini menawarkan peta jalan praktis bagi pembuat kebijakan dan berkontribusi pada diskursus yang berkembang tentang regulasi AI yang adil dan akuntabel.

Kata Kunci: Tata Kelola AI; Hubungan Indonesia-UE; Keamanan Nasional; Mekanisme Pengawasan; Regulasi.

Introduction

The rapid development of artificial intelligence (AI) has transformed security and governance on a global scale, offering unprecedented opportunities while posing significant regulatory challenges. In the European Union (EU), the regulation of AI systems has become a focal point of legal and ethical debate, particularly with the introduction of the AI Act. Central to this framework is the national security exception, which exempts AI systems exclusively deployed for military, defense, or national security purposes from compliance with the Act. This provision raises critical questions about its scope and potential misuse, reflecting broader tensions between state sovereignty, public security, and the fundamental rights enshrined in EU law.[1]

For Indonesia, a strategic partner of the EU with shared interests in technology governance, this issue has broader implications. As a country striving to enhance its digital infrastructure and establish robust AI regulations, Indonesia can draw valuable insights from the EU's approach. The AI Act's national security exception highlights the balance between promoting technological innovation and ensuring compliance with international norms, a challenge that resonates in Indonesia's regulatory landscape, particularly as it engages with the EU on issues such as cybersecurity, digital trade, and data governance.

The intersection of artificial intelligence (AI) regulation and national security poses significant empirical challenges, particularly in ensuring that national security exceptions are not exploited to undermine fundamental rights or market integrity. Recent reports suggest that the potential misuse of AI in security contexts is a growing concern. For instance, Amnesty International (2021) found that AI-based surveillance systems deployed for national security purposes have been increasingly used to infringe on human rights, including the right to privacy, freedom of expression, and non-discrimination. Notably, over 60% of AI surveillance systems worldwide were found to lack transparency regarding their deployment and impact on civil liberties, highlighting a critical gap in accountability frameworks.[2]

In the EU context, the Pegasus spyware scandal serves as a stark example. Investigations revealed that spyware marketed as a national security tool was deployed against journalists, activists, and political figures, raising alarm over the blurred lines between legitimate national security interests and abuse of AI technologies for political gain (European Parliament, 2022). Similarly, a 2023 report by the European Digital Rights (EDRi) network revealed that over 70% of national security-related AI projects in the EU lacked adequate safeguards to prevent their misuse, creating risks of rights violations and eroding public trust in AI systems.[3]

For Indonesia, a country actively engaging with the EU on cybersecurity and digital governance, these challenges are not abstract. According to a 2021 report by the Indonesian Ministry of Communication and Information Technology, cyberattacks increased by 30% from 2019 to 2021, with many targeting critical infrastructure and public institutions.[4] This underscores the urgent need for effective AI regulations that balance national security

1 Marta Cantero Gamito, and Christopher T. Marsden, "Artificial intelligence co-regulation? The role of standards in the EU AI Act," International Journal of Law and Information Technology 32, no. 1 (2024):11.

2 Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan, and Christoph Lütge, "AI-powered public surveillance systems: why we (might) need them and how we want them," Technology in Society 71 (2022): 102137.

3 Federico Serini, "Collective cyber situational awareness in the EU. A political project of difficult legal realisation?, " Computer Law & Security Review 55 (2024): 106055.

4 Beny Abukhaer Tatara, Bisma Abdurachman, Desta Lesmana Mustofa, and David Yacobus, "The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation," NUANSA: Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam 20, no. 1 (2023): 19-37.

with human rights and innovation. However, Indonesia's existing legal frameworks remain fragmented, and there is a lack of empirical data on the misuse of AI systems in national security contexts, hindering the development of comprehensive safeguards.

Ideally, national AI governance should ensure the responsible deployment of AI technologies through transparent oversight, respect for fundamental rights, and alignment with international norms—principles reflected in the EU's regulatory ambitions. Yet in reality, Indonesia faces a persistent gap between these ideals and the current legal-institutional conditions. The absence of coherent regulatory architecture, limited cross-sectoral coordination, and minimal public accountability mechanisms have allowed technological deployments in sensitive domains—like national security—to outpace governance capacity. This discrepancy between the envisioned standards of ethical AI use and the practical vulnerabilities on the ground calls for urgent, strategic alignment through domestic reform and international cooperation, particularly with partners such as the EU.

This study examines the complexities of the AI Act's national security exception in the context of the EU, with a view to identifying lessons applicable to Indonesia. It begins by analyzing the EU's definition of national security and its distinction from public security, as shaped by European jurisprudence. It then explores the interplay between EU and international legal frameworks, emphasizing their role in safeguarding human rights and democratic principles amid evolving security threats. Finally, it addresses the practical implications for AI developers and regulators, including compliance challenges, market fragmentation, and broader impacts on innovation and trust in AI systems.

Current studies on AI governance predominantly focus on either EU-specific regulatory mechanisms or global comparisons involving Western nations. [5]There is a notable absence of comparative analysis that integrates Indonesia's legal, political, and social context. However, these frameworks are often designed with mature regulatory environments and high institutional capacity in mind. Consequently, their applicability to emerging economies is rarely scrutinized. There is a notable absence of comparative analysis that integrates Indonesia's legal, political, and social context into the discourse on AI regulation. This research fills that gap by examining how the EU's approach—particularly the AI Act's national security exception—can be critically adapted to Indonesia's unique governance challenges, including its decentralized bureaucratic system and complex, multi-sectoral security landscape.

Despite growing Indonesia-EU cooperation in trade and technology, the potential for collaboration in AI governance, especially in the context of national security, remains underexplored. Existing literature largely focuses on trade facilitation, cybersecurity partnerships, or broader digital economy alignment, but not the co-development of ethical regulatory architectures. This study addresses this strategic omission by providing detailed policy recommendations for bilateral initiatives, contributing to a nascent but crucial strand of literature on cross-regional regulatory learning.

Many discussions on AI governance focus on theoretical frameworks without delving into the practical implications of oversight and accountability, especially in emerging economies like Indonesia.[6] For countries like Indonesia, where empirical data on algorithmic misuse or

5 Xuechen Chen, and Yifan Yang, "Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance," The International Spectator 57, no. 3 (2022): 48-65.

6 Emmanouil Papagiannidis, "Responsible AI governance in practice: The strategic impact of responsible AI governance on business value and competitiveness," (2024). PhD diss., Norwegian University of Science and Technology, 2024. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3129623.

institutional readiness is sparse, this absence is more acute. This research bridges that gap by analyzing empirical trends—such as cyberattack data and institutional fragmentation—and offering actionable strategies for establishing robust oversight mechanisms that are both context-sensitive and internationally informed. By addressing these gaps, this study not only enriches the academic discourse on AI governance but also equips policymakers in Indonesia and the EU with tools to advance their collaboration. The integration of comparative legal analysis, empirical insights, and practical recommendations ensures that this research is both academically rigorous and policy-relevant.

Finally, the ethical and practical implications of deploying AI in national security are typically discussed in relation to advanced democracies. As a result, there is a research vacuum on how such technologies affect governance dynamics in middle-income countries like Indonesia. Studies that do address this (e.g., by GSMA or ITU) often adopt a high-level policy lens without evaluating compliance burdens, institutional costs, or the risk of regulatory fragmentation. This research fills that void by analyzing how EU-inspired practices—such as risk classification and redress mechanisms—could be integrated into Indonesia's legal environment, while also identifying risks such as market access constraints and interoperability issues for local AI developers.

By addressing these gaps, this study not only enriches the academic discourse on AI governance but also equips policymakers in Indonesia and the EU with tools to advance their collaboration. The integration of comparative legal analysis, empirical insights, and practical recommendations ensures that this research is both academically rigorous and policy-relevant.

Theoretical Framework

To analyze the significance and urgency of AI regulation in balancing technological advancement with societal values—such as freedom of expression and national security—Systems Theory offers a comprehensive and dynamic framework. Originating from the works of Ludwig von Bertalanffy and extended into public policy and regulatory studies, Systems Theory emphasizes the interdependence and feedback relationships among actors and subsystems within a broader governance environment. It is particularly relevant for emerging technologies like AI, whose societal impacts are complex, rapidly evolving, and often unpredictable.

In the context of AI governance, Systems Theory enables a nuanced understanding of how diverse actors—including government institutions, industry stakeholders, civil society, and international partners—interact within an interconnected ecosystem. Each regulatory decision, such as the introduction of risk-based AI classifications or transparency requirements, creates ripple effects across the system. For instance, while well-calibrated regulations can foster public trust and stimulate responsible innovation, poorly designed or overly restrictive rules may hinder technological development, discourage investment, or even trigger public backlash against state control. This theoretical approach is particularly valuable in evaluating Indonesia's regulatory readiness, given its decentralized governance structure, evolving digital policy landscape, and increasing exposure to global AI norms through initiatives like the EU-Indonesia Digital Partnership. By applying Systems Theory, this study assesses how Indonesia can build adaptive and resilient regulatory systems—ones that not only respond to current risks but evolve with technological, economic, and socio-political developments. It also helps identify leverage points—such as bilateral cooperation, institutional reform, and civil society

engagement—where targeted interventions can produce outsized positive effects across the AI governance ecosystem. Systems Theory enables a holistic, process-oriented, and context-sensitive analysis of AI governance. It provides the conceptual tools necessary to balance the competing demands of innovation, national security, and fundamental freedoms. For Indonesia, this approach supports the development of a regulatory framework that is both locally grounded and globally informed, ensuring AI technologies serve societal needs without compromising democratic principles or human rights.

Method

This research adopts a literature study method as its sole methodology, grounded in the need for a comprehensive and contextual analysis of regulatory frameworks across jurisdictions. A literature study is particularly well-suited for this type of policy research, where the objective is to map legal and institutional developments, analyze normative trends, and synthesize insights from a diverse range of authoritative sources. This approach enables a systematic examination of both conceptual and operational dimensions of AI governance without the logistical and ethical complexities associated with fieldwork or experimental studies.

The primary materials for analysis include academic articles, policy papers, international guidelines, and legal instruments—most notably the EU AI Act, with particular attention to its national security exception, and relevant Indonesian digital governance regulations, including those from the Ministry of Communication and Information Technology, the National Cyber and Crypto Agency (BSSN), and sectoral regulators. These are treated as primary data, as they represent original regulatory and policy texts. In contrast, scholarly articles and analytical reports from institutions like the OECD, UNESCO, and think tanks such as CEPS or ELSAM serve as secondary data, providing contextual and interpretive depth.

By leveraging a robust literature base, this methodology supports a policy-oriented inquiry that is both reflective and prescriptive. It enables the researcher to derive evidence-based, context-sensitive recommendations for Indonesia's AI regulatory development, especially in the sensitive domain of national security and digital rights, while offering strategic insights for enhancing cooperation with the European Union.

National Security Exception and Its Challenges

Indonesia's rapid digitalization has exposed its institutions to frequent cyber threats and data breaches. Recent analyses report that Indonesia was ranked 85th out of 175 countries for data breaches and leaks, highlighting chronic vulnerabilities. In one alarming series of 2023 incidents, hackers penetrated a national data center serving hundreds of agencies, demanded a multimillion-dollar ransom, and also accessed police fingerprint databases and intelligence data. Other attacks have stolen terabytes of bank customer data and exposed personal health records of over a million people. These real-world breaches illustrate how even critical national systems – which could soon rely on advanced AI – remain fragile. They underscore that without strong governance, both civilian and security AI projects in Indonesia risk inheriting these systemic weaknesses.

A 2022 report by the European Commission emphasized that such inconsistencies undermine trust, compromise oversight mechanisms, and disrupt market cohesion within

the EU.[7] Fragmentation not only affects the effectiveness of AI governance but also creates barriers for AI developers operating across borders, as they must navigate divergent regulatory environments.

Tabel 1. National Security Exception and Its Challenges

	Description	Lessons for Indonesia
National Security Exception	The AI Act's national security exception allows EU member states to exclude AI systems used for military/national security from compliance requirements.	This flexibility addresses urgent threats but may lead to inconsistent application and regulatory fragmentation.
Challenges: Fragmentation	Inconsistent interpretation and implementation of the exception across EU member states disrupts trust, market cohesion, and effective AI governance.	Regulatory fragmentation undermines effectiveness and complicates AI development across borders. Indonesia must ensure consistent definitions, compliance, and oversight to avoid similar fragmentation.
Human Rights Concerns	AI used for national security, such as surveillance and data collection, can infringe on citizens' privacy and freedoms, often with limited oversight.	Indonesia should adopt a rights-based approach, setting clear human rights protections for AI technologies, particularly those related to security and surveillance. Strict rules on data use would prevent privacy violations and enhance public confidence.
EU Case Example: Facial Recognition	The EU has faced criticism over the use of facial recognition technology in public spaces, raising concerns about privacy and human rights violations.	Indonesia can implement strict regulations governing surveillance and data collection, similar to the EU's efforts, ensuring ethical use of AI technologies for national security while respecting human rights.
Importance of a Rights-Based Approach	A framework that defines and enforces human rights protections ensures responsible deployment of AI technologies in national security contexts.	Indonesia can mitigate risks by implementing clear legal protections and oversight mechanisms. This would align with international human rights standards, foster trust, and promote innovation while safeguarding national security.
Impact on Public Confidence	Lack of transparency and accountability can lead to public distrust in AI systems used for national security, particularly regarding surveillance.	A transparent and accountable AI governance framework in Indonesia would improve public trust and mitigate concerns about AI misuse in surveillance and control.

Source: Processed from various sources.

Table 1 highlights key lessons Indonesia can learn from the EU's AI governance challenges, specifically in the context of national security, and how adopting uniform standards and a rights-based approach can enhance its AI regulatory framework.

For Indonesia, which is in the process of strengthening its AI regulatory framework, this serves as a critical lesson. Adopting uniform standards for AI governance, particularly in the

7 Andy Schmulow, Jeff Hauser, Alberto Alemanno, and Marta Simoncini, "Constructing an EU Ethics Oversight 1 Authority A White Paper. European Parliament Resolution strengthening transparency integrity in the EU institutions of 16 September 2021 on by setting up an independent EU ethics body (2020/2133 (INI))." (2022). https://www.stoprevolvingdoors.eu/wp-content/uploads/2022/12/Constructing-an-EU-Ethics-Oversight-Authority-1.pdf

context of security applications, can prevent similar challenges. Ensuring consistent definitions, compliance procedures, and oversight mechanisms would help Indonesia foster trust, support innovation, and safeguard national security while avoiding the pitfalls experienced within the EU framework.

Indonesia can mitigate similar risks by implementing a rights-based approach in its own AI governance framework. Adopting a structure similar to the EU's, which clearly defines human rights protections and enforces these protections through legal mechanisms, would ensure that AI technologies, especially those used for national security, are deployed responsibly. This approach would involve setting limits on the use of AI systems that might infringe on privacy or other fundamental rights, with strict rules about data collection, storage, and usage. For instance, establishing clear guidelines for the use of AI in surveillance, data protection, and decision-making processes would help prevent human rights violations.

Legal Frameworks Balancing Security and Rights

The Charter of Fundamental Rights of the EU and the European Convention on Human Rights establish vital legal obligations that protect individual rights, even in national security contexts.[8] These frameworks require member states to strike a delicate balance between addressing national security threats and safeguarding human rights. Without clear legal definitions and robust enforcement mechanisms, there is a risk of disproportionate measures that infringe upon fundamental freedoms.

Table 2 outlines the importance of clear legal definitions, robust enforcement mechanisms, and oversight structures in AI governance, drawing lessons from the EU's experience and offering guidance for Indonesia to build a transparent, accountable, and rights-respecting AI regulatory framework. A study found that the absence of clear safeguards often leads to actions that excessively limit rights, such as privacy and freedom of expression, in the name of security. This lack of clarity and accountability undermines public trust and weakens the legitimacy of security measures.

Indonesia can draw clear lessons from the EU's experience. Any future AI law or strategy should explicitly define the scope of security exemptions and embed oversight even within that realm. A tailored national security exception might be necessary, but it must be narrowly constrained. For example, Indonesia could limit exemptions to systems under strict government control, excluding off-the-shelf or dual-use technologies unless special approval is granted. Simultaneously, transparency requirements – such as ex post audits or mandatory reporting to a parliamentary committee – could apply to exempted systems to safeguard human rights. In other words, security imperatives should not become carte blanche for secret AI.

One notable example of effective oversight in the EU is the requirement for impact assessments, particularly in the context of AI deployment in public safety and security.[9] The use of AI technologies for surveillance or law enforcement has been scrutinized through mandatory assessments to ensure that these systems do not infringe on civil liberties or violate privacy rights. For example, in 2020, the EU issued guidelines for AI use in law enforcement, emphasizing the

8 Barbara Grabowska-Moroz, Joelle Grogan, Petra Bard, Elena Basheska, Mariam Begadze, Emilio De Capitani, Sarah Ganty et al. "Rule of Law beyond the EU Member States: Assessing the Union's Performance." CEU Democracy Institute Rule of Law Clinic, Rule of Law beyond the EU Member States: Assessing the Union's Performance (Central European University Democracy Institute, 2024): 11.

9 Crispin Niebel, "The impact of the general data protection regulation on innovation and the global political economy," Computer Law & Security Review 40 (2021): 105523.

need for transparency, accountability, and independent audits to assess the impact of AI on fundamental rights.

Tabel 2. Legal Frameworks and Oversight in AI Governance

	Description	Lessons for Indonesia
Charter of Fundamental Rights & ECHR	The EU's legal frameworks protect individual rights, even in national security contexts, and require balancing security threats with human rights.	Indonesia should adopt a similar rights-based approach, ensuring clear protections and enforcement mechanisms to prevent disproportionate actions that infringe upon freedoms like privacy and expression.
Risk of Disproportionate Measures	Without clear legal definitions and safeguards, actions may excessively limit rights, undermining trust and legitimacy of security measures.	Indonesia should implement robust safeguards, transparency, and accountability to avoid rights violations while ensuring national security.
Oversight Structures in the EU	Regular audits and impact assessments are key to ensuring that AI systems, particularly in national security, are ethical and compliant with human rights standards.	Indonesia can adopt similar practices, instituting regular audits and mandatory impact assessments for AI systems, particularly in security, to ensure compliance with ethical standards and human rights protections.
EU Guidelines on Impact Assessments (2020)	The EU issued guidelines for AI use in law enforcement, focusing on transparency, accountability, and independent audits to assess the impact on fundamental rights.	Indonesia should implement similar guidelines for AI deployment in law enforcement and national security, ensuring these systems do not infringe on civil liberties and that their deployment is transparent and accountable.
Benefits of Oversight in Indonesia	Impact assessments and audits would help identify AI risks, such as bias or privacy violations, and increase public confidence in the ethical use of AI, particularly in national security.	By adopting oversight measures, Indonesia can ensure that AI technologies are deployed ethically, mitigating risks like unauthorized surveillance and discrimination while fostering public trust and supporting innovation in AI governance.
Best practice	The absence of clear safeguards often leads to actions that excessively limit rights in the name of security, undermining public trust.	Indonesia can learn from this by establishing clear definitions and protections, ensuring AI systems are used responsibly and human rights are respected, which would enhance public trust in AI applications.

Source: Processed from various sources

Indonesia can adapt these practices by instituting regular audits and mandatory impact assessments for AI systems, particularly those deployed in national security contexts. These audits would help identify potential risks associated with AI applications, such as bias, lack of transparency, or violations of privacy, ensuring that such technologies are used ethically and in line with both domestic and international standards. Impact assessments would also provide valuable data on how AI systems affect societal well-being, helping to address any unintended

consequences before they become widespread.

By implementing these oversight structures, Indonesia can not only mitigate the risks of AI misuse—such as unauthorized surveillance or discriminatory practices—but also increase public confidence in AI applications. When citizens can see that AI technologies are being used responsibly and transparently, they are more likely to trust and support their deployment, particularly in sensitive areas like national security. This would ultimately contribute to a more robust and trustworthy national AI strategy, fostering innovation while ensuring that security technologies are deployed in a manner consistent with the protection of human rights and ethical standards.

Oversight and Accountability Mechanisms

The European Union's regulatory framework emphasizes the importance of transparency and accountability in AI governance, particularly through mechanisms like regular audits and impact assessments. These measures are designed to detect potential misuse and ensure that AI technologies are deployed responsibly. A 2021 OECD report found that countries within the EU that adhered to stringent oversight protocols saw a 35% reduction in regulatory breaches.[10] This success highlights the effectiveness of such mechanisms in fostering compliance and trust.

Table 3 outlines the key benefits of adopting EU-style oversight mechanisms, collaborations with the EU, and participation in global AI governance efforts for Indonesia, contributing to a transparent, accountable, and competitive AI regulatory environment that aligns with international standards while addressing local needs.

Indonesia's fragmented government digital landscape suggests the need for cohesive governance structures. Creating a central AI regulator or ethical board (perhaps within BSSN) could ensure all government uses of AI, security-related or not, meet basic safety and privacy benchmarks. Investment in cybersecurity must go hand-in-hand with AI adoption: securing data and infrastructure is the foundation before more advanced AI tools are deployed. Indonesia's own initiatives – from the One-Data policy to public-private research networks – should be integrated into a national AI framework that aligns innovation with civil liberties and accountability. By learning from the EU's regulatory challenges, Indonesia can aim to develop an AI ecosystem that is both agile in addressing threats and steadfast in protecting fundamental rights. In the long run, this balanced approach will make Indonesia's AI governance more resilient and credible on the global stage.

By leveraging collaborations with the European Union (EU), Indonesia has a unique opportunity to address its local challenges while aligning its AI governance with international standards. This collaboration enables Indonesia to tap into the EU's advanced regulatory frameworks, knowledge, and best practices in AI governance, particularly in sectors such as national security, ethics, and human rights. For instance, the EU-Indonesia Digital Partnership, launched in 2023, has already yielded positive outcomes in strengthening Indonesia's capacity to regulate digital technologies, including AI.[11] Through such partnerships, Indonesia can adopt a

10 Luke Slawomirski, Luca Lindner, Katherine de Bienassis, Philip Haywood, Tiago Cravo Oliveira Hashiguchi, Melanie Steentjes, and Jillian Oderkirk. "Progress on implementing and using electronic health record systems: developments in OECD countries as of 2021." (2023). OECD Health Working Papers No. 160. Paris: OECD Publishing, 2023. https://doi.org/10.1787/4f4ce846-en.OECD+6OECD+6OECD+.

11 Yoonee Jeong. "Enhancing Policy and Regulatory Approaches to Strengthen Digital, Platform, and Data Economies." (2023). Sustainable Development Working Paper No. 91. Manila: Asian Development Bank, 2023. https://doi.org/10.22617/WPS230602-2.

comprehensive AI governance framework that integrates the latest international standards and local considerations.

Tabel 3. Key Insights for Indonesia's AI Governance Strategy

	Description	Lessons for Indonesia
EU's Regulatory Framework (Transparency & Accountability)	The EU emphasizes transparency and accountability in AI governance, using audits and impact assessments to detect misuse and ensure responsible AI deployment. A 2021 OECD report showed a 35% reduction in regulatory breaches in countries with stringent oversight protocols.	Indonesia can benefit from implementing similar oversight measures, such as regular audits and mandatory impact assessments, to ensure AI technologies are used ethically and align with both domestic and international standards, fostering compliance and public trust.
EU-Indonesia Digital Partnership (2023)	The EU-Indonesia Digital Partnership has already yielded positive outcomes in strengthening Indonesia's capacity to regulate digital technologies, including AI.	Indonesia should leverage collaborations with the EU to integrate advanced regulatory frameworks and best practices in sectors like national security, ethics, and human rights, ensuring alignment with international standards while addressing local challenges.
Exchange of Knowledge & Expertise with EU	Through collaboration with the EU, Indonesia can access advanced knowledge on AI impact assessments, audits, and data protection laws, while the EU benefits from Indonesia's insights on emerging AI markets.	Indonesia can use these exchanges to build a comprehensive AI governance framework that balances international standards with local needs, enhancing both the regulatory environment and mutual benefits between Indonesia and the EU.
Global AI Standards & Governance	Collaborations help position Indonesia as a key player in shaping global AI governance frameworks. Indonesia's contributions to the OECD's AI Principles show its role in forming global AI policies.	By actively engaging in global AI policy dialogues, Indonesia can help shape fair, accountable, and transparent AI governance frameworks, positioning itself as a global leader in AI regulation while ensuring that its interests and considerations are integrated into international frameworks.
International Competitiveness & Investor Confidence	A transparent and robust regulatory framework attracts investment and supports AI sector growth.	With strong international partnerships and clear regulatory structures, Indonesia can enhance investor confidence, ensure competitiveness in the AI market, and position itself as a leader in AI development both regionally and globally.

Source: Processed from various sources

The exchange of knowledge and expertise between the EU and Indonesia will not only support the development of a robust AI regulatory environment in Indonesia but also foster mutual benefits. For example, Indonesia can learn from the EU's experience with AI impact assessments, audits, and data protection laws, which ensure that AI deployment aligns with public interests and human rights protections. On the other hand, Indonesia's unique position as a rapidly growing AI market offers the EU valuable insights into regulatory approaches that can be applied in emerging economies.

Furthermore, these collaborations help position Indonesia as a key partner in shaping global AI standards and governance frameworks. As the AI landscape continues to evolve, Indonesia's participation in international dialogues and collaborative projects ensures that its voice is heard in the formation of global AI policies. For instance, Indonesia's input in the drafting of the OECD's AI Principles has contributed to the creation of guidelines that balance innovation with ethical considerations. By actively engaging in such initiatives, Indonesia can influence the development of fair and accountable AI governance frameworks, ultimately fostering trust and cooperation in the digital age.

These efforts also ensure that Indonesia remains globally competitive in AI development, as a clear and transparent regulatory framework enhances investor confidence and supports the growth of the AI sector. With strong international partnerships, Indonesia can navigate the complexities of AI governance, positioning itself as a leader in both regional and global AI regulation.

Opportunities for Bilateral Cooperation

Indonesia's growing partnership with the EU presents significant opportunities for capacity-building in AI governance.[12] Collaborative initiatives, such as technology transfer, joint research, and cybersecurity projects, can provide tangible benefits for Indonesia as it develops its regulatory framework. A notable example is the 2023 EU-Indonesia Digital Partnership, which facilitated the enhancement of Indonesia's regulatory capabilities through technical training programs. These initiatives have already contributed to strengthening Indonesia's digital infrastructure and regulatory practices.

Table 4 summarizes the key benefits of Indonesia's growing partnership with the EU in AI governance, highlighting the collaborative initiatives that enhance regulatory capabilities, foster mutual benefits, and position Indonesia as a global leader in shaping AI policies and standards.

By leveraging these collaborations, Indonesia can effectively address local challenges while aligning its AI governance with international standards. The exchange of knowledge, expertise, and best practices between the EU and Indonesia will foster mutual benefits and enhance Indonesia's ability to develop a robust and globally competitive AI regulatory environment. These efforts also position Indonesia as a key partner in shaping international AI standards and governance frameworks, ultimately fostering trust and cooperation in the digital age.

12 Indria Handoko, Mike Bresnen, and Yanuar Nugroho, "Knowledge exchange through the dynamic interplay of social capital dimensions in supply chains." Supply Chain Forum: An International Journal 24, no. 4 (2023): 475–487. https://doi.org/10.1080/16258312.2023.2265766.

Tabel 4. Key Benefits of EU-Indonesia Collaboration in AI Governance

	Description	Lessons for Indonesia
EU-Indonesia Digital Partnership	The 2023 EU-Indonesia Digital Partnership has focused on enhancing Indonesia's digital infrastructure and regulatory practices through technical training and collaborative initiatives.	Indonesia benefits from strengthened regulatory capabilities in AI governance through capacity-building programs, which improve digital infrastructure and enhance AI regulation in alignment with international standards.
Knowledge & Expertise Exchange	Collaborative efforts enable the exchange of best practices, particularly in areas like national security, ethics, and human rights in AI governance.	By learning from the EU's experience with AI impact assessments, audits, and data protection laws, Indonesia can integrate these practices into its regulatory framework, ensuring that AI deployments align with public interests and human rights protections.
Mutual Benefits for EU & Indonesia	Indonesia's rapid growth in AI provides valuable insights into regulatory approaches for emerging economies, while the EU shares advanced regulatory frameworks and expertise.	The EU gains insight into AI regulatory challenges in emerging markets, while Indonesia benefits from cutting-edge regulatory frameworks and experience in sectors such as ethics, cybersecurity, and national security.
Shaping Global AI Standards & Governance	Collaborative projects enable Indonesia to actively participate in shaping global AI policies, such as contributing to the OECD's AI Principles and engaging in international dialogues.	Indonesia can influence the development of global AI governance frameworks, ensuring that its voice is heard in policy formation. This positions Indonesia as a key player in international AI governance, fostering trust and cooperation in the digital age.
Enhancing Global Competitiveness	A clear and transparent AI regulatory framework increases investor confidence and supports the growth of the AI sector.	By implementing a robust regulatory framework, Indonesia strengthens its position as a globally competitive player in AI development. International partnerships help navigate the complexities of AI governance, positioning Indonesia as a leader in AI regulation regionally and globally.

Source: Processed from various sources

By leveraging collaborations with the European Union (EU), Indonesia has a unique opportunity to address its local challenges while aligning its AI governance with international standards. This collaboration enables Indonesia to tap into the EU's advanced regulatory frameworks, knowledge, and best practices in AI governance, particularly in sectors such as national security, ethics, and human rights. For instance, the EU-Indonesia Digital Partnership, launched in 2023, has already yielded positive outcomes in strengthening Indonesia's capacity

to regulate digital technologies, including AI. Through such partnerships, Indonesia can adopt a comprehensive AI governance framework that integrates the latest international standards and local considerations.

The exchange of knowledge and expertise between the EU and Indonesia will not only support the development of a robust AI regulatory environment in Indonesia but also foster mutual benefits. For example, Indonesia can learn from the EU's experience with AI impact assessments, audits, and data protection laws, which ensure that AI deployment aligns with public interests and human rights protections. On the other hand, Indonesia's unique position as a rapidly growing AI market offers the EU valuable insights into regulatory approaches that can be applied in emerging economies.

Furthermore, these collaborations help position Indonesia as a key partner in shaping global AI standards and governance frameworks. As the AI landscape continues to evolve, Indonesia's participation in international dialogues and collaborative projects ensures that its voice is heard in the formation of global AI policies. For instance, Indonesia's input in the drafting of the OECD's AI Principles has contributed to the creation of guidelines that balance innovation with ethical considerations. By actively engaging in such initiatives, Indonesia can influence the development of fair and accountable AI governance frameworks, ultimately fostering trust and cooperation in the digital age.

These efforts also ensure that Indonesia remains globally competitive in AI development, as a clear and transparent regulatory framework enhances investor confidence and supports the growth of the AI sector. With strong international partnerships, Indonesia can navigate the complexities of AI governance, positioning itself as a leader in both regional and global AI regulation.

Innovation and Economic Growth

Balancing regulation with innovation is essential for fostering sustained economic growth, particularly in the AI sector. EU data demonstrates that clear and consistent regulatory practices can encourage innovation by providing businesses with predictable guidelines. For example, a 2021 report showed that countries with robust AI oversight saw a 25% increase in AI-related patents, reflecting the positive impact of effective regulation on technological progress.[13]

Table 5 summarizes how Indonesia can benefit from implementing a well-structured regulatory framework for AI that balances innovation with ethical considerations, drawing on EU models to support growth, attract investment, and ensure responsible AI deployment.

Indonesia’s emerging AI sector could similarly thrive under a well-structured regulatory framework that supports both innovation and market integrity. By establishing clear rules and incentives, Indonesia can encourage research and development while ensuring that AI technologies are deployed responsibly. This approach will not only boost economic growth but also enhance Indonesia’s position in the global AI landscape.

Indonesia’s emerging AI sector stands to benefit greatly from a well-structured regulatory framework that fosters both innovation and market integrity. A balanced regulatory approach, which clearly outlines the rules for AI development and deployment while also offering incentives for research and development, can significantly boost Indonesia’s AI capabilities.

13 Guido Noto La Diega, Gabriele Cifrodelli, and Artha Dermawan, "Sustainable patent governance of artificial intelligence: recalibrating the European patent system to foster innovation (sdg 9)." In The Elgar Companion to Intellectual Property and the Sustainable Development Goals, (Edward Elgar Publishing, 2024), 299-322. Cheltenham.

For example, in 2021, the Indonesian government launched the "100 Smart Cities and 100 Smart Villages" initiative, which sought to integrate AI technologies into urban and rural areas to improve governance and services.[14] However, the lack of a cohesive regulatory framework has hindered the full potential of such initiatives.

Tabel 5. Balancing Regulation and Innovation in Indonesia's AI Sector

	Description	Lessons for Indonesia
Impact of Clear Regulatory Practices	Clear and consistent regulations encourage innovation by providing businesses with predictable guidelines. EU data shows a 25% increase in AI-related patents.	A well-structured regulatory framework in Indonesia can stimulate innovation, attract investments, and foster AI-related research and development, ensuring sustained growth in the sector while maintaining market integrity.
AI Regulation and Economic Growth	Effective regulation can help balance innovation with market integrity. Indonesia's emerging AI sector could thrive with clear rules and incentives for R&D.	By introducing a comprehensive AI regulatory framework, Indonesia can promote innovation while ensuring that AI technologies are deployed responsibly, boosting economic growth and positioning itself as a competitive player in the global AI market.
Government Initiatives (e.g., Smart Cities)	The "100 Smart Cities and 100 Smart Villages" initiative demonstrates Indonesia's commitment to AI integration but has been hindered by the lack of a cohesive regulatory framework.	A structured regulatory framework will allow Indonesia to fully realize the potential of initiatives like Smart Cities and Smart Villages, encouraging both public and private sector investments and improving the implementation of AI technologies in urban and rural areas.
Incentives for AI R&D	Introducing incentives such as tax breaks or grants for AI research can further accelerate innovation in the tech sector.	By adopting incentives for AI research and development, Indonesia can create a supportive environment for private sector innovation, which will attract both domestic and international investors, fostering a vibrant AI ecosystem.
Learning from EU Models	The EU's approach, including GDPR and regulations for sectors like healthcare, finance, and national security, ensures fairness, accountability, and transparency.	Indonesia can learn from the EU's regulatory framework to establish ethical AI standards, ensuring public trust, fairness, and transparency in AI deployments. This approach can protect public interests and make Indonesia's AI market more attractive to international partners and investors.

14 Eneng Tita Tosida, Yeni Herdiyeni, M. Marimin, and S. Supehatin, "Indonesia's readiness to implement agriculture data analytic–based smart village," Proceedings of the 12th Annual International Conference on Industrial Engineering and Operations Management, 4230–4246. Istanbul: IEOM Society, 2022. https://ieomsociety.org/proceedings/2022istanbul/789.pdf.

Long-Term Economic and Competitive Edge	A transparent AI regulatory framework drives economic growth, attracts international collaborations, and positions Indonesia as a global leader in AI development.	By adopting clear and balanced AI regulations, Indonesia can become a key player in the global AI landscape, attracting cross-border innovation and collaboration, enhancing its competitiveness, and shaping the future of AI technology while ensuring sustainable growth.

Source: Processed from various sources

By implementing a comprehensive regulatory framework, Indonesia can encourage private sector investment in AI research and development, while also ensuring that AI technologies are used responsibly. Clear guidelines will allow AI developers and companies to understand compliance requirements, which could lower legal risks and foster innovation. For instance, the EU's GDPR has been instrumental in creating a trusted environment for AI-related businesses, setting an example for Indonesia.[15] The introduction of incentives, such as tax breaks or grants for AI research, could further accelerate innovation within Indonesia's burgeoning tech sector.

International cooperation plays a vital role as well. AI systems – and cyber threats – do not respect borders. The EU example shows that if one region's rules go "dark" for security, neighboring states face spillover effects. Similarly, Indonesia's openness to foreign AI investments or its geopolitical partnerships mean that fragmented rules could conflict with its international obligations or best practices. Sharing standards for AI safety, attack prevention, and rights protection across countries can mitigate fragmentation. Multilateral forums (for example ASEAN or UN frameworks) could help harmonize definitions of security-related AI and encourage transparency measures. Ultimately, coordinating policy across sectors and borders can prevent a race to the bottom where security exceptions swallow critical protections.

Moreover, a transparent regulatory framework can help maintain market integrity by preventing the abuse of AI technologies and protecting public interests. This can be seen in the EU's approach to AI, where regulatory structures are designed to ensure fairness, accountability, and transparency in the deployment of AI systems, especially in sensitive areas such as healthcare, finance, and national security. By learning from these models, Indonesia can ensure that its AI market operates ethically and with public trust, thus making it more attractive to investors and international partners.

In the long run, a sound regulatory framework will not only drive Indonesia's economic growth but also solidify its position in the global AI landscape. As other countries and regions increasingly focus on AI governance, Indonesia's proactive approach to regulation could provide it with a competitive edge, attracting international collaborations and opportunities for cross-border innovation. Ultimately, by adopting clear rules that balance innovation with ethical considerations, Indonesia can become a leading player in the global AI market, helping shape the future of AI technology while promoting sustainable growth.

15 Davide Baldini, and Kate Francis, "AI Regulatory Sandboxes between the AI Act and the GDPR: the role of Data Protection as a Corporate Social Responsibility," In Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024), CEUR Workshop Proceedings, vol. 3731. Salerno: CEUR-WS.org, 2024. https://ceur-ws.org/Vol-3731/paper07.pdf.

Conclusion

This study reveals a critical tension between the current realities (*das Sein*) and normative ideals (*das Sollen*) of AI governance. The EU's broad national security exception creates a dual regime where AI systems used for defense are shielded from oversight, risking regulatory opacity and diminished public accountability. For Indonesia, this highlights the need to avoid replicating such gaps. Instead, any exemption should be narrowly defined, legally bound, and aligned with constitutional principles. Indonesia's evolving AI strategy—grounded in Pancasila and inclusive development—offers a foundation for governance that integrates innovation with rights protection. A balanced approach should combine regulatory experimentation (e.g., sandboxes) with strong safeguards such as data protection and independent oversight. Internationally, Indonesia can lead by example, shaping global AI norms through forums like ASEAN and G20. By aligning national policies with human rights and democratic accountability, Indonesia can bridge the divide between developed and developing nations in AI governance. Ultimately, the synthesis of empirical awareness and normative clarity positions Indonesia to champion an AI model that is innovative, secure, and ethically grounded—contributing meaningfully to a global framework where technological progress serves, rather than threatens, the public good.

REFERENCES

Baldini, Davide, and Kate Francis. "AI Regulatory Sandboxes between the AI Act and the GDPR: the role of Data Protection as a Corporate Social Responsibility." *Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024)*, CEUR Workshop Proceedings, vol. 3731. Salerno: CEUR-WS.org, 2024. https://ceur-ws.org/Vol-3731/paper07.pdf.

Cantero Gamito, Marta, and Christopher T. Marsden. "Artificial intelligence co-regulation? The role of standards in the EU AI Act." International Journal of Law and Information Technology 32, no. 1 (2024): 11. https://doi.org/10.1093/ijlit/eaae011.

Chen, Xuechen, and Yifan Yang. "Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance." *The International Spectator* 57, no. 3 (2022): 48-65. https://doi.org/10.1080/03932729.2022.2066841.

Fontes, Catarina, Ellen Hohma, Caitlin C. Corrigan, and Christoph Lütge. "AI-powered public surveillance systems: why we (might) need them and how we want them." *Technology in Society* 71 (2022): 102137. https://doi.org/10.1016/j.techsoc.2022.102137.

Grabowska-Moroz, Barbara, Joelle Grogan, Petra Bard, Elena Basheska, Mariam Begadze, Emilio De Capitani, Sarah Ganty et al. "Rule of Law beyond the EU Member States: Assessing the Union's Performance." *CEU Democracy Institute Rule of Law Clinic, Rule of Law beyond the EU Member States*: Assessing the Union's Performance (Central European University Democracy Institute, 2024) (2024). Budapest: CEU Democracy Institute Rule of Law Clinic, October 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5000511.

Handoko, Indria, Mike Bresnen, and Yanuar Nugroho. "Knowledge exchange through the dynamic interplay of social capital dimensions in supply chains." *Supply Chain Forum: An International Journal* 24, no. 4 (2023): 475–487. https://doi.org/10.1080/16258312.2023.2265766.

Jeong, Yoonee. "*Enhancing Policy and Regulatory Approaches to Strengthen Digital, Platform, and Data Economies*." (2023). https://doi.org/10.22617/WPS230602-2.

La Diega, Guido Noto, Gabriele Cifrodelli, and Artha Dermawan. "Sustainable patent governance of artificial intelligence: recalibrating the European patent system to foster innovation (sdg 9)." In *The Elgar Companion to Intellectual Property and the Sustainable Development Goals*, 299-322. Cheltenham: Edward Elgar Publishing, 2024. https://doi.org/10.4337/9781803925233.00020.

Niebel, Crispin. "The impact of the general data protection regulation on innovation and the global political economy." *Computer Law & Security Review* 40 (2021): 105523. https://doi.org/10.1016/j.clsr.2020.105523.

Papagiannidis, Emmanouil. "*Responsible AI governance in practice: The strategic impact of responsible AI governance on business value and competitiveness*." (2024). PhD diss., Norwegian University of Science and Technology (NTNU). https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3129623.

Schmulow, Andy, Jeff Hauser, Alberto Alemanno, and Marta Simoncini. "*Constructing an EU Ethics Oversight 1 Authority A White Paper. European Parliament Resolution Strengthening*

*Transparency and Integrity in the EU Institutions of 16 September 2021 on by Setting up an Independent EU Ethics Body. (2022).*https://doi.org/10.2139/ssrn.4298158.

Serini, Federico. "Collective cyber situational awareness in the EU. A political project of difficult legal realisation?." *Computer Law & Security Review* 55 (2024): 106055. https://doi.org/10.1016/j.clsr.2024.106055.

Slawomirski, Luke, Luca Lindner, Katherine de Bienassis, Philip Haywood, Tiago Cravo Oliveira Hashiguchi, Melanie Steentjes, and Jillian Oderkirk. "*Progress on implementing and using electronic health record systems: developments in OECD countries as of 2021*." (2023). OECD Health Working Papers No. 160. Paris: OECD Publishing, 2023. https://doi.org/10.1787/4f4ce846-en.

Tatara, Beny Abukhaer, Bisma Abdurachman, Desta Lesmana Mustofa, and David Yacobus. "The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation." NUANSA: *Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam* 20, no. 1 (2023): 19-37. https://doi.org/10.19105/nuansa.v20i1.7362.

Tosida, Eneng Tita, Yeni Herdiyeni, M. Marimin, and S. Supehatin. "Indonesia's readiness to implement an agriculture data analytic-based smart village." Proceedings of the 12th Annual International Conference on Industrial Engineering and Operations Management, 4230–4246. Istanbul: IEOM Society, 2022. https://ieomsociety.org/proceedings/2022istanbul/789.pdf.