

Formulating a Responsive Regulatory Architecture for Artificial Intelligence Misuse: A Comparative Legal Politics Study of Indonesia and the Netherlands

St. Muslimah Suciati^{a*}, Idris Saputra^a, La Ode Muhammad Saleh Saputra^a, Gerrit Henk Addink^b

^a Faculty of Law, Universitas Halu Oleo, Kendari, Indonesia.

^b Utrecht University, Utrecht, Netherlands

 : sitimuslimahsuciati@gmail.com

Corresponding Author*



Abstract

Introduction: The rapid development of Artificial Intelligence (AI) has created complex legal challenges involving privacy, reputation, accountability, digital evidence, and legal certainty. Indonesia and the Netherlands provide relevant comparative contexts because both are rooted in civil law traditions but demonstrate different approaches to AI governance.

Purposes of the Research: This study aims to analyze the legal politics and regulatory configuration governing AI misuse in Indonesia and the Netherlands, identify Indonesia's regulatory gaps, and formulate a context-specific reform model based on relevant Dutch practices.

Methods of the Research: This study employs normative legal research using comparative and conceptual approaches. Primary legal materials include Indonesian legislation, the EU Artificial Intelligence Act, the General Data Protection Regulation, Dutch criminal law, and relevant jurisprudence. The materials are analyzed qualitatively through deductive and prescriptive-comparative reasoning using legal politics, responsive law, risk-based regulation, and human-centric AI governance as analytical frameworks.

Results Main Findings of the Research: The findings indicate that Indonesia has a predominantly development-oriented and fragmented regulatory configuration, relying on general and sectoral instruments, while the Netherlands demonstrates a more rights-centred, risk-based, and institutionally coordinated framework. Three gaps are identified in Indonesia: substantive AI-specific norms, institutional oversight, and procedural mechanisms for AI-related evidence and enforcement. This study proposes a Three-Tier Regulatory Architecture comprising AI-specific legislation as a substantive *lex specialis*, an AI supervisory authority, and adaptive enforcement and evidentiary mechanisms. The model provides a pathway for shifting Indonesia from reactive regulation toward responsive and anticipatory AI governance while maintaining legal certainty, rights protection, and regulatory proportionality.

Keywords: Artificial Intelligence Misuse; Legal Politics; Regulatory Reform; Comparative Law.

Submitted: 2026-04-29	Revised: 2026-08-28	Accepted: 2026-08-30	Published: 2026-08-31
How To Cite: St. Muslimah Suciati, Idris Saputra, La Ode Muhammad Saleh Saputra, and Gerrit Henk Addink. "Formulating a Responsive Regulatory Architecture for Artificial Intelligence Misuse: A Comparative Legal Politics Study of Indonesia and the Netherlands." PATTIMURA Legal Journal 5 no. 2 (2026): 139-167. https://doi.org/10.47268/pela.v5i2.25563			
Copyright © 2026 Author(s)  Creative Commons Attribution-NonCommercial 4.0 International License			

INTRODUCTION

The development of *Artificial Intelligence* (AI) has fundamentally changed the patterns of social, economic, and state governance relations. AI is no longer just a computing aid, but has transformed into a decision-making system that impacts the health, financial, education,

defense, and law enforcement sectors.¹ This phenomenon has accelerated digitalization, resulting in high efficiency, while simultaneously creating new avenues for illegal activities. Globally, AI is recognized as a double-edged sword; on one hand, it can enhance public welfare, but on the other, it carries the potential to give rise to systemic risks.² The misuse of AI, such as deepfakes for fraud and defamation, algorithmic bias in public decision-making, massive privacy violations through AI-based surveillance, and the use of AI for cybercrime, has become a threat affecting social stability and national security.³ Therefore, the need for responsive AI governance has become an urgent legal agenda.

Reports from various institutions such as the World Economic Forum and INTERPOL identify AI-based crime, including adaptive cyberattacks and large-scale data manipulation, as serious threats to global security and stability.⁴ Without appropriate regulatory design, AI has the potential to become an instrument that deepens social injustice and vulnerability. This indicates that the misuse of AI cannot be viewed as an ordinary crime, but rather as a new legal phenomenon that is cross-jurisdictional and has far-reaching impacts. Consequently, AI regulation must be understood as part of the state's obligation to maintain public order and protect the rights of its citizens.

The international legal community has responded to this situation through various normative instruments, emphasizing the importance of ethical and human rights-based AI governance. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) highlights the principles of human rights, inclusiveness, transparency, and accountability as the foundation of global ethics in the development and utilization of AI.⁵ These principles

¹ Aman Kumar Mishra et al., "Revolutionizing Government Operations," in *Conversational Artificial Intelligence*, ed. Romil Rawat (Wiley, 2024), 607–34, <https://doi.org/10.1002/9781394200801.ch34>.

² Mahmoud Mohieldin, Maria Alejandra Gonzalez-Perez, and Mohamed Zahran, "The Double-Edged Sword: AI's Promise and Threat in Addressing Societal Challenges," in *AI-Powered Sustainable Business* (Cham: Palgrave Macmillan, 2025), 19–40, https://doi.org/10.1007/978-3-031-93357-8_2.

³ Shasha Yu and Fiona Carroll, "Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges," in *Artificial Intelligence in Cyber Security: Impact and Implications*, ed. Reza Montasari and Hamid Jahankhani (Cham: Springer, 2021), 157–75, https://doi.org/10.1007/978-3-030-88040-8_6.

⁴ Muhammad Abdullah et al., "Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data," *Analytics* 4, no. 3 (2025): 25, <https://doi.org/10.3390/analytics4030025>.

⁵ Michał Balcerzak, "Implications of the United Nations Human Rights Standards for the Development of Artificial Intelligence," in *Artificial Intelligence and International Human Rights Law* (Cheltenham: Edward Elgar Publishing, 2024), 6–24, <https://doi.org/10.4337/9781035337934.00008>.

require that AI-generated decisions remain traceable, supervised, and accountable to humans, thereby preventing AI from becoming a "black box" immune to legal oversight.⁶ The Organization for Economic Co-operation and Development Artificial Intelligence (OECD AI) Principles 2019 also emphasize that AI systems must be lawful, ethical, and robust, which means complying with applicable laws, respecting human rights values,⁷ and designed to minimize the risk of failure or misuse. This set of international principles reflects a paradigm shift, signifying that AI regulation is not merely a matter of technical policy choice, but rather a normative obligation of the state to protect human dignity and public order.

One of the main challenges in AI governance is the phenomenon of law's latency, referring to the lag in legal frameworks keeping pace with technological advancement.⁸ Legal systems are generally designed for conventional patterns of conduct, whereas AI presents new forms of offenses that are anonymous, automated, and difficult to trace. In deepfake cases, for instance, the perpetrator's identity can be concealed through global networks, while victims may suffer damages within minutes.⁹ Another issue arises in the aspect of legal liability, as the relationship between developers, users, and AI systems is often unclear. This has sparked debate on whether existing laws can sufficiently be adapted through an adaptive regulation approach, or if normative reconstruction is required by establishing a specific legal framework or *lex specialis* for AI. This choice is not merely technical but constitutes part of the state's legal policy, which determines whether AI regulation will be risk-oriented, human rights-based, or focused on accelerating innovation.

Indonesia, as a country with very high internet penetration, is facing an escalation in the misuse of Artificial Intelligence (AI).¹⁰ This phenomenon shows that AI not only increases

⁶ Joel Frenette, "Ensuring Human Oversight in High-Performance AI Systems: A Framework for Control and Accountability," *World Journal of Advanced Research and Reviews* 20, no. 2 (2023): 1507–16, <https://doi.org/10.30574/wjarr.2023.20.2.2194>.

⁷ Irēna Barkāne et al., "Integrating Ethical Principles and Human Rights Based Approach in the EU Artificial Intelligence Act and the Council of Europe Convention on Artificial Intelligence: Interplay of Ethics and Law in the AI Regulation Debate," *Journal of the University of Latvia. Law*, no. 19 (2025): 43–59, <https://doi.org/10.22364/jull.19.03>.

⁸ Leo S. F. Lin, "Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud," *Laws* 14, no. 4 (2025): 46, <https://doi.org/10.3390/laws14040046>.

⁹ Asher Flynn et al., "Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery," *Journal of Interpersonal Violence*, September 9, 2025, 1–35, <https://doi.org/10.1177/08862605251368834>.

¹⁰ Abidin Fikri and Tina Amelia, "Indonesia's Legal Policy on Protecting Personal Data from Artificial Intelligence Abuse," ed. Y. Jusman et al., *SHS Web of Conferences* 204 (2024): 1–11, <https://doi.org/10.1051/shsconf/202420407002>.

technological efficiency, but also expands the scope of digital crimes that are difficult to control.¹¹ Normatively, Indonesia does not yet have a specific law on AI, meaning law enforcement still relies on fragmented regulations, such as Law Number 1 of 2024 concerning the Second Amendment to the Information and Electronic Transactions Law and Law Number 27 of 2022 concerning Personal Data Protection. The Circular Letter of the Minister of Communication and Informatics Number 9 of 2023 regarding Artificial Intelligence Ethics remains at the level of soft law, lacking sufficient enforceability, thus creating a disparity between the public's need for legal protection and the available normative instruments. Indonesia lacks an omnibus regulation or a specific law that comprehensively governs the AI framework, covering development, implementation, and accountability for misuse. This situation reflects that Indonesia's legal policy in the AI sector has not yet demonstrated a clear and integrated direction.

In contrast, the Netherlands has established a relatively comprehensive AI governance system within the legal framework of the European Union. The Netherlands is bound by the EU AI Act 2024, which adopts a risk-based approach by classifying AI systems into categories of minimal, limited, high, and unacceptable risk, along with proportionate legal obligations based on the level of threat.¹² Article 14 of the EU AI Act explicitly requires that high-risk AI systems be designed and developed in such a way that they can be effectively supervised by humans. At the national level, the Netherlands integrates the AI regime with the General Data Protection Regulation (GDPR) and the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*). Article 22 of the GDPR grants individuals the right not to be subject to a decision based solely on automated processing which produces legal effects or similarly significant effects concerning them. This regulation provides a strong normative basis for controlling the use of AI in public and private decision-making processes. The Hague Court of Justice ruling in the SyRI (System Risk Indication) case in 2020, which stated that the use of social monitoring algorithms by the government violates Article 8 of the European Convention

¹¹ Zulfikar Hasan and Diska Sendi Marisna, "Artificial Intelligence: Making Crime Easier in the World of Finance?," *AL-ARBAH: Journal of Islamic Finance and Banking* 6, no. 2 (2024): 223–56, <https://doi.org/10.21580/al-arbah.2024.6.2.22187>.

¹² Nicoletta Rangone and Luca Megale, "Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making," *European Journal of Risk Regulation* 16, no. 3 (2025): 1082–97, <https://doi.org/10.1017/err.2025.13>.

on Human Rights (ECHR),¹³ demonstrates how human rights principles serve as parameters to test the legitimacy of the use of AI by the state.

The Netherlands also adopts a human-centric approach to AI governance, placing human dignity, non-discrimination, and transparency as absolute principles that cannot be compromised in the name of technological efficiency.¹⁴ The Netherlands also has a strong data protection authority, the Autoriteit Persoonsgegevens, which plays a key role in data-driven AI oversight.¹⁵ Consequently, the Netherlands can be positioned as a regulatory laboratory offering best practices for comparison with Indonesia's still fragmented conditions.

Indonesia and the Netherlands share legal systems rooted in the civil law tradition. Indonesia inherited the codification structure and legalistic approach from the Dutch legal system, yet faces significant challenges regarding regulatory fragmentation in addressing the misuse of Artificial Intelligence (AI). In Indonesia, handling AI misuse still relies on general instruments such as the Information and Electronic Transactions Law and the Personal Data Protection Law, which were not originally designed to govern algorithmic accountability, proof of synthetic content, and the attribution of responsibility between developers and users. Conversely, the Netherlands has developed a more mature AI regulatory ecosystem through the integration of the EU AI Act (Regulation (EU) 2024/1689), the GDPR, and the strengthening of supervisory bodies such as the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and transparency mechanisms like the Algorithm Register (Algoritmeregister). This disparity highlights the urgency to identify Indonesia's regulatory gaps while mapping Dutch best practices that can be selectively adapted to fit Indonesia's national socio-legal context.

The urgency of this research lies in the normative need to address the legal vacuum (*Rechtsvacuum*) in AI regulation in Indonesia, which creates conditions of impunity for

¹³ Adamantia Rachovitsa and Niclas Johann, "The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case," *Human Rights Law Review* 22, no. 2 (2022): 1-15, <https://doi.org/10.1093/hrlr/ngac010>.

¹⁴ Farman Saeed Sedeeq and Percem Arman, "Human-Centric AI Governance: An Adaptive Public International Law Framework for Ethical and Inclusive AI Regulation in Public Health," *Journal of Law, Medicine & Ethics* 53, no. 4 (2025): 563-74, <https://doi.org/10.1017/jme.2025.10175>.

¹⁵ Lucas M Haitsma, "Addressing Discrimination in Algorithmic Profiling: Examining Risk Governance in Dutch Public Social Security Agencies," *European Journal of Social Security* 27, no. 2 (2025): 191-212, <https://doi.org/10.1177/13882627251351093>.

perpetrators of AI misuse and leaves victims without adequate legal protection. This phenomenon indicates that the issue is not merely technical-technological but represents a legal crisis requiring analysis from the perspective of legal policy. Therefore, this comparative study is essential to formulate the direction of legal policy and design regulatory reforms for AI in Indonesia that are more responsive, adaptive, and oriented towards the protection of fundamental rights and legal certainty.

Previous studies show that research on AI regulation in Indonesia has evolved but remains focused on specific sectors or limited to general policy recommendations. Umami Maskanah, in the *Jambura Law Review*, emphasizes the importance of utilizing AI within the civil justice system and offers a practical framework to ensure that AI implementation remains aligned with the principles of due process and the protection of litigants' rights.¹⁶ Meanwhile, Prabu Revolusi and Radians Krisna Febriandy, in the *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, propose a regulatory strategy based on cross-country comparative learning, highlighting policy approaches from the European Union, the United States, and Singapore.¹⁷ Both studies have made significant contributions by demonstrating the urgency of establishing AI regulation and the necessity for ethical standards and algorithmic accountability. However, existing research is limited by the lack of in-depth focus on AI misuse as a form of criminality and human rights violation, as well as the absence of a systematic legal policy analysis to determine the direction for establishing a specific legal framework or *lex specialis* for AI in Indonesia. Therefore, this study aims to fill this gap by focusing on the configuration of regulations concerning AI misuse through the perspective of legal policy, and by formulating a model for normative reform that is both operational and contextual.

The novelty of this research lies in its normative-comparative approach, which specifically compares the legal policies governing AI misuse between Indonesia and the Netherlands both civil law jurisdictions while utilizing the EU AI Act and Dutch law enforcement practices as

¹⁶ Umami Maskanah, "Artificial Intelligence in Civil Justice: Comparative Legal Analysis and Practical Frameworks for Indonesia," *Jambura Law Review* 7, no. 1 (2025): 225–42, <https://doi.org/10.33756/jlr.v7i1.27786>.

¹⁷ Prabu Revolusi and Radians Krisna Febriandy, "Developing AI Regulations in Indonesia: Policy Recommendations Based on Comparative Policy Analysis from the European Union, the United States, and Singapore," *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi* 6, no. 2 (2025): 1035–49, <https://doi.org/10.63447/jimik.v6i2.1380>.

relevant references of best practices for adaptation in Indonesia. This study not only maps existing regulations but also analyzes the policy configuration through the legal policies that underpin the regulatory models in each country. The objectives are to examine how legal policies and regulatory frameworks concerning the misuse of artificial intelligence are structured within the positive legal systems of Indonesia and the Netherlands, including the characteristics of regulatory fragmentation in Indonesia and the multi-layered structure of regulation in the Netherlands. Furthermore, this research aims to formulate a model of regulatory reform for Indonesia to address the normative vacuum regarding AI misuse, based on the best practices of regulation and law enforcement in the Netherlands. Consequently, this study offers a scientific contribution in the form of a prescriptive design for AI regulatory reform that is compatible with the existing legal system. This approach is expected to strengthen the direction of national law-making, ensuring it is responsive to the threats posed by AI misuse while remaining aligned with the principles of fundamental rights protection and legal certainty.

METHODS OF THE RESEARCH

This study employs normative legal research focusing on the analysis of legal policy and the configuration of regulations concerning artificial intelligence misuse within the legal systems of Indonesia and the Netherlands. The research utilizes comparative and conceptual approaches by comparing the regulatory frameworks and law enforcement practices related to AI misuse in both countries, while examining them through the perspective of legal policy. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, Law Number 1 of 2024 concerning the Second Amendment to the Information and Electronic Transactions Law, Law Number 27 of 2022 concerning Personal Data Protection, the Criminal Code, the EU AI Act (Regulation (EU) 2024/1689), the GDPR (Regulation (EU) 2016/679), as well as Dutch national legal provisions such as the *Wetboek van Strafrecht* and relevant court decisions such as the SyRI case. Secondary legal materials consist of books, indexed law journals, academic articles, reports from international institutions, and previous studies discussing AI regulation, AI-based cybercrime, and legal policy for digital regulatory reform.

Tertiary legal materials include legal dictionaries, legal encyclopedias, and supporting sources such as regulatory indexes and glossaries of AI technology terms. The legal materials are processed through inventorying, relevance identification, classification, and systematization based on the themes of regulation, law enforcement, and models for AI regulatory reform. Furthermore, analysis is conducted qualitatively using deductive reasoning and prescriptive-comparative argumentation to draw conclusions regarding the patterns of legal policy governing AI misuse in Indonesia and the Netherlands, as well as to design a model of regulatory reform suitable for adaptation in Indonesia.

RESULTS AND DISCUSSION

A. Legal Politics and Configuration of Artificial Intelligence Abuse Regulations in the Positive Legal Systems of Indonesia and the Netherlands

Indonesia's AI legal policy is grounded in Pancasila and the 1945 Constitution as the grundnorm that determines the direction and boundaries of national legal development in the technological sector. The principle of Just and Civilized Humanity obliges the state to ensure that AI development does not compromise human dignity, while the principle of Social Justice for All the People of Indonesia demands the equitable distribution of AI benefits alongside equal protection against the risks of misuse. Article 28G paragraph (1) of the 1945 Constitution guarantees everyone's right to protection of their person, honor, dignity, and property, whereas Article 28D paragraph (1) guarantees the right to recognition, assurance, protection, and fair legal certainty. Together, these articles form a constitutional mandate for the state to regulate AI misuse that threatens these fundamental rights. However, this constitutional mandate has not yet been translated into an adequate positive legal architecture, creating a contradiction between strong constitutional guarantees and the reality of weak legal protection. Ideologically, Indonesia's legal policy in the digital technology sector exhibits developmentalist-statist characteristics, whereby the state utilizes digital transformation as a primary instrument for accelerating economic development¹⁸ resulting in innovation and digital economic growth being prioritized over legal protection against technological risks.

¹⁸ Lorena Valencia-Gálvez et al., *The Routledge International Handbook of Social Work Teaching*, ed. Jarosław Przeperski and Rajendra Baikady (London: Routledge, 2024), <https://doi.org/10.4324/9781003422402>.

The National Criminal Code established under Law Number 1 of 2023, which will come into full effect in 2026, does not explicitly regulate AI-based criminal offenses. AI misuse must instead be constructed using conventional offenses, such as fraud under Article 378 of the old Criminal Code, which is reformulated in Article 492 of the National Criminal Code, forgery of letters or electronic documents under Articles 263–264 of the old Criminal Code, and defamation under Articles 310–311 of the old Criminal Code. Dogmatically, this forced interpretation approach faces difficulties because the objective and subjective elements of these offenses were designed for human conduct, not for situations where AI systems contribute autonomously to the consequences of a legal event. The aspect of *mens rea* (guilty mind) becomes problematic when the perpetrator merely initiates the system, while the specific harmful content is generated through automated processing.¹⁹ Without the reformulation of offenses or the recognition of technological risk parameters, general criminal law tends to lag behind and is only capable of addressing cases where the element of human intent is very clear.

The enactment of Law Number 27 of 2022 concerning Personal Data Protection and the revision of the Law on Information and Electronic Transactions demonstrates the dominance of state interests and the digital industry within the digital economy. While the Personal Data Protection Law adopts global data protection principles, this has not yet been followed by the establishment of a strong independent supervisory authority.²⁰ This results in the Personal Data Protection Law ability to regulate AI-based data processing practices remaining limited. The revisions to the Information and Electronic Transactions Law are primarily aimed at addressing criticism of its loose provisions,²¹ rather than restructuring the legal framework to address the emergence of AI misuse. This pattern aligns with the characteristics of a reactive-incidental legal policy, where regulations are enacted in response to specific incidents and public pressure, rather than being the result of long-term legal planning.

¹⁹ Thuy Dung Le and Nicola Döring, “Perspectives on Non-Consensual Deepfake Pornography: A Content Analysis of Reddit Discussions Initiated by Perpetrators, Victims, and Bystanders,” *Sexuality & Culture*, March 4, 2026, 1–25, <https://doi.org/10.1007/s12119-026-10566-x>.

²⁰ Dhea Cantik and Adhining Prabawati Rahmahani, “The Urgency of Establishing a Supervisory Agency for the Implementation of Personal Data Protection in the Implementation of the Personal Data Protection Law,” *International Journal of Science and Environment (IJSE)* 6, no. 1 (2026): 300–308, <https://doi.org/10.51601/ijse.v6i1.332>.

²¹ Afisa Afisa et al., “Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia,” *The Journal of Society and Media* 8, no. 2 (2024): 424–44, <https://doi.org/10.26740/jsm.v8n2.p424-444>.

As the *lex specialis* for cyberspace, Law Number 1 of 2024 concerning the Second Amendment to the Information and Electronic Transactions Law also fails to incorporate specific norms related to AI. Article 27 regulates the distribution of prohibited content, Article 28 addresses the dissemination of false and misleading information, and Article 30 governs illegal access to electronic systems; however, none of these provisions define or refer to AI systems. In practice, law enforcement agencies apply these articles to cases of digital fraud and defamation involving AI. Nevertheless, the absence of a definition for AI and specific standards of proof for AI-generated content results in inconsistent application and creates significant room for varying interpretations.

Law Number 27 of 2022 concerning Personal Data Protection holds significant potential for AI regulation. Article 22 stipulates that any automated processing of personal data producing legal effects or significantly impacting the data subject must be based on explicit consent and principles of lawful processing. Article 23 grants data subjects the right to object to decisions based solely on automated processing. Although the concept of automated decision-making is inherently relevant to AI usage, the lack of authoritative clarification on whether and to what extent specific AI systems qualify as "automated decision-making systems" under the Personal Data Protection Law prevents this norm from functioning optimally as a control mechanism against misuse. Furthermore, the absence of an independent data supervisory authority reduces the effectiveness of enforcing these norms in practice.

The dimension of legal policy is evident in the deepfake advertisement case involving Dr. Tony Setiobudi. In this case, Dr. Tony's likeness and voice were used without permission in a deepfake video to promote a diabetes medication called "Glucoformin". The video spread widely on social media and unofficial websites, misleading the public and triggering complaints from consumers who felt deceived as the product did not match the claims made.²² His legal team reported the incident to the East Java Regional Police using Article 35 in conjunction with Article 27A of Law Number 1 of 2024 concerning the Second Amendment to

²² Tony Hermawan, "Dokter Spesialis Ortopedi Hingga Para Perempuan Menjadi Korban Deepfake Video Maupun Foto," February 21, 2026, https://surabaya.tribunnews.com/jawa-timur/1931843/dokter-spesialis-ortopedi-hingga-para-perempuan-menjadi-korban-deepfake-video-maupun-foto#google_vignette.

the Information and Electronic Transactions Law. The use of the Information and Electronic Transactions Law as a "general framework" indicates that the regulatory configuration for AI misuse in Indonesia still relies on conventional cyber norms, without specific provisions regarding deepfakes, facial biometric data, or the liability of algorithm developers and distribution platforms. Consequently, legal resolution heavily depends on how law enforcement officials construct and interpret existing provisions.

From the perspective of legal policy, the Dr. Tony case illustrates a paradox between highly advanced technological penetration and a legal architecture that still views AI merely as a tool and an object of law.²³ Liability is focused on the human actors who distribute or create the content, while structural factors such as the design of deepfake systems, platform business models that drive content virality, and the absence of algorithmic transparency standards remain untouched by the positive legal framework. Facial features and voices, as biometric data used to generate deepfakes, should technically fall under the category of special personal data requiring stricter protection under the Personal Data Protection Law. This reinforces the argument that Indonesia's legal policy still operates within an *ex post* logic of addressing consequences, rather than employing an *ex ante* regulatory design that governs obligations for transparency, risk assessment, and oversight mechanisms for high-risk AI systems.

In contrast to Indonesia, the Netherlands' AI legal policy is built upon the *rechtsstaat* tradition, which emphasizes the rule of law and the protection of fundamental rights as the primary boundaries for technological innovation.²⁴ Constitutionally, the Dutch Constitution (*Grondwet*) provides a strong foundation through Article 1 regarding the prohibition of discrimination and Article 10 concerning the protection of privacy. Beyond the national constitution, the Netherlands is also bound by the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union, which reinforce the

²³ Dyah Permata Budi Asri, Irmanjaya Thaher, and Riya Widayanti, "Artificial Intelligence, Legal Culture, and the Indonesian Formal Legal System: Negotiating Norms in The Regulation of Emerging Technologies," *Journal of Cultural Analysis and Social Change* 10, no. 3 (2025): 457–68, <https://doi.org/10.64753/jcasc.v10i3.2439>.

²⁴ Stéphanie Laulhé Shaelou and Yulia Razmetaeva, "Challenges to Fundamental Human Rights in the Age of Artificial Intelligence Systems: Shaping the Digital Legal Order While Upholding Rule of Law Principles and European Values," *ERA Forum* 24, no. 4 (2023): 567–87, <https://doi.org/10.1007/s12027-023-00777-2>.

state's obligation to safeguard individual rights against technological intervention.²⁵ Accordingly, the Netherlands' legal policy is more rights-based rather than developmentalist. This approach aligns with the paradigm of human-centric AI governance, which upholds human dignity as an absolute principle.²⁶ Within this paradigm, AI is considered legitimate as long as it does not violate human rights or create systemic discrimination. Consequently, the Netherlands has been quicker to establish oversight and accountability systems for AI usage, particularly in the public sector.

A distinctive feature of Dutch legal policy is its multi-level governance system, whereby AI regulation is determined not only by national law but also by the supranational framework of the European Union. The Netherlands is directly bound by EU regulations which apply *erga omnes*,²⁷ In particular, the EU AI Act (Regulation EU 2024/1689). The EU AI Act adopts a risk-based approach by categorizing AI systems into unacceptable risk (totally prohibited), high risk (permitted with strict obligations), limited risk, and minimal risk,²⁸ and regulate obligations such as risk management, data governance, technical documentation, transparency, and human oversight.²⁹ Article 14 of the EU AI Act stipulates that high-risk AI systems must be designed and operated in such a way that they are subject to effective human oversight, with the aim of preventing or minimizing risks to health, safety, or fundamental rights. Consequently, AI misuse in the Netherlands is viewed not only as an unlawful act but also as a failure to comply with risk management obligations.

Dutch legal policy regarding algorithmic accountability is reflected in the initiative to establish an Algorithm Register. Since 2022, the Dutch government has been developing a public register containing information on algorithms and AI systems used by government

²⁵ Douwe Korff, "First Do No Harm: The Potential of Harm Being Caused to Fundamental Rights and Freedoms by State Cybersecurity Interventions," in *Research Handbook on Human Rights and Digital Technology* (Cheltenham: Edward Elgar Publishing, 2025), 126–65, <https://doi.org/10.4337/9781035308514.00015>.

²⁶ Anton Sigfrids et al., "Human-Centricity in AI Governance: A Systemic Approach," *Frontiers in Artificial Intelligence* 6 (2023): 1–9, <https://doi.org/10.3389/frai.2023.976887>.

²⁷ CL Lim and Ryan Martínez Mitchell, "Neutral Rights And Collective Countermeasures For Erga Omnes Violations," *International and Comparative Law Quarterly* 72, no. 2 (2023): 361–91, <https://doi.org/10.1017/S0020589323000076>.

²⁸ Johanna Chamberlain, "The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective," *European Journal of Risk Regulation* 14, no. 1 (2023): 1–13, <https://doi.org/10.1017/err.2022.38>.

²⁹ 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 (2024), <https://doi.org/10.1093/ijlit/eaee011>.

agencies in decision-making processes that affect citizens.³⁰ This register requires agencies to explain the purpose, legal basis, type of data used, and the underlying logic of the system, thereby creating space for public oversight and democratic control over the state's use of AI.³¹ The choice to prioritize algorithmic transparency over bureaucratic efficiency reflects a legal policy that places public accountability as the core value of AI governance. This differs from Indonesia, which lacks similar algorithmic transparency mechanisms, both at the regulatory level and in institutional practice.

Jurisprudence in the Netherlands also plays a significant role in shaping AI legal policy. In the case of *Stichting Syri v. Staat der Nederlanden* (The Hague District Court, 2020), the court ruled that the use of the System Risk Indication (SyRI) violated Article 8 of the ECHR regarding the right to privacy, as it failed to meet the principles of necessity and proportionality and carried the potential to cause discrimination.³² This ruling orders a halt to the use of Syri and sets an important precedent that state use of AI must be subject to strict European human rights standards.³³ The courts act as a corrective force, ensuring that government AI innovation remains within the boundaries of fundamental rights, rather than being subject solely to considerations of fiscal efficiency or social control.

The regulatory framework concerning AI misuse in the Netherlands is shaped by the interaction of the EU AI Act, the GDPR, and national criminal law. The General Data Protection Regulation (GDPR) serves as the foundation for privacy regulation, with Article 22 prohibiting decision-making based solely on automated processing that produces legal effects or similarly significant effects concerning the individual. Additionally, Articles 13 and 14 require controllers to provide clear information regarding the use of automated processing. The GDPR also mandates a Data Protection Impact Assessment (DPIA) for high-risk processing, thereby

³⁰ Diana Mariana Popa, "Frontrunner Model for Responsible AI Governance in the Public Sector: The Dutch Perspective," *AI and Ethics* 5, no. 3 (2025): 2789–99, <https://doi.org/10.1007/s43681-024-00596-2>.

³¹ Esther Nieuwenhuizen, "Algorithm Registers: A Box-Ticking Exercise or Meaningful Tool for Transparency?," *Information Polity* 29, no. 4 (2024): 415–33, <https://doi.org/10.1177/15701255241297107>.

³² Rachovitsa and Johann, "The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case."

³³ Chippy Abraham, "Automated Justice and the Performance of Law: Kafka's The Trial in the Age of Algorithmic Governance," *Law, Culture and the Humanities*, July 7, 2025, <https://doi.org/10.1177/17438721251351015>.

necessitating risk evaluation and mitigation measures prior to system deployment.³⁴ On the other hand, the Dutch Criminal Code (Wetboek van Strafrecht) provides the basis for prosecution regarding fraud (oplichting, Article 326), defamation (smaad and laster, Articles 261–262), and computer offenses reformulated through the Wet Computercriminaliteit III to address phenomena such as deepfakes and digital manipulation. This combination equips the Netherlands with a set of instruments that are more adaptive to AI misuse compared to Indonesia's regulatory structure.

The existence of the Autoriteit Persoonsgegevens (AP) as an independent data and AI supervisory authority is a key distinguishing element between the regulatory configurations of the Netherlands and Indonesia. The AP has the authority to conduct investigations, impose substantial administrative fines of up to 4% of annual global turnover, issue binding decisions, and publish interpretative guidelines regarding the use of AI and algorithms.³⁵ The AP is also involved in coordinating algorithmic oversight across sectors through mechanisms such as the AI & Algorithmic Risks Report, which maps the risks of AI use in the public and private sectors.³⁶ With such an institutional design, Dutch AI legal policy is not merely present in normative texts but is also manifested in continuous enforcement and oversight practices.

The comparison between Indonesia and the Netherlands reveals that differences in regulatory configuration are not merely technical but result from distinct legal policy choices. Indonesia tends to adopt a development-first model that prioritizes digital economic growth, whereas the Netherlands implements a rights-first model that establishes protection as a prerequisite for innovation. This difference can be understood as a tension between the paradigm of innovation-friendly regulation and that of rights-based governance. Consequently, Indonesia produces regulations that are more reactive and sectoral, while the Netherlands develops a multi-layered and integrated framework. These variations are also influenced by institutional capacity, as the Netherlands possesses a strong independent

³⁴ Arzu Galandarli, "Mitigating AI Risks: A Comparative Analysis of Data Protection Impact Assessments under GDPR and KVKK," *Journal of Data Protection & Privacy* 7, no. 3 (2025): 252–73, <https://doi.org/10.69554/ATTT2755>.

³⁵ Maranke Wieringa, "Hey SyRI, Tell Me about Algorithmic Accountability: Lessons from a Landmark Case," *Data & Policy* 5 (2023): 1–24, <https://doi.org/10.1017/dap.2022.39>.

³⁶ Haitsma, "Addressing Discrimination in Algorithmic Profiling: Examining Risk Governance in Dutch Public Social Security Agencies."

supervisory authority, whereas Indonesia still faces institutional weaknesses. From a legal policy perspective, regulatory fragmentation in Indonesia indicates a lack of political will to establish a coherent *lex specialis* for AI. Conversely, regulatory coherence in the Netherlands demonstrates a clear and consistent legal policy commitment to safeguarding citizens' rights. Thus, this comparison confirms that the success of AI regulation is highly dependent on the design of legal policy and the capacity of the institutions that support it.

B. A Regulatory Reform Model for Indonesia to Address the Normative Void on AI Abuse

The paradigm for reforming artificial intelligence regulation in Indonesia demands a fundamental shift from a reactive model to a responsive-anticipatory model. Historically, Indonesia has tended to apply a reactive regulatory approach, addressing AI misuse only after incidents occur using legal instruments that were not originally designed for such phenomena. This pattern is evident in the reliance on the Information and Electronic Transactions Law, the Criminal Code, and sectoral regulations, which are only capable of addressing the consequences rather than controlling the source of risks. Given the rising number of AI misuse cases, the reactive model is not only inadequate but also risks deepening the public's crisis of confidence in the law. Therefore, AI regulatory reform must transition toward a responsive-anticipatory framework capable of preventing harm before it escalates.

Responsive Law theory by Nonet and Selznick classifies legal development into three types: repressive law, autonomous law, and responsive law.³⁷ Repressive law serves the interests of power, autonomous law emphasizes formal certainty, while responsive law is the most mature form because it is able to adapt to social needs without losing its normative integrity.³⁸ In the context of AI, responsive law requires regulations that are adaptive to technological changes while remaining committed to protecting human rights. Indonesia's current condition reflects a tendency toward autonomous law, which enforces existing formal norms but fails to effectively address the reality of AI misuse. Consequently, the state often acts too late, with

³⁷ Agam Ibnu Asa, Misnal Munir, and Rr. Siti Murti Ningsih, "Nonet And Selznick's Responsive Law Concept In A Historical Philosophy Perspective," *CREPIDO* 3, no. 2 (2021): 96–109, <https://doi.org/10.14710/crepido.3.2.96-109>.

³⁸ Ahmad Faiz Shobir Alfikri and Maziya Rahma Wahda, "Compilation of Islamic Law: The Face of Responsive Legal Products as the Accommodative Politics of the New Order Government," *Recht Studiosum Law Review* 4, no. 1 (2025): 1–11, <https://doi.org/10.32734/rslr.v4i1.18591>.

victims already suffering reputational or financial damage before the law intervenes. The responsive law model urges the state to establish preventive frameworks and control mechanisms from the early stages of technology deployment.

The Dutch experience underscores that effective AI regulation cannot be built merely by incrementally expanding interpretations of conventional legal instruments. The Netherlands demonstrates that controlling AI misuse stems from systemic coherence – the integration of the EU AI Act, the GDPR, algorithmic transparency mechanisms, and strong institutional oversight. This systemic coherence transforms AI regulation from a collection of fragmented rules into a complete architecture that maps risks, defines obligations, and provides clear enforcement pathways. Such an ecosystem reveals that the strength of AI regulation lies in a mutually supportive, multi-layered design.

The proposed multi-layered model for reforming artificial intelligence regulation in Indonesia is structured into three levels: the substantive legal layer (specific AI legislation), the institutional layer (independent supervisory authority), and the procedural layer (adaptive enforcement mechanisms). The first layer focuses on enacting a National Artificial Intelligence Law (NAI Law) as a *lex specialis* to fill the substantive normative gap. The second layer improves the institutional structure by establishing an independent National AI Supervisory Body with strong regulatory and oversight mandates. The third layer reforms procedural law and standards of proof to align with the characteristics of digital evidence and AI-based crime *modus operandi*. All three layers must operate simultaneously, as the failure of one will weaken the entire system. Therefore, this reform model is systemic and cannot be reduced to mere sectoral changes. This three-layer architecture also aligns with Indonesia's need to close normative gaps while building implementation capacity.

The first layer of reform requires the establishment of the NAI Law as a specific law governing AI systems comprehensively. The unique and complex nature of AI – involving anonymity, cross-jurisdictional reach, semi-autonomy, and rapid impact – cannot be optimally addressed by general norms such as the Criminal Code or the Information and Electronic Transactions Law. Enacting the NAI Law also fulfills the need to provide legal certainty for

businesses and technology users. Without a *lex specialis*, law enforcement officials will continue to force interpretations of traditional provisions, risking violations of the legality principle and leading to inconsistent rulings. Furthermore, the NAI Law can serve as an umbrella framework integrating sectoral regulations to prevent normative fragmentation.

The design of the NAI Law should incorporate the principles of Better Regulation developed by the European Union, which can be adapted to prevent the creation of regulations that are normatively strong but weak in implementation.³⁹ The principle of proportionality requires that the regulatory burden be proportionate to the level of risk,⁴⁰ ensuring that low-risk AI systems are not burdened with unnecessary heavy obligations, while high-risk systems are subject to strict regulation. The principle of transparency requires that the process of formulating and implementing AI regulations is open, supervisable, and inclusive of diverse stakeholders,⁴¹ not limited to the technology industry. Coherence requires that the NAI Law aligns with the Personal Data Protection Law, the Information and Electronic Transactions Law, the Criminal Code, and sectoral regulations to avoid conflicts or new normative gaps. The principle of effectiveness demands that the established norms can be practically enforced by institutions with adequate resources and authority.

The first essential substantive element to be included in the NAI Law is the establishment of precise and operational legal definitions regarding AI systems and their types of misuse. These definitions are not merely technical terminology but legal prerequisites to ensure legal certainty and uphold the principle of legality. In criminal law, the maxim *nullum crimen, nulla poena sine lege* requires clear formulations of offenses to prevent criminalization through broad interpretations. The lack of clear definitions has thus far made it difficult for law enforcement officials to classify specific acts as AI misuse, leading to inconsistent application of the law. From the perspective of Gustav Radbruch, clear definitions are a necessary condition

³⁹ Claire A. Dunlop and Claudio M. Radaelli, "Better Regulation in the European Union," in *Innovation and Regulatory Agencies* (Cheltenham: Edward Elgar Publishing, 2022), 303–13, <https://doi.org/10.4337/9781839108990.00031>.

⁴⁰ Martin Ebers, "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act," *European Journal of Risk Regulation* 16, no. 2 (2025): 684–703, <https://doi.org/10.1017/err.2024.78>.

⁴¹ Brady Lund et al., "Standards, Frameworks, and Legislation for Artificial Intelligence (AI) Transparency," *AI and Ethics* 5, no. 4 (2025): 3639–55, <https://doi.org/10.1007/s43681-025-00661-4>.

for realizing legal certainty (rechtssicherheit), which stands as one of the three fundamental values of law, alongside usefulness (zweckmäßigkeit) and justice (gerechtigkeit).⁴²

The next element is the adoption of a risk-based approach to AI regulation. Guided by the EU AI Act, AI systems are classified into four risk levels: unacceptable, high, limited, and minimal risk, with proportionate legal obligations applicable to each category.⁴³ For Indonesia, a similar framework can be adapted by categorizing risks as follows: first, unacceptable risk, which must be completely prohibited; second, high risk, which mandates strict risk management standards, audits, and human oversight for AI used in law enforcement, finance, healthcare, and essential public services; third, limited risk, which imposes transparency obligations, such as the requirement to disclose that users are interacting with an AI system; and fourth, minimal risk, which is sufficiently governed by ethical guidelines. This classification creates space for innovation in low-risk AI applications while providing maximum protection against systems that potentially threaten fundamental rights. Practically, this scheme implements Jeremy Bentham's idea of legal utility, which seeks to balance the benefits of AI innovation against potential harms by allocating regulatory intervention proportional to the level of risk.⁴⁴

In addition to risk classification, the NAI Law must establish a clear legal liability regime to prevent structural impunity. This regime defines the chain of responsibility between AI developers, system operators or providers, and end users. Developers are responsible for aspects of design, security, and the mandatory disclosure of system limitations,⁴⁵ while the operator is responsible for compliance with the use and human supervision of the system being

⁴² Ahmad Zumar Syafiq and Suparno, "Implementation of the Principles of Legal Certainty and the Principles of Justice towards Tax Amnesty II Policy on Voluntary Tax Disclosure," *Journal of Law, Politic and Humanities* 5, no. 2 (2025): 1328–38, <https://doi.org/10.38035/jlph.v5i2.1309>.

⁴³ Henry Fraser and José-Miguel Bello y Villarino, "Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough," *European Journal of Risk Regulation* 15, no. 2 (2024): 431–46, <https://doi.org/10.1017/err.2023.57>.

⁴⁴ Hysmir Idrizi, *Artificial Intelligence in Legal Systems*, ed. Eriona Çela, Narasimha Rao Vajjhala, and Behrouz Aslani (Boca Raton: Chapman and Hall/CRC, 2025), <https://doi.org/10.1201/9781003541899>.

⁴⁵ Conrad Sanderson et al., "AI Ethics Principles in Practice: Perspectives of Designers and Developers," *IEEE Transactions on Technology and Society* 4, no. 2 (2023): 171–87, <https://doi.org/10.1109/TTS.2023.3257303>.

operated.⁴⁶ Users are responsible for using AI for permitted purposes, including the prohibition of use for fraud or identity manipulation.⁴⁷ For high-risk AI systems, the principle of strict liability should be considered to avoid placing the burden of proof on the victim. This principle aligns with the theory of risk (*risico aansprakelijkheid*), which states that the party who creates exceptional risks to society through technology under their control must bear the consequences of any resulting harm. This regime should also be supplemented by compensation mechanisms for victims and administrative sanctions against corporate actors to ensure a deterrent effect.

Another essential element is the binding obligation of transparency and explainability for AI systems that interact directly with the public. The NAI Law must mandate the disclosure that users are interacting with an AI system, as well as the requirement to provide comprehensible explanations when automated decisions have a significant impact on individuals.⁴⁸ This obligation is in line with the right to information under Article 28F of the 1945 Constitution of the Republic of Indonesia, which states that "Every person has the right to communicate and obtain information...". Without transparency, individuals cannot demand corrections or object to decisions made by AI that are detrimental to them. Furthermore, the obligation to label AI-generated content, such as through digital watermarking, must be implemented to curb the spread of deepfakes.⁴⁹ This mechanism serves as an *ex ante* preventive measure, enabling the public to distinguish between authentic and synthetic content before harm occurs. Transparency through the obligation of explainability is a minimum requirement to ensure that AI systems do not operate as "black boxes".⁵⁰

The reform must also incorporate specific criminal provisions that explicitly criminalize forms of AI misuse. Special criminal regulations are necessary to end the reliance on the

⁴⁶ Ahmed Oudah Mohammed Al-Dulaimi and Mohammed Abd-Al Wahab Mohammed, "Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector," *International Journal of Law and Management*, March 5, 2025, <https://doi.org/10.1108/IJLMA-08-2024-0295>.

⁴⁷ Kamrul Faisal, "Controller Responsibilities in AI-Driven Processing of Vulnerable Data Subjects: A Legal Framework for Risk Mitigation, Proportionality, and Compliance," *AI and Ethics* 6, no. 1 (2026): 92, <https://doi.org/10.1007/s43681-025-00899-y>.

⁴⁸ Ronan Hamon et al., "Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making," *IEEE Computational Intelligence Magazine* 17, no. 1 (2022): 72–85, <https://doi.org/10.1109/MCI.2021.3129960>.

⁴⁹ David Ghiurău and Daniela Elena Popescu, "Distinguishing Reality from AI: Approaches for Detecting Synthetic Content," *Computers* 14, no. 1 (2024): 1–33, <https://doi.org/10.3390/computers14010001>.

⁵⁰ Nipuna Thalpage, "Unlocking the Black Box: Explainable Artificial Intelligence (XAI) for Trust and Transparency in AI Systems," *Journal of Digital Art & Humanities* 4, no. 1 (2023): 31–36, https://doi.org/10.33847/2712-8148.4.1_4.

construction of conventional offenses, which are often incompatible with the characteristics of AI. These specific offenses should include the creation and distribution of deepfakes with malicious intent, the use of AI for identity manipulation, AI-based financial fraud utilizing voice cloning, and the dissemination of AI-driven disinformation that affects public interests. Criminal formulations must address the element of *mens rea* (guilty mind) in a manner adapted to the semi-autonomous nature of AI systems. For instance, configuring or designing an AI system to cause harm should be regarded as equivalent to direct intent (*dolus directus*).⁵¹ Without such provisions, perpetrators could argue that the harm resulted from a "system error" rather than human malice. Therefore, specific criminal provisions serve to broaden criminalization and clarify the liability structure in AI-based crimes.

The second layer of reform is the establishment of the National Artificial Intelligence Supervisory Board (NAISB) as an independent body responsible for overseeing the implementation of the NAI Law. This initiative draws from the Dutch experience, which demonstrates that AI regulation is only effective when supported by a strong authority such as the Autoriteit Persoonsgegevens. In legal institutionalism theory, norms cannot be separated from the institutions that enforce them, interpret them, and develop technical standards.⁵² Structurally, the NAISB needs to be established as a state auxiliary body that does not fall under the jurisdiction of any ministry, particularly not under the ministry responsible for promoting the digital economy, in order to safeguard supervisory independence. The independence of the NAISB is not merely an organizational design choice but a constitutional prerequisite for upholding the rule of law, which demands a clear separation between the state's interest as a promoter of innovation and its role as the protector of its citizens.⁵³ Furthermore, the NAISB must be granted normative authority to issue binding guidelines, investigative powers to conduct audits and access AI system data, as well as adjudicative authority to impose

⁵¹ Daniele Amoroso and Benedetta Giordano, "Who Is to Blame for Autonomous Weapons Systems' Misdoings?," in *Use and Misuse of New Technologies*, ed. Elena Carpanelli and Nicole Lazzerini (Cham: Springer International Publishing, 2019), 211–32, https://doi.org/10.1007/978-3-030-05648-3_11.

⁵² Henrique A Castro, "Institutions Are Not Rules: Realigning the Ontology Behind Theories of Change," *Political Studies* 72, no. 4 (2024): 1512–33, <https://doi.org/10.1177/00323217231179551>.

⁵³ Laurent Pech, "The Rule of Law as a Well-Established and Well-Defined Principle of EU Law," *Hague Journal on the Rule of Law* 14, no. 2–3 (2022): 107–38, <https://doi.org/10.1007/s40803-022-00176-8>.

administrative sanctions. The sanction model can adopt the GDPR framework, which allows fines based on a percentage of global revenue as an effective deterrent instrument.

The third layer of reform involves procedural strengthening through the revision of procedural law and evidence standards capable of accommodating AI-based digital evidence. One of the biggest obstacles in enforcing laws against AI misuse is the difficulty of proving the authenticity of synthetic content and tracing the digital evidence chain involving cross-border servers. Specific standards of proof are required that recognize the role of AI forensic experts as crucial evidence providers. Additionally, a digital chain of custody protocol is necessary to guarantee the integrity of evidence throughout the handling process.⁵⁴ Procedural strengthening must also include training for law enforcement officials to enable them to technically identify patterns of AI misuse. Lawrence Friedman's legal system theory posits that the effectiveness of law is determined by legal substance, legal structure, and legal culture.⁵⁵ The NAI Law reforms the legal substance, the NAISB reforms the institutional structure, while procedural updates and capacity building strengthen legal culture. Without procedural reform, even strong substantive norms and supervisory institutions will lose their effectiveness due to difficulties in proving cases and limited enforcement capacity.

Beyond procedural reforms, a rapid response mechanism specifically for deepfakes must be designed, given their nature of extremely fast and massive dissemination. Conventional criminal proceedings are often time-consuming, meaning victims may already suffer severe reputational and financial damage before a verdict is reached. Therefore, the NAISB needs the authority to issue interim takedown orders within 24–48 hours after a report is verified. This mechanism represents a form of preventive administrative law aimed at halting ongoing harm. It also aligns with the principles of responsive law, which emphasize the need for quick and adaptive protection of the public.⁵⁶ However, this authority must be accompanied by control

⁵⁴ Tommaso D'Anna et al., "The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data," *Healthcare* 11, no. 5 (2023): 634, <https://doi.org/10.3390/healthcare11050634>.

⁵⁵ Henny Saida Flora, Mac Thi Hoai Thuong, and Ratna Deliana Erawati, "The Orientation and Implications of New Criminal Code: An Analysis of Lawrence Friedman's Legal System," *Jurnal IUS Kajian Hukum Dan Keadilan* 11, no. 1 (2023): 113–25, <https://doi.org/10.29303/ius.v11i1.1169>.

⁵⁶ Zhi Li and Wenxiang Zhang, "Technology in Education: Addressing Legal and Governance Challenges in the Digital Era," *Education and Information Technologies* 30, no. 7 (2025): 8413–43, <https://doi.org/10.1007/s10639-024-13036-9>.

procedures to prevent its misuse in arbitrarily restricting freedom of expression. Therefore, the design must include verification standards, time limits, and mechanisms for objections or appeals. Consequently, the rapid response mechanism for deepfakes serves as a vital instrument to bridge the gap between the speed of technology and the slowness of legal processes.

The NAI Law must also incorporate built-in adaptability mechanisms to prevent regulatory obsolescence. AI regulation faces unique challenges because technology evolves extremely rapidly; consequently, non-adaptive rules risk becoming irrelevant in a short time. Adaptability can be achieved through mandatory periodic reviews for example, every two years—to update definitions and risk classifications. Additionally, regulatory sandboxes should be established to allow AI innovation to be tested in a controlled environment without compromising public protection.⁵⁷ The NAI Law must also delegate technical authority to the NAISB to establish AI technical standards that can be updated without requiring amendments to the law. This mechanism aligns with the concept of responsive regulation by Ayres and Braithwaite, which emphasizes regulatory flexibility to adapt to changing conditions.⁵⁸ Therefore, adaptability is not merely a design choice but a necessary condition for AI regulation to remain effective in the face of technological evolution.

The overarching principle guiding all reforms must be human-centric AI governance, which upholds human dignity and fundamental rights as absolute boundaries for technological innovation. The Dutch experience, as seen in the ruling of *Stichting SyRI v. Staat der Nederlanden* (2020), demonstrates that government use of AI can be halted if it violates the right to privacy as guaranteed by Article 8 of the ECHR. This ruling confirms that state efficiency cannot justify sacrificing citizens' fundamental rights through opaque algorithmic profiling. This principle strongly resonates with Article 28G paragraph (1) of the 1945 Constitution regarding the protection of personal life and human dignity. Consequently,

⁵⁷ Jon Truby et al., “A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications,” *European Journal of Risk Regulation* 13, no. 2 (2022): 270–94, <https://doi.org/10.1017/err.2021.52>.

⁵⁸ Jeroen van der Heijden, “Responsive Regulation in the Context of Environmental Regulation,” in *Research Handbook on Environmental Regulation* (Cheltenham: Edward Elgar Publishing, 2026), 51–62, <https://doi.org/10.4337/9781789903362.00010>.

human-centric governance is not the transplantation of foreign values, but rather the implementation of Indonesia's existing constitutional values. Furthermore, reforms must be designed to be interoperable with international standards such as the OECD AI Principles and the UNESCO Recommendation on the Ethics of AI, ensuring that Indonesia remains integrated within the global governance framework.

CONCLUSION

This study demonstrates that the principal difference between Indonesia and the Netherlands in addressing AI misuse lies not simply in the existence or absence of AI-specific regulation, but in the configuration and interaction of substantive rules, institutional oversight, and enforcement mechanisms. Indonesia possesses a strong constitutional basis for protecting privacy, dignity, equality, and legal certainty, yet its regulatory response to AI misuse remains predominantly fragmented and reactive, relying on general and sectoral legislation. By contrast, the Netherlands operates within a multi-level regulatory architecture combining the EU AI Act, the GDPR, national legal instruments, algorithmic transparency mechanisms, and institutional oversight. The comparison therefore indicates that regulatory effectiveness is closely associated with the coherence between legal norms, institutional capacity, and enforceable procedural mechanisms. The central contribution of this study is the Three-Tier Regulatory Architecture proposed for Indonesia. The model conceptualises AI regulatory reform as an integrated system consisting of (1) a substantive layer, (2) an institutional layer, and (3) a procedural layer. The substantive layer requires an AI-specific legal framework capable of establishing clear definitions, risk classification, liability allocation, transparency obligations, and human-oversight requirements. The institutional layer requires an independent or appropriately designated supervisory authority with clearly defined jurisdiction, audit and investigation powers, and coordination mechanisms with existing sectoral regulators. The procedural layer requires AI-sensitive enforcement mechanisms, including standards for evaluating AI-generated evidence, strengthened digital-forensic capabilities, and rapid protective measures for serious AI-related harms. The comparative lesson from the Netherlands should not be understood as a recommendation to transplant

European regulation into Indonesia. Rather, relevant regulatory practices should be selectively adapted to Indonesia's constitutional values, institutional structure, and socio-legal conditions. The principal policy implication is therefore a shift from predominantly ex post and incident-driven regulation toward a responsive and anticipatory governance model in which regulatory intervention is proportionate to technological risk while preserving innovation, legal certainty, and fundamental rights. This study is subject to a limitation inherent in its normative-comparative design: it primarily evaluates legal norms, institutional arrangements, and jurisprudential materials and does not empirically measure the effectiveness of AI enforcement in either jurisdiction. Future research should therefore examine the implementation of the proposed architecture through empirical studies of regulatory institutions, judicial practice, platform liability, AI-generated evidence, and victim compensation mechanisms. Such research would provide an empirical basis for assessing whether the proposed three-tier architecture can translate normative reform into effective protection against AI misuse.

REFERENCES

- Abdullah, Muhammad, Muhammad Munib Nawaz, Bilal Saleem, Maila Zahra, Effa binte Ashfaq, and Zia Muhammad. "Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data." *Analytics* 4, no. 3 (2025): 25. <https://doi.org/10.3390/analytics4030025>.
- Abraham, Chippy. "Automated Justice and the Performance of Law: Kafka's The Trial in the Age of Algorithmic Governance." *Law, Culture and the Humanities*, July 7, 2025. <https://doi.org/10.1177/17438721251351015>.
- Afisa, Afisa, Zuly Qodir, Akhmad Habibullah, and Unggul Sugiharto. "Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia." *The Journal of Society and Media* 8, no. 2 (2024): 424–44. <https://doi.org/10.26740/jsm.v8n2.p424-444>.
- Ahmad Zumar Syafiq, and Suparno. "Implementation of the Principles of Legal Certainty and the Principles of Justice towards Tax Amnesty II Policy on Voluntary Tax Disclosure." *Journal of Law, Politic and Humanities* 5, no. 2 (2025): 1328–38. <https://doi.org/10.38035/jlph.v5i2.1309>.
- Al-Dulaimi, Ahmed Oudah Mohammed, and Mohammed Abd-Al Wahab Mohammed. "Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector." *International Journal of Law and Management*, March 5, 2025. <https://doi.org/10.1108/IJLMA-08-2024-0295>.
- Alfikri, Ahmad Faiz Shobir, and Maziya Rahma Wahda. "Compilation of Islamic Law: The Face

of Responsive Legal Products as the Accommodative Politics of the New Order Government." *Recht Studiosum Law Review* 4, no. 1 (2025): 1-11. <https://doi.org/10.32734/rslr.v4i1.18591>.

Amoroso, Daniele, and Benedetta Giordano. "Who Is to Blame for Autonomous Weapons Systems' Misdoings?" In *Use and Misuse of New Technologies*, edited by Elena Carpanelli and Nicole Lazzerini, 211-32. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-05648-3_11.

Asa, Agam Ibnu, Misnal Munir, and Rr. Siti Murti Ningsih. "Nonet And Selznick's Responsive Law Concept In A Historical Philosophy Perspective." *CREPIDO* 3, no. 2 (2021): 96-109. <https://doi.org/10.14710/crepido.3.2.96-109>.

Asri, Dyah Permata Budi, Irmanjaya Thaher, and Riya Widayanti. "Artificial Intelligence, Legal Culture, and the Indonesian Formal Legal System: Negotiating Norms in The Regulation of Emerging Technologies." *Journal of Cultural Analysis and Social Change* 10, no. 3 (2025): 457-68. <https://doi.org/10.64753/jcasc.v10i3.2439>.

Balcerzak, Michał. "Implications of the United Nations Human Rights Standards for the Development of Artificial Intelligence." In *Artificial Intelligence and International Human Rights Law*, 6-24. Cheltenham: Edward Elgar Publishing, 2024. <https://doi.org/10.4337/9781035337934.00008>.

Barkāne, Irēna, Celia Fernández Aller, Evelynne A. Tauchnitz, Iva Ramuš Cvetkovič, Manja Skočir, and Aleš Završnik. "Integrating Ethical Principles and Human Rights Based Approach in the EU Artificial Intelligence Act and the Council of Europe Convention on Artificial Intelligence: Interplay of Ethics and Law in the AI Regulation Debate." *Journal of the University of Latvia. Law*, no. 19 (2025): 43-59. <https://doi.org/10.22364/jull.19.03>.

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 (2024). <https://doi.org/10.1093/ijlit/eaee011>.

Cantik, Dhea, and Adhining Prabawati Rahmahani. "The Urgency of Establishing a Supervisory Agency for the Implementation of Personal Data Protection in the Implementation of the Personal Data Protection Law." *International Journal of Science and Environment (IJSE)* 6, no. 1 (2026): 300-308. <https://doi.org/10.51601/ijse.v6i1.332>.

Castro, Henrique A. "Institutions Are Not Rules: Realigning the Ontology Behind Theories of Change." *Political Studies* 72, no. 4 (2024): 1512-33. <https://doi.org/10.1177/00323217231179551>.

Chamberlain, Johanna. "The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective." *European Journal of Risk Regulation* 14, no. 1 (2023): 1-13. <https://doi.org/10.1017/err.2022.38>.

D'Anna, Tommaso, Maria Puntarello, Giovanni Cannella, Giovanni Scalzo, Roberto Buscemi, Stefania Zerbo, and Antonina Argo. "The Chain of Custody in the Era of Modern

Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data." *Healthcare* 11, no. 5 (2023): 634. <https://doi.org/10.3390/healthcare11050634>.

Dunlop, Claire A., and Claudio M. Radaelli. "Better Regulation in the European Union." In *Innovation and Regulatory Agencies*, 303–13. Cheltenham: Edward Elgar Publishing, 2022. <https://doi.org/10.4337/9781839108990.00031>.

Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act." *European Journal of Risk Regulation* 16, no. 2 (2025): 684–703. <https://doi.org/10.1017/err.2024.78>.

Faisal, Kamrul. "Controller Responsibilities in AI-Driven Processing of Vulnerable Data Subjects: A Legal Framework for Risk Mitigation, Proportionality, and Compliance." *AI and Ethics* 6, no. 1 (2026): 92. <https://doi.org/10.1007/s43681-025-00899-y>.

Fikri, Abidin, and Tina Amelia. "Indonesia's Legal Policy on Protecting Personal Data from Artificial Intelligence Abuse." Edited by Y. Jusman, D. Mutiarin, A. Paksie, E. Saptutyningsih, S. Pau Loke, A. Khaliq, A.R. Ridzuan, and C.B. Tenorio. *SHS Web of Conferences* 204 (2024): 1–11. <https://doi.org/10.1051/shsconf/202420407002>.

Flora, Henny Saida, Mac Thi Hoai Thuong, and Ratna Deliana Erawati. "The Orientation and Implications of New Criminal Code: An Analysis of Lawrence Friedman's Legal System." *Jurnal IUS Kajian Hukum Dan Keadilan* 11, no. 1 (2023): 113–25. <https://doi.org/10.29303/ius.v11i1.1169>.

Flynn, Asher, Anastasia Powell, Asia Eaton, and Adrian J. Scott. "Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery." *Journal of Interpersonal Violence*, September 9, 2025, 1–35. <https://doi.org/10.1177/08862605251368834>.

Fraser, Henry, and José-Miguel Bello y Villarino. "Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough." *European Journal of Risk Regulation* 15, no. 2 (2024): 431–46. <https://doi.org/10.1017/err.2023.57>.

Galandarli, Arzu. "Mitigating AI Risks: A Comparative Analysis of Data Protection Impact Assessments under GDPR and KVKK." *Journal of Data Protection & Privacy* 7, no. 3 (2025): 252–73. <https://doi.org/10.69554/ATTT2755>.

Ghiurău, David, and Daniela Elena Popescu. "Distinguishing Reality from AI: Approaches for Detecting Synthetic Content." *Computers* 14, no. 1 (2024): 1–33. <https://doi.org/10.3390/computers14010001>.

Haitsma, Lucas M. "Addressing Discrimination in Algorithmic Profiling: Examining Risk Governance in Dutch Public Social Security Agencies." *European Journal of Social Security* 27, no. 2 (2025): 191–212. <https://doi.org/10.1177/13882627251351093>.

Hamon, Ronan, Henrik Junklewitz, Ignacio Sanchez, Gianclaudio Malgieri, and Paul De Hert.

- "Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making." *IEEE Computational Intelligence Magazine* 17, no. 1 (2022): 72–85. <https://doi.org/10.1109/MCI.2021.3129960>.
- Hasan, Zulfikar, and Diska Sendi Marisna. "Artificial Intelligence: Making Crime Easier in the World of Finance?" *AL-ARBAH: Journal of Islamic Finance and Banking* 6, no. 2 (2024): 223–56. <https://doi.org/10.21580/al-arbah.2024.6.2.22187>.
- Heijden, Jeroen van der. "Responsive Regulation in the Context of Environmental Regulation." In *Research Handbook on Environmental Regulation*, 51–62. Cheltenham: Edward Elgar Publishing, 2026. <https://doi.org/10.4337/9781789903362.00010>.
- Hermawan, Tony. "Dokter Spesialis Ortopedi Hingga Para Perempuan Menjadi Korban Deepfake Video Maupun Foto," February 21, 2026. https://surabaya.tribunnews.com/jawa-timur/1931843/dokter-spesialis-ortopedi-hingga-para-perempuan-menjadi-korban-deepfake-video-maupun-foto#google_vignette.
- Idrizi, Hysmir. *Artificial Intelligence in Legal Systems*. Edited by Eriona Çela, Narasimha Rao Vajjhala, and Behrouz Aslani. Boca Raton: Chapman and Hall/CRC, 2025. <https://doi.org/10.1201/9781003541899>.
- Joel Frenette. "Ensuring Human Oversight in High-Performance AI Systems: A Framework for Control and Accountability." *World Journal of Advanced Research and Reviews* 20, no. 2 (2023): 1507–16. <https://doi.org/10.30574/wjarr.2023.20.2.2194>.
- Korff, Douwe. "First Do No Harm: The Potential of Harm Being Caused to Fundamental Rights and Freedoms by State Cybersecurity Interventions." In *Research Handbook on Human Rights and Digital Technology*, 126–65. Cheltenham: Edward Elgar Publishing, 2025. <https://doi.org/10.4337/9781035308514.00015>.
- Le, Thuy Dung, and Nicola Döring. "Perspectives on Non-Consensual Deepfake Pornography: A Content Analysis of Reddit Discussions Initiated by Perpetrators, Victims, and Bystanders." *Sexuality & Culture*, March 4, 2026, 1–25. <https://doi.org/10.1007/s12119-026-10566-x>.
- Li, Zhi, and Wenxiang Zhang. "Technology in Education: Addressing Legal and Governance Challenges in the Digital Era." *Education and Information Technologies* 30, no. 7 (2025): 8413–43. <https://doi.org/10.1007/s10639-024-13036-9>.
- Lim, CL, and Ryan Martínez Mitchell. "Neutral Rights And Collective Countermeasures For Erga Omnes Violations." *International and Comparative Law Quarterly* 72, no. 2 (2023): 361–91. <https://doi.org/10.1017/S0020589323000076>.
- Lin, Leo S. F. "Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud." *Laws* 14, no. 4 (2025): 46. <https://doi.org/10.3390/laws14040046>.
- Lund, Brady, Zeynep Orhan, Nishith Reddy Mannuru, Ravi Varma Kumar Bevara, Brett

- Porter, Meka Kasi Vinaih, and Padmapadanand Bhaskara. "Standards, Frameworks, and Legislation for Artificial Intelligence (AI) Transparency." *AI and Ethics* 5, no. 4 (2025): 3639–55. <https://doi.org/10.1007/s43681-025-00661-4>.
- Maskanah, Umami. "Artificial Intelligence in Civil Justice: Comparative Legal Analysis and Practical Frameworks for Indonesia." *Jambura Law Review* 7, no. 1 (2025): 225–42. <https://doi.org/10.33756/jlr.v7i1.27786>.
- Mishra, Aman Kumar, Amit Kumar Tyagi, Sathian Dananjayan, Anand Rajavat, Hitesh Rawat, and Anjali Rawat. "Revolutionizing Government Operations." In *Conversational Artificial Intelligence*, edited by Romil Rawat, 607–34. Wiley, 2024. <https://doi.org/10.1002/9781394200801.ch34>.
- Mohieldin, Mahmoud, Maria Alejandra Gonzalez-Perez, and Mohamed Zahran. "The Double-Edged Sword: AI's Promise and Threat in Addressing Societal Challenges." In *AI-Powered Sustainable Business*, 19–40. Cham: Palgrave Macmillan, 2025. https://doi.org/10.1007/978-3-031-93357-8_2.
- Nieuwenhuizen, Esther. "Algorithm Registers: A Box-Ticking Exercise or Meaningful Tool for Transparency?" *Information Polity* 29, no. 4 (2024): 415–33. <https://doi.org/10.1177/15701255241297107>.
- Pech, Laurent. "The Rule of Law as a Well-Established and Well-Defined Principle of EU Law." *Hague Journal on the Rule of Law* 14, no. 2–3 (2022): 107–38. <https://doi.org/10.1007/s40803-022-00176-8>.
- Popa, Diana Mariana. "Frontrunner Model for Responsible AI Governance in the Public Sector: The Dutch Perspective." *AI and Ethics* 5, no. 3 (2025): 2789–99. <https://doi.org/10.1007/s43681-024-00596-2>.
- Rachovitsa, Adamantia, and Niclas Johann. "The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case." *Human Rights Law Review* 22, no. 2 (2022): 1–15. <https://doi.org/10.1093/hrlr/ngac010>.
- Rangone, Nicoletta, and Luca Megale. "Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making." *European Journal of Risk Regulation* 16, no. 3 (2025): 1082–97. <https://doi.org/10.1017/err.2025.13>.
- Revolusi, Prabu, and Radians Krisna Febriandy. "Developing AI Regulations in Indonesia: Policy Recommendations Based on Comparative Policy Analysis from the European Union, the United States, and Singapore." *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi* 6, no. 2 (2025): 1035–49. <https://doi.org/10.63447/jimik.v6i2.1380>.
- Sanderson, Conrad, David Douglas, Qinghua Lu, Emma Schleiger, Jon Whittle, Justine Lacey, Glenn Newnham, Stefan Hajkowicz, Cathy Robinson, and David Hansen. "AI Ethics Principles in Practice: Perspectives of Designers and Developers." *IEEE Transactions on Technology and Society* 4, no. 2 (2023): 171–87. <https://doi.org/10.1109/TTS.2023.3257303>.
- Sedeeq, Farman Saeed, and Percem Arman. "Human-Centric AI Governance: An Adaptive

Public International Law Framework for Ethical and Inclusive AI Regulation in Public Health." *Journal of Law, Medicine & Ethics* 53, no. 4 (2025): 563–74. <https://doi.org/10.1017/jme.2025.10175>.

Shaelou, Stéphanie Laulhé, and Yulia Razmetaeva. "Challenges to Fundamental Human Rights in the Age of Artificial Intelligence Systems: Shaping the Digital Legal Order While Upholding Rule of Law Principles and European Values." *ERA Forum* 24, no. 4 (2023): 567–87. <https://doi.org/10.1007/s12027-023-00777-2>.

Sigfrids, Anton, Jaana Leikas, Henrikki Salo-Pöntinen, and Emmi Koskimies. "Human-Centricity in AI Governance: A Systemic Approach." *Frontiers in Artificial Intelligence* 6 (2023): 1–9. <https://doi.org/10.3389/frai.2023.976887>.

Thalpage, Nipuna. "Unlocking the Black Box: Explainable Artificial Intelligence (XAI) for Trust and Transparency in AI Systems." *Journal of Digital Art & Humanities* 4, no. 1 (2023): 31–36. https://doi.org/10.33847/2712-8148.4.1_4.

Truby, Jon, Rafael Dean Brown, Imad Antoine Ibrahim, and Oriol Caudevilla Parellada. "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications." *European Journal of Risk Regulation* 13, no. 2 (2022): 270–94. <https://doi.org/10.1017/err.2021.52>.

Valencia-Gálvez, Lorena, Sonia Romero-Pérez, Juan Carlos Ruiz-Flores, and Carlos Andrade-Guzmán. *The Routledge International Handbook of Social Work Teaching*. Edited by Jarosław Przeperski and Rajendra Baikady. London: Routledge, 2024. <https://doi.org/10.4324/9781003422402>.

Wieringa, Maranke. "'Hey SyRI, Tell Me about Algorithmic Accountability': Lessons from a Landmark Case." *Data & Policy* 5 (2023): 1–24. <https://doi.org/10.1017/dap.2022.39>.

Yu, Shasha, and Fiona Carroll. "Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges." In *Artificial Intelligence in Cyber Security: Impact and Implications*, edited by Reza Montasari and Hamid Jahankhani, 157–75. Cham: Springer, 2021. https://doi.org/10.1007/978-3-030-88040-8_6.

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.

PATTIMURA Legal Journal (Pela) is an open access and peer-reviewed journal published by Postgraduate Program Doctoral of Law, Universitas Pattimura, Ambon, Indonesia.

