Global Journal of Law, AI & Ethics (GJLAE)
Journal homepage: https://journals.cognispectra.com/index.php/gjlae/index
Vol. 1, No. 1, August 2025, pp. 14-19
E-ISSN : 3110-8733

Personal Data Protection in the Era of Artificial Intelligence: A Critical Review of Indonesia's Regulatory Readiness Based on OECD Principles

Nendy Akbar Rozaq Rais[1*], **Hariyadi Fajar Nugroho**[2]

[1] **Institut Teknologi Bisnis AAS Indonesia**
[2] **Universitas Muhammadiyah Surakarta**

DOI: 10.65917/gjlae.v1.i1.15

ABSTRACT

Purpose of the Study: This study aims to evaluate the readiness of Indonesian law in regulating personal data protection in the era of artificial intelligence (AI), by highlighting the conformity of national regulations to international standards, especially the OECD Principles and regulations of developed countries such as the European Union.
Methodology: A normative-juridical approach with a qualitative comparative method was used, analyzing Law No. 27 of 2022 (PDP Law) and related instruments. The OECD Principles on AI served as an evaluative framework. The analysis was structured in four stages: (1) identifying OECD principles; (2) mapping provisions in Indonesian law; (3) analyzing regulatory gaps; and (4) comparing with selected jurisdictions (EU, Japan, Singapore, Brazil, India). Case studies were used to illustrate practical implications.
Results: The results of the study show that although several aspects such as the principle of consent and data security have been accommodated in the PDP Law, there is still a legal gap in terms of liability for AI violations, algorithm audits, and transparency of automated decisions. Comparison with regulations of developed countries highlights substantial gaps in the protection of data subject rights.
Applications of This Study: This study can be used as a normative and practical reference for policy makers in designing a legal framework that is adaptive to the development of AI technology, while increasing legal awareness among technology developers and other stakeholders.
Novelty/Originality of This Study: This study offers a critical approach to AI regulation in Indonesia using the OECD Principles as an evaluative parameter, and identifies aspects of the law that have not been widely studied, such as the mechanism for objecting to automated decisions and the right to be forgotten in the context of artificial intelligence.

Keywords:
Artificial Intelligence; Personal Data Protection; AI Regulation; OECD Principles

Received: 3 June 2025
Revised: 22 August 2025
Accepted: 22 August 2025
Available online: 22 August 2025

Corresponding Author:
Nendy Akbar Rozaq Rais
E-mail Address :
Nendy_akbar@itbaas.ac.id

1. INTRODUCTION

The development of Artificial Intelligence (AI) has accelerated significantly in the last decade, making it one of the main components in digital transformation in various sectors (McKinsey Global Survey, 2021; Miller, 2024) [17] [18]. Globally, AI has been widely implemented in public service systems, the digital financial sector (fintech), health services, and electronic government systems (e-government) (Gesk & Leyer, 2022) [11]. According to the McKinsey Global Survey report (2021), more than 50% of large companies in the world have adopted AI technology to improve efficiency and decision-making. In Indonesia, the use of AI is starting to be directed to support national programs such as digitalization of public services, smart cities, and technology-based justice systems (Rizkinaswara, 2022) [24]. One of the main characteristics of AI is its ability to process and analyze big data automatically and quickly (Barredo Arrieta et al., 2020) [2]. However, most of the data collected and analyzed by AI systems is personal data, including sensitive information such as identity, medical records, behavioral preferences, and biometric data (Das, 2025) [7]. This raises concerns about the risk of privacy violations, data misuse, and non-transparent automated decision-making (Brkan, 2019) [4]. In this context, protection of personal data becomes very important, considering that the data is the main asset in the AI work process. Law Number 27 of 2022 concerning Personal Data Protection is an initial milestone in the state's efforts to protect individual privacy rights, but it does not explicitly regulate the complexity of the use of

personal data by AI-based systems (Law on Personal Data Protection, 2022). The application of Artificial Intelligence (AI) technology in the processing of personal data has given rise to various significant legal risks (Fikri & Amelia, 2024; Osano, 2025) [10] [21]. One crucial issue is the potential for violation of individual privacy due to automatic data processing without adequate consent (Jubaidi & Khoirunnisa, 2024) [16]. In addition, the algorithms used in AI systems often show bias that can be detrimental to certain groups (Ferrara, 2023a) [8], especially when used in the public sector or financial services that involve assessing individuals. In the context of Indonesian law, although Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) has been passed, this regulation does not explicitly regulate legal liability for violations committed by AI-based systems. The PDP Law also does not provide clear guidelines regarding algorithm audit mechanisms, supervision of automated decision-making processes, and determination of parties who can be held accountable. This ambiguity creates a legal vacuum that has the potential to weaken the protection of the rights of personal data subjects in a digital ecosystem that is increasingly dominated by autonomous technology. Therefore, an in-depth legal study is needed to evaluate the readiness of national regulations in facing the legal challenges posed by the development of AI.

In response to the legal challenges posed by the development of AI, a number of developed countries have adopted a more comprehensive and adaptive regulatory framework. One widely recognized international reference is the OECD Principles on Artificial Intelligence, declared by the Organisation for Economic Co-operation and Development (OECD) in 2019 (OECD, 2019). These principles emphasize five main aspects: inclusiveness and human well-being, transparency and explainability of the AI decision-making process, accountability of actors involved, resilience of AI systems to risks, and protection of human rights and civil liberties. Countries such as the European Union and Japan have used the OECD principles as a basis for designing national AI policies, including in regulating legal responsibilities, algorithm audits, and protecting personal data more firmly (Cancela-Outeda, 2024) [5]. The European Union has even drafted an AI Act that explicitly regulates risk classification and establishes legal obligations for developers and users of AI systems. This example shows that the OECD principles can serve as a relevant evaluation parameter in assessing the extent to which national laws, including Indonesia, are prepared to anticipate the ethical and legal implications of the use of AI, especially in relation to the processing of personal data (Rahman, 2024) [23]. Therefore, it is important to examine the integration between these international principles and the national legal framework in order to close the regulatory gaps that still exist. When compared to the OECD principles that have been adopted by many developed countries, Indonesia's legal framework in regulating the use of AI, especially in relation to the protection of personal data, still shows a number of substantial gaps (Zuwanda et al., 2024) [26]. Law Number 27 of 2022 concerning Personal Data Protection does regulate the principles of consent, limitation of purposes, and data security, but its implementation is still limited and has not touched on crucial aspects in detail such as transparency in the use of algorithms, the obligation to audit AI systems, and accountability for automated decisions (OECD, 2019) [20]. In addition, although the right to access, correct, and delete data has been mentioned, the implementation of the right to be forgotten does not yet have a clear procedural basis, especially in the context of digital platforms and decentralized AI systems. The PDP Law also does not explicitly require the provision of transparent information to data subjects regarding how the algorithm works, the types of data processed, and the potential risks. This is contrary to the OECD principle which encourages openness and clarity in the decision-making process by AI systems. The absence of norms governing the mechanism for objections to automated decisions also shows that the Indonesian legal framework does not fully guarantee individual control over their personal data. Thus, although Indonesia has a formal legal basis, the substance of its regulations is still not fully in line with international standards in dealing with the ethical and legal challenges of the use of AI. This research is very urgent considering the rapid development of Artificial Intelligence (AI) technology which is increasingly widespread in various sectors, while the regulatory framework for personal data protection in Indonesia is not yet fully adaptive to these dynamics (Abdullah, 2024) [1]. The existing legal gap has the potential to weaken the protection of data subjects' rights and pose a risk of privacy violations and injustice due to AI-based automated decisions. Therefore, this study aims to critically assess the readiness of Indonesian law in regulating personal data protection in the AI era by referring to international principles such as the OECD. The expected scientific contribution of this study is to provide a comprehensive normative review of existing regulations, while identifying weaknesses and legal loopholes that need to be fixed. Practically, this study also aims to produce legal policy recommendations that can assist regulators in formulating a more responsive, accountable, and transparent legal framework, so as to ensure effective personal data protection amidst advances in AI technology.

2. Theoretical Framework

Regulation of emerging technologies such as AI is characterized by uncertainty, rapid evolution, and cross-sectoral implications. Three theoretical lenses are relevant:

1. **Precautionary Principle**: emphasizes early action to prevent harm amid uncertainty.
2. **Risk-based Regulation**: focuses on proportionate oversight depending on risk levels.
3. **Adaptive Governance**: stresses flexibility and iterative learning in policymaking

This study adopts adaptive governance as the guiding framework, evaluating how Indonesia can integrate OECD principles while accounting for its socio-economic context.

3. Method

This study uses a qualitative method with a normative-juridical approach, which aims to analyze and evaluate personal data protection regulations in Indonesia in the context of the use of Artificial Intelligence (AI). The research data are in the form of national laws and regulations, policy documents, and international principles such as the OECD Principles on

Artificial Intelligence. The analysis was carried out through in-depth document and literature studies to identify regulatory gaps, and compare them with global standards to provide more effective and accountable policy recommendations. This approach is in accordance with the legal research standards in the SINTA 2 journal because it focuses on normative studies and legal interpretations. reserved for technical editing by the journal's editorial team.

This research employs a normative-juridical approach supported by qualitative comparative analysis. The OECD AI Principles (2019) serve as evaluative benchmarks. The method consists of:

- **Stage 1:** Identification of OECD principles (transparency, accountability, inclusiveness, resilience, human rights).
- **Stage 2:** Mapping of Indonesian provisions (PDP Law 2022 and related regulations).
- **Stage 3:** Gap analysis between Indonesian law and OECD principles.
- **Stage 4:** Comparative analysis with selected countries (EU, Japan, Singapore, Brazil, India). The inclusion of developing countries enriches contextual relevance. Data sources include legislation, policy documents, international reports, and academic studies. Case illustrations are incorporated (e.g., AI in recruitment, wrongful detention, BPJS data breach) to ground the normative analysis.

4. RESULTS AND DISCUSSION

4.1 National Regulation Analysis

An in-depth analysis of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and other supporting regulations reveals that national regulations have established a number of fundamental principles that support the protection of data subject rights. One of the main achievements is the regulation regarding explicit consent from data owners prior to collection and processing, as well as the obligation of data controllers to ensure the security and confidentiality of personal data managed. In addition, the PDP Law regulates the principle of purpose limitation which limits the use of data only for purposes that have been approved by the data subject, while requiring data controllers to implement risk mitigation measures related to personal data. This regulation marks significant progress in building a legal foundation for personal data protection that is responsive to the digital era. However, the results of the study also show a number of substantive weaknesses that are obstacles in facing the specific challenges of the use of Artificial Intelligence (AI). The PDP Law does not explicitly regulate the legal accountability mechanism for violations arising from automated decisions made by the AI system, so there is a gap in norms that allows for legal confusion regarding who is responsible in the event of data misuse or algorithmic bias. In addition, current regulations do not yet regulate adequate transparency obligations regarding the AI-based decision-making process, including the obligation to disclose the working principles of the algorithm, the parameters used, and the potential impact of the automated decision on the data subject. The aspect of independent algorithm audits to prevent discrimination and bias is also not yet explicitly regulated in the national legal framework. Furthermore, the rights inherent in data subjects, such as the right to object to automated decisions (right to object) and the right to delete data (right to be forgotten), still do not have a clear and effectively accessible implementation mechanism (Intani & Syafira, 2025) [15]. The absence of these detailed regulations has the potential to create legal uncertainty and reduce the effectiveness of personal data protection amidst the rapid advancement of AI technology (Botes, 2023) [3]. Therefore, although the PDP Law has provided a strong initial foundation, these regulations need to be strengthened and refined to accommodate the complexities and risks that arise from the responsible use of AI.

4.2 Comparison with OECD Principles and Developed Country Regulations

A comparison between personal data protection regulations in Indonesia and the principles put forward by the Organisation for Economic Co-operation and Development (OECD) shows a significant gap that has the potential to hinder the effectiveness of legal protection for data subjects in the era of Artificial Intelligence (AI). The OECD has established core principles such as transparency, accountability, fairness, and the individual's right to access and control personal data, including the right to be forgotten, as global standards in AI and personal data regulation. These principles require transparency in the data processing process and clear accountability mechanisms for data managers, which aim to minimize the risk of discrimination and privacy violations resulting from automated decisions. In comparison, the European Union through the European AI Act and the General Data Protection Regulation (GDPR) offers a much more comprehensive and detailed regulatory framework in addressing these issues (Rahman, 2024) [23]. The EU regulation explicitly regulates the obligation for independent algorithmic audits, the obligation for transparency in automated decision-making, and strong data subject rights including effective complaint and enforcement mechanisms. This shows that regulations in developed countries have anticipated and responded to the complexity of risks arising from the use of AI in processing personal data..

Table 1. Comparison of Personal Data Protection in Indonesia with OECD and other Developed Countries

Regulatory Aspects	Indonesia (Law No. 27 of 2022)	OECD Principles	European Union (GDPR & AI Act)	Description /Gap
Transparency of	Approval requirements, but	Full transparency over data	Disclosure obligations of	Indonesia has not explicitly

Data Processing	transparency regarding algorithms is limited	processing and use	automated decision-making methods and algorithms	regulated algorithm transparency
Data Subject Consent	Explicit consent is required	Consent as a basic principle	Informed consent with withdrawal option	Quite appropriate, but implementation needs to be strengthened
Data Controller Accountability	Obligation to maintain data security and confidentiality	The controller is fully responsible	Controllers must ensure algorithm audits and risk mitigation	Indonesia has yet to clearly regulate algorithmic audits and accountability for AI
The Right to Be Forgotten	Regulated, but implementation mechanisms are not yet detailed	Data subject's right to erase data	The express right to effective data erasure	The implementation mechanism in Indonesia still needs to be clarified
Algorithm Audit and Monitoring	Not explicitly stated	Algorithm monitoring and evaluation mechanisms	Mandatory independent audits, strict oversight of AI at risk	Absence of independent algorithmic audit rules in the PDP Law
Automated Decision Making	It is regulated in general terms, without details of objection mechanisms.	Protection against detrimental automated decisions	Right to object and review automated decisions	Indonesian regulations do not yet accommodate the right to object specifically.

The regulatory gap between Indonesia and OECD standards and international best practices has quite serious implications. The absence of adequate provisions regarding algorithm transparency, independent audits, and mechanisms for protecting data subjects' rights poses the risk of weak legal protection for individuals, which in turn can lead to public distrust of AI technology and data management institutions (Greenstein, 2022) [12]. In addition, the regulatory gap has the potential to open loopholes for misuse of personal data and algorithmic bias that are not legally detected, resulting in negative impacts both socially and economically. Therefore, adapting and integrating OECD principles in the development of national regulations is a necessity in order to strengthen an adaptive and equitable personal data protection legal system in Indonesia.

4.3 Impact of Regulatory Gaps on the Protection of Data Subject Rights

Regulatory gaps in personal data protection, particularly related to the use of Artificial Intelligence (AI) technology, pose significant legal and ethical risks to the protection of data subject rights in Indonesia. The ambiguity of norms in Law No. 27 of 2022 regarding the mechanism for accountability for losses caused by automated decisions, the absence of independent algorithmic audits, and the lack of adequate transparency instruments, open up space for privacy violations, data misuse, and discrimination resulting from algorithmic bias (Cheong, 2024; Radanliev, 2025) [6] [22]. A recent study from Australia revealed that the use of AI in the recruitment process can discriminate against job applicants with certain accents or disabilities that affect the way they speak. Research by Dr. Natalie Sheard from the University of Melbourne shows that limited and biased training data, especially that sourced from the US, can disadvantage non-English speakers and individuals with disabilities. AI in recruitment tends to fail to recognize diverse accents, with transcription error rates reaching 22% for some non-English speakers. In addition, the lack of transparency in AI decisions has legal implications, as neither recruiters nor applicants understand how decisions are made. Dr. Sheard calls for regulatory reforms, including specific AI legislation and strengthening anti-discrimination laws to address these issues (Ferrara, 2023b; Hanna et al., 2025; Hasanzadeh et al., 2025; Murikah et al., 2024; Sheard, 2023) [9] [13] [14] [19] [25].

In the context of criminal justice, a case in Maryland, USA, illustrates how over-reliance on AI technology can lead to wrongful detention. Alonzo Cornelius Sawyer was arrested based on his identification by an AI facial recognition system, despite physical differences and alibis supported by witnesses. This detention highlights the dangers of automation bias, where blind trust in AI results ignores contradictory evidence.

The social consequences of this regulatory vacuum include a decline in public trust in institutions that manage personal data and digital systems that increasingly dominate social and economic interactions. From a legal perspective, the absence of norms that provide proactive protection against misuse of AI systems places data subjects in a legally weak position in terms of both remediation and proof. This is contrary to the principles of justice and protection of human rights which are the pillars of a state based on the rule of law. For institutions, legal risks in the form of lawsuits, administrative sanctions, and reputational damage can have a systemic impact on operational sustainability, especially in strategic sectors such as finance, health, and government that increasingly rely on AI technology. Therefore, comprehensive regulatory improvements based on the principle of prudence are urgent to ensure that technological developments do not outpace legal protection instruments.

4.4 Practical and Policy Implications

The results of the analysis show that personal data protection regulations in Indonesia, especially in the context of the use of Artificial Intelligence (AI) technology, are not yet fully adaptive and responsive to the complexity of legal issues raised by the development of this technology. In a situation where AI systems are increasingly involved in decision-making that has a direct impact on citizens' civil rights—whether in the employment, financial, public service, or law enforcement sectors—a regulatory framework is needed that is not only reactive, but also proactive and based on the principle of prudence.

The ideal regulation going forward should include explicit regulations on algorithm audits as an instrument to ensure transparency and accountability in the automated decision-making process. Algorithmic audits serve to ensure that the system used is free from discriminatory bias, and that the data used is valid, relevant, and does not cause unequal treatment. In addition, a right to object mechanism is needed for decisions made automatically by the AI system. This mechanism provides space for data subjects to demand a human review if they feel disadvantaged by the results of algorithmic decisions, in line with the principle of procedural justice..

The practical implications of these findings are the need for legislators and regulators—especially the Ministry of Communication and Information and the Personal Data Protection Supervisory Board—to draft implementing regulations for Law No. 27 of 2022 that are more comprehensive and responsive to the use of AI technology. These implementing regulations can adopt international principles, such as the OECD AI Principles and the European Union's regulations in the EU AI Act, as references in setting standards for algorithm audits, data transparency, and protection of data subject rights.

In addition, legal policy recommendations also include strengthening the capacity of supervisory institutions, preparing national ethical guidelines for AI developers and users, and creating efficient public complaint mechanisms. A cross-sectoral (multi-stakeholder) collaborative approach is also needed so that the resulting policies are not only legally valid, but also operational and contextual in practice.

Thus, Indonesian regulations need to be designed not only to regulate existing technology, but also to anticipate the potential impacts of technology that continues to develop. Adaptive and responsive regulations not only strengthen legal protection for citizens, but also encourage public trust in ethical and human rights-based digital transformation.

4.5 Study Limitations and Suggestions for Further Research

This study has several limitations that need to be openly acknowledged as part of academic integrity. First, the approach of this study is normative juridical with the main focus on the analysis of laws and regulations and principles of international law. Although this approach provides a comprehensive understanding of the normative dimensions of personal data protection regulations and AI, this study has not included empirical dimensions that can enrich the analysis, such as in-depth interviews with policy makers, legal practitioners, AI developers, or data subjects as end users. This limits the research's ability to describe the practical dynamics of regulatory implementation in the field.

Second, this study has not comprehensively reviewed a multidisciplinary approach that combines legal perspectives with the fields of information technology, ethics, and social sciences. In fact, the issue of data protection in the context of AI has complex and interrelated cross-sectoral implications. Third, the scope of the international comparative analysis in this study is still limited to the OECD principles and several regulations from developed countries, so it does not represent the diversity of regulatory approaches in developing countries or in other regional frameworks, such as ASEAN.

Therefore, further research is recommended to take a more holistic and multidisciplinary approach, by combining normative and empirical studies. Further research could involve surveys or interviews with key actors in the public and private sectors to evaluate the effectiveness of regulatory implementation and perceptions of the legal and ethical risks of AI use. In addition, a broader comparative approach to the legal systems of developing countries is also important to formulate adaptive strategies that are more contextual to Indonesia's needs. Cross-disciplinary research that combines law, public policy, computer science, and technology ethics is also highly recommended to strengthen the conceptual and policy basis for data protection in the era of artificial intelligence..

5. CONCLUSION

The increasingly widespread use of Artificial Intelligence (AI) technology brings new legal challenges, especially in the protection of personal data. Although Indonesia has Law No. 27 of 2022, this regulation does not fully address the complexity of the risks posed by AI, such as automated decisions and the use of data without explicit consent. The results of the comparison with the OECD principles and regulations of developed countries show gaps in the aspects of transparency, accountability, and data subject rights. This condition has the potential to weaken legal protection and increase the risk of privacy violations. Therefore, it is necessary to strengthen more responsive and comprehensive regulations, including the regulation of the responsibilities of AI actors, algorithm audits, and objection mechanisms. This research provides a normative contribution as a basis for policy makers in formulating legal policies that are adaptive to the development of AI. Indonesia’s PDP Law provides a foundation but lacks mechanisms to address AI-specific risks. Comparative insights reveal the need for adaptive governance frameworks that combine international standards with contextual realities. Beyond descriptive legal analysis, this study contributes theoretically by positioning Indonesia as a case of AI governance in developing countries. The findings highlight the urgency of algorithm audits, accountability frameworks, and enforceable rights to ensure personal data protection in the AI era.

REFERENSI

[1] Abdullah, A. M. (2024). Pelindungan Hak Privasi terhadap Pengumpulan Data Pribadi oleh AI Generatif Berdasarkan Percakapan dengan Pengguna. *Padjadjaran Law Review*, *12*(2), 145–156. https://doi.org/10.56895/plr.v12i2.1796

[2] Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[3] Botes, M. (2023). Regulating scientific and technological uncertainty: The precautionary principle in the context of human genomics and AI. *South African Journal of Science*, *119*(5/6). https://doi.org/10.17159/sajs.2023/15037

[4] Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, *27*(2), 91–121. https://doi.org/10.1093/ijlit/eay017

[5] Cancela-Outeda, C. (2024). The EU's AI act: A framework for collaborative governance. *Internet of Things*, *27*, 101291. https://doi.org/10.1016/j.iot.2024.101291

[6] Cheong, B. C. (2024). Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, *6*. https://doi.org/10.3389/fhumd.2024.1421273

[7] Das, I. (2025, April 18). *AI and Data Privacy: Mitigating Risks in the Age of Generative AI Tools*. Qualys. https://blog.qualys.com/product-tech/2025/02/07/ai-and-data-privacy-mitigating-risks-in-the-age-of-generative-ai-tools

[8] Ferrara, E. (2023a). Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies. *Sci*, *6*(1), 3. https://doi.org/10.3390/sci6010003

[9] Ferrara, E. (2023b). Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies. *Sci*, *6*(1), 3. https://doi.org/10.3390/sci6010003

[10] Fikri, A., & Amelia, T. (2024). Indonesia's Legal Policy on Protecting Personal Data from Artificial Intelligence Abuse. *SHS Web of Conferences*, *204*, 07002. https://doi.org/10.1051/shsconf/202420407002

[11] Gesk, T. S., & Leyer, M. (2022). Artificial intelligence in public services: When and why citizens accept its usage. *Government Information Quarterly*, *39*(3), 101704. https://doi.org/10.1016/j.giq.2022.101704

[12] Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*(3), 291–323. https://doi.org/10.1007/s10506-021-09294-4

[13] Hanna, M. G., Pantanowitz, L., Jackson, B., Palmer, O., Visweswaran, S., Pantanowitz, J., Deebajah, M., & Rashidi, H. H. (2025). Ethical and Bias Considerations in Artificial Intelligence/Machine Learning. *Modern Pathology*, *38*(3), 100686. https://doi.org/10.1016/j.modpat.2024.100686

[14] Hasanzadeh, F., Josephson, C. B., Waters, G., Adedinsewo, D., Azizi, Z., & White, J. A. (2025). Bias recognition and mitigation strategies in artificial intelligence healthcare applications. *Npj Digital Medicine*, *8*(1). https://doi.org/10.1038/s41746-025-01503-7

[15] Intani, A. A., & Syafira, A. (2025). The Right to be Forgotten: Protecting Emergency Contact in the Reform of Personal Data Protection Policy in Indonesia. *South-East Asian Journal of Advanced Law and Governance (SEAJ ALGOV)*, *2*(1), 38–52.

[16] Jubaidi, D., & Khoirunnisa, K. (2024). Artificial Intelligence in the Perspective of Indonesian Law: Subject or Object of Law? *Asian Journal of Education and Social Studies*, *50*(11), 302–314. https://doi.org/10.9734/ajess/2024/v50i111655

[17] McKinsey Global Survey. (2021). *The state of AI in 2021*. https://www.mckinsey.com/capabilities/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021

[18] Miller, K. (2024, March 18). Privacy in an AI Era: How Do We Protect Our Personal Information? *Stanford HAI*. https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information

[19] Murikah, W., Nthenge, J. K., & Musyoka, F. M. (2024). Bias and ethics of AI systems applied in auditing—A systematic review. *Scientific African*, *25*, e02281. https://doi.org/10.1016/j.sciaf.2024.e02281

[20] OECD. (2019). *Artificial Intelligence in Society*. OECD. https://doi.org/10.1787/eedfee77-en

[21] Osano. (2025, January 28). *AI and Data Privacy: Exploring the Privacy Risks in the Era of Artificial Intelligence*. Osano. https://www.osano.com/articles/ai-and-data-privacy?utm_source=chatgpt.com

[22] Radanliev, P. (2025). AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development. *Applied Artificial Intelligence*, *39*(1). https://doi.org/10.1080/08839514.2025.2463722

[23] Rahman, R. A. (2024). Artificial Intelligence Regulation on Labour Market: Comparative Perspectives on the European Union Artificial Intelligence Act in the Indonesian Context. *Lex Scientia Law Review*, *8*(1). https://doi.org/10.15294/lslr.v8i1.3465

[24] Rizkinaswara, L. (2022, July 20). *Gerakan Menuju 100 Smart City*. Ditjen Kominfo. https://aptika.kominfo.go.id/2022/07/gerakan-menuju-100-smart-city-2/#:~:text=Pada%202021%20program%20ini%20difokuskan,mendukung%20program%20nasional%2C%20yaitu%20berupa:

[25] Sheard, N. (2023). *Submission in response to the Australian Government's' Safe and Responsible AI in Australia: Discussion Paper'*.

[26] Zuwanda, Z. S., Lubis, A. F., Solapari, N., Sakmaf, M. S., & Triyantoro, A. (2024). Ethical and Legal Analysis of Artificial Intelligence Systems in Law Enforcement with a Study of Potential Human Rights Violations in Indonesia. *The Easta Journal Law and Human Rights*, *2*(03),176–185. https://doi.org/10.58812/eslhr.v2i03.283