






Artificial Intelligence in The Implementation of Public Governance: Public Data Security Vulnerabilities in Indonesia

Dimas Agustian¹, S.Y. Regif¹, Hendrikus Hironimus Botha¹, Andre Pattipeilohy¹, Samsul Ode²

¹ Prodi Administrasi Publik, FISIP, Universitas Timor, Kefamenanu, Timor Tengah Utara

² Prodi Ilmu Pemerintahan, FEBIS, Universitas 17 Agustus 1945 Jakarta, Sunter Permai Raya, Kota Jakarta Utara

*Koresponden email: dimas.agustian.adm@unimor.ac.id

ABSTRACT

Received: February 23, 2025

Revised: March 11, 2025

Accepted: March 30, 2025

Keywords:

Artificial Intelligence, Public Governance, Public Data Security.

This study examines the implementation of Artificial Intelligence (AI) in public governance in Indonesia, focusing on its potential for service improvement and data security challenges. Governments globally, including in Indonesia, are increasingly utilizing AI for efficiency, policy analysis, and public services. However, increased AI-driven online services heighten the risks to personal data security and privacy, alongside broader cyber threats. Significant concerns about data privacy breaches, lack of transparency, and amplification of bias in AI systems used by governments, which can lead to unfair and discriminatory outcomes. Unregulated or unsupervised AI in government-posing risks such as data privacy breaches, legal non-compliance, operational disruption, and erosion of public trust. The use of AI has led to debates on the use of AI in public governance and its security has been extensively discussed in recent literature across multiple dimensions. Using a literature review method, the analysis shows AI has significant potential to enhance public service efficiency and quality (e.g., via chatbots and data analysis), but its implementation in Indonesia is hindered by infrastructure limitations, human resource capacity, ethical aspects, and data security vulnerabilities. Indonesia faces significant public data security vulnerabilities, marked by frequent data breach incidents and AI-driven cyberattacks, exacerbated by inadequate infrastructure, regulations, and low awareness. The study concludes Indonesia lacks comprehensive AI regulations. Strengthening technical capabilities, improving education, fostering international cooperation, updating legislation, and strict law enforcement are necessary to protect data and ensure responsible AI use in public governance.

INTRODUCTION

Governments around the world are increasingly utilising artificial intelligence (AI) to improve public safety and governance (OECD, 2024; Zuiderwijk et al., 2021). AI is used to accelerate document processing, more in-depth policy analysis, and accelerate public services so that governance becomes more innovative and accountable (Alhosani & Alhashmi, 2024; Kulal et al., 2024; Selten & Klievink, 2024). AI helps analyse large amounts of data for more informed decision-making in sectors such as health, education and infrastructure (Bajwa et al., 2021; Soori et al., 2024). In addition, AI can automate repetitive tasks, allowing public servants to focus on more strategic roles (Rožman et al., 2023).

For example, AI chatbots are helping customer service in the world's transport sector improve service efficiency (Abel Uzoka et al., 2024; Ma'rup et al., 2024). The use of AI also increases transparency and reduces corruption through automated systems that monitor activities in real-time and keep accurate records. (Adam & Fazekas, 2021; Hartanto et al., 2024).

However, the rise of AI-powered online public services brings greater risks to personal data protection and privacy breaches, as well as broader cybersecurity challenges (Adebola Folorunso et al., 2024; Binhammad et al., 2024; Ejijami, 2024; Jada & Mayayise, 2024; Ye et al., 2024).

Therefore, AI governance should include restrictions that ensure AI systems remain safe, ethical, and respectful of human rights (Papagiannidis et al., 2025; Pirozzoli, 2024; Rodrigues, 2020; United Nations Educational, 2021; WHO, 2021). The government needs to make clear rules and provide training to officials so that AI development can proceed responsibly and fairly (Sandeep Reddy, 2023).

AI has offered new ways to improve public governance, it still has the potential to improve government accountability and public services (Zuiderwijk et al., 2021). Although not yet visible at this stage, such accountability can occur by using AI to test the accuracy of government algorithms. (Novelli et al., 2024). This process involves the AI sending various input variables to a government algorithm to determine how the algorithm makes decisions (Loi & Spielkamp, 2021). This enables the assessment of potential biases based on protected social categories (such as profession, ethnicity, gender, and religion). Through the use of social media data, AI can also be used to identify patterns and changes in public opinion, thus providing feedback to identify emerging issues, and improve government responses to the public. (Gerlich et al., 2023).

Along with the enthusiasm for the use of AI in governance, a number of ethical, social, political, and legal/regulatory challenges are increasingly being scrutinised. Many national governments and international government organisations have

organised discussions, issue briefings, and research related to AI with public data security policies, such as Indonesia's (Dewi & Hidayat, 2022; Fikri & Amelia, 2024; Gandawidjaja et al., 2025; Wadipalapa et al., 2024), Australia (Dawson, 2019), Tiongkok (Xuan, 2023), Eropa (European Commission, 2019); Singapura (PDPC, 2018); Inggris (Leslie, 2019); AS (Committee on Artificial Intelligence of the National Science & Council, 2019); dan OECD (2019). In addition to traditional digital rights concerns around privacy, surveillance and data protection, the results of these research reports often highlight challenges that lead to bias and discrimination; transparency, accountability and clarity; technical accuracy; and legality and due process. (Fjeld et al., 2020; Mittelstadt et al., 2016). Therefore, it is necessary to explore and analyse Artificial Intelligence in the implementation of public governance, especially in addressing the vulnerability of public data security in Indonesia.

Artificial intelligence (AI) is a multidisciplinary field of science and technology that focuses on making computers and machines capable of performing work that would normally require human intelligence (Müller Editor, 2017; Xu et al., 2021). The work of these systems includes reasoning, learning, problem-solving, perception, language understanding, and decision-making. AI systems are designed to simulate human cognitive functions, allowing them to analyse data, recognise patterns, make predictions, and adapt to new information without explicit human programming. (Collins et al., 2021).

The implementation of public governance refers to the practical application of governance principles, such as transparency, accountability, participation, efficiency, and effectiveness, within public sector institutions to ensure that government actions are responsible, responsive, and serve the public interest. Good public governance is essential for building public trust, improving service delivery, and achieving sustainable development goals. (Azzahra, 2023; Budiawan et al., 2022; Guntur, 2017). A public data security vulnerability is a weakness in a system, application, or process that can be exploited to gain un-authorised access to, misuse, or compromise sensitive public data. (Borky & Bradley, 2019). These vulnerabilities affect a wide range of sectors, including government, healthcare, education and private companies, and can result in significant losses, such as data breaches, identity theft, financial fraud and loss of public trust (George, 2008). The debate on the use of AI in public governance and its security has been widely discussed in the current literature across multiple dimensions. By OECD(2024), AI can increase government productivity by improving internal operations and making public policies and services more inclusive, responsive, and accountable. AI can strengthen oversight capacity and support independent institutions to increase transparency and effectiveness in governance. AI-based automation can transform service delivery models and regulatory processes, potentially improving decision-making and strategic planning in public administration.

However, there are significant concerns about data privacy breaches, lack of transparency, and amplification of bias in AI systems used by governments, which can lead to unfair and discriminatory outcomes. Unregulated or unsupervised AI in government-poses risks such as data privacy breaches, legal non-compliance, operational disruption, and erosion of public trust. AI infrastructure is vulnerable to cyberattacks, requiring a design-based security approach to protect AI systems and sensitive data ((Mensah, 2023)

The political legitimacy of AI governance, particularly on a global scale, is still debated, emphasising that AI governance must be democratic and transparent at a minimum to maintain public trust(Erman & Furendal, 2024). A distinction is made between 'governance by AI' (AI systems making decisions) and 'AI governance' (governing the development and application of AI), with each raising different normative and legitimacy issues(Jaiswal, 2022). The opacity of AI decision-making, such as in facial recognition or automated policy enforcement, challenges democratic accountability and public oversight(Cheong, 2024). Necessarily, an effective AI governance framework emphasises privacy protection, bias mitigation, ethical guidelines, sustainability, and infrastructure security to ensure safe and responsible use of AI in the public sector. Broader internet governance issues overlap with AI governance, highlighting challenges in multi-stakeholder coordination and cybersecurity threats that transcend jurisdictions, which also affect AI governance in the public sector.(Bokhari & Myeong, 2017; United Nation, 2024). Modern AI governance frameworks place privacy protection and data security as key pillars. This is driven by growing concerns over potential data breaches and misuse of personal information by AI systems, particularly when used in public services involving sensitive citizen data. This framework demands clear regulations and strong data protection mechanisms, as well as the integration of human rights principles in every AI policy and implementation. One key novelty is the recognition that AI governance cannot be effective without multi-stakeholder engagement likely government, private sector, civil society, and academia. This collaborative process often faces coordination challenges, divergent interests, and perspective gaps. It is hoped that multi-stakeholder discussions will open up perspectives and lead to more inclusive solutions. Through this analysis will find parts that can close the gap in AI governance in public spaces in Indonesia.

METHODS

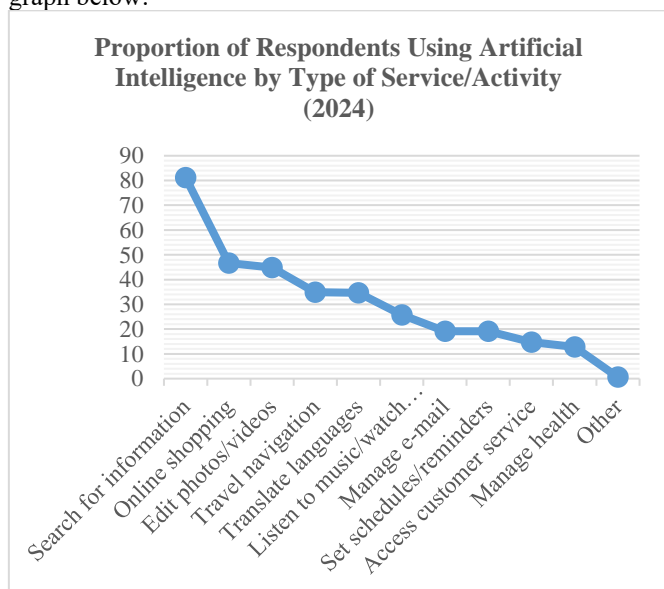
The desk study method, also known as library research, is a qualitative research approach that involves collecting and analysing data from literature and sources available in libraries, such as books, journals, articles, magazines, newspapers, and encyclopaedias.(George, 2008; Lim, 2024). This method does not involve fieldwork or direct data collection from subjects, but relies on ready-made data and documented information to answer research questions or solve problems(Kabir, 2016; Taherdoost, 2021). The steps in the literature study method are (Francis Lau and Craig Kuziemy, 2016), (Hannah Snyder, 2019); (1). Data Collection, systematically gathering information from various library materials and digital databases. This includes keyword searching, subject searching using specific terms or descriptors, and browsing collections organised by subject to find relevant sources (2). Research Process which involves identifying relevant sources, locating them, gaining access, evaluating their relevance and reliability, and integrating findings into a coherent analysis or report. (3). Purpose and Use to provide background, compare theories, analyse existing knowledge, and support further research. It is particularly useful for descriptive and comparative studies and can serve as a basic step in broader research projects. (4). The researcher acts as the main instrument for data collection and analysis, interpreting information from the literature to draw conclusions.

RESULTS AND DISCUSSION

Artificial Intelligence in the Implementation of Public Governance

The application of artificial intelligence (AI) in improving public services, particularly in automated decision-making by governments, shows great potential despite its currently limited use. AI in the public sector can operate in three main forms: detecting patterns, sorting populations, and making predictions, all of which can help speed up and improve the accuracy of decision-making. Governments are already using computer algorithms to assist officials in decision-making, and the current trend is towards greater automation without direct human involvement. However, the use of true AI is still limited and sometimes difficult to distinguish from advanced statistical analysis-based systems.

AI is able to optimise the process of collecting, analysing and interpreting complex data, thus enabling more accurate and efficient predictions in public decision-making. Examples of AI applications in public services in Indonesia include the use of chatbots for health services (such as BPJS Kesehatan), which improves efficiency and quality of service and creates public value through procedural fairness and public trust. In the field of government administration, AI is used for document processing, voice and text recognition, and analysis of public service complaints that can be automatically routed to the relevant agencies, accelerating response and public oversight. AI is also applied to detect potential tax fraud, manage traffic flow, and predict the number of tourists and economic impact in the tourism sector, all of which contribute to more informed and rapid decision-making. In Indonesia, the use of Artificial Intelligence is targeted in various matters related to public interest. the following data is presented in the graph below:



Source: Katadata Insight Centre (KIC) research report, 2024

Pic. 1. Proportion of Respondents Using Artificial Intelligence by Type of Service/Activity (2024)

In late 2024, KIC conducted a survey in 38 Indonesian provinces to map people's experiences with AI. And it turns out, out of 1,255 respondents, more than half (65%) have used AI for various purposes. In this group of AI-using respondents, the majority or 81% use the technology to find information. While AI offers efficiency and improved service quality, significant challenges remain, including infrastructure limitations, technology gaps between regions, and human

resource capacity to master AI technologies. Adaptive and collaborative policy development between the government, private sector, and educational institutions is essential to support the development of human resource capacity and AI technology infrastructure. Ethical aspects, privacy, and data security are also important concerns in the application of AI for public decision-making, so it is necessary to design policies that pay attention to these matters so that the use of AI can be responsible.

A chatbot or virtual assistant is an artificial intelligence (AI)-powered computer programme designed to interact with users through spoken or written conversations, both in text and voice, with the aim of mimicking natural human communication. Chatbots are able to answer questions, provide information, and perform certain tasks automatically and efficiently. In the context of government and public governance services that are complex and diverse, accurate, relevant, and easily accessible information is required at any time. To be effective in public services, chatbots in government usually integrate several technologies. This aims to: (a). improve the efficiency and speed of public services. (b). reduce the workload of government employees in handling routine enquiries. (c). expand access to public services without time and place restrictions. (d). support the digital transformation of government towards more responsive and transparent services.

Governments are also increasingly using AI to improve public safety and public governance. The increased use of online public services comes with greater risks to data protection and privacy breaches, as well as broader cybersecurity challenges. AI is being used to identify emerging real-time patterns to enable government responses to assess denial-of-service cyberattacks or other malicious cyberwarfare activities. Governments are also investigating how to use AI to detect and respond to disinformation campaigns, which can be used to disrupt the political process or public safety. Governments are increasingly using artificial intelligence (AI) to improve public safety and public governance, especially in the context of online public services that are at risk of data protection and privacy breaches and broader cybersecurity challenges.

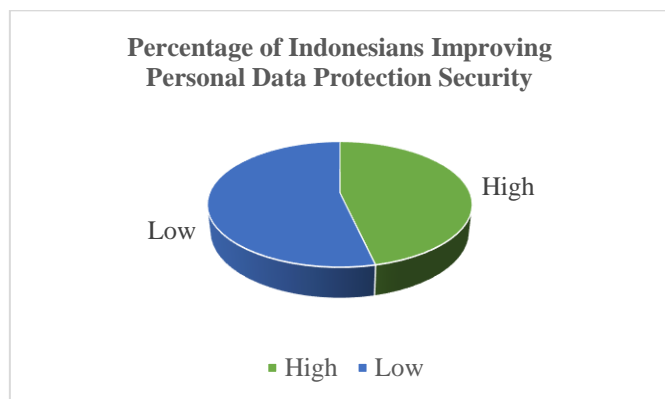
AI is being used to identify threat patterns in real-time, enabling rapid government response in assessing cyberattacks or other malicious cyberwarfare activities. In addition, AI is also being developed to detect and respond to disinformation campaigns that can disrupt political processes and public safety. The utilisation of AI in government is also geared towards improving the efficiency of public services by providing more accurate information and customised services to users, while strengthening the relationship between government and society.

However, the use of AI presents challenges related to data security, public trust, and the need for strict regulations to manage risks and ensure safety and ethics in the use of AI. The government is working to implement the principles of transparency, accountability, data privacy, and security in the management of AI, as well as strengthening cooperation with security forces to deal with the threat of AI-based crimes. Indonesia needs to accelerate digital transformation through the implementation and acceleration of integrated services with better data security, for example through a secure Single Sign-on system to reduce data leakage and repetitive data entry or other simultaneous authentication systems.

Regulatory enforcement is an important area in the Indonesian government's use of AI, especially in the context of ensuring legal compliance and effectiveness of existing regulations. The Indonesian government has issued several policies and regulations governing the use of AI, such as the Minister of Communication and Information Circular Letter No. 9 of 2023 on the Ethics of Artificial Intelligence, which became the initial legal umbrella for the ethical and responsible use of AI. The government also encourages AI regulations that protect user privacy and data, ensure transparency, accountability, and encourage ethical and non-discriminatory use of AI. This is important so that AI-assisted law enforcement can be fair and not cause human rights violations. Strategies for AI regulation in Indonesia include developing clear policies, involving various stakeholders, and encouraging international collaboration so that AI-based law enforcement can be effective and in line with global standards.

Public Data Security Vulnerabilities in Indonesia

Indonesia has faced many significant personal data breach incidents, including data from the government, e-commerce, banking and healthcare sectors. The personal data of millions of citizens, including sensitive data such as Taxpayer Identification Numbers (NPWP) and electronic ID card data, have been leaked and spread online. In 2021, approximately 239.74 million cyberattacks were recorded in Indonesia, with the capital city of Jakarta as the main target. Major incidents such as the ransomware attack on the National Data Centre in Surabaya and the e-visa data leak show weaknesses in data security management in the public sector. Online fraud is the most common case of data security vulnerability experienced by internet users in Indonesia. The following data is presented:



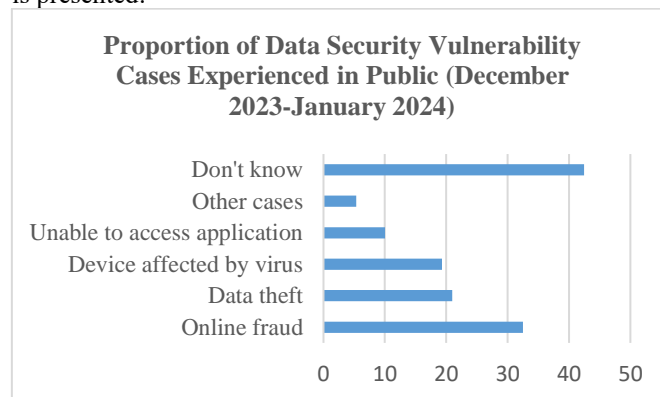
Source: Ministry of Communication and Information of the Republic of Indonesia, 2021

Pic. 2. Percentage of Indonesians Improving Personal Data Protection Security

Inadequate security infrastructure that has not fully adopted international standards such as ISO 27001, making data vulnerable to hacking, malware and phishing attacks. Lack of effective regulation and consistent monitoring of the implementation of the Personal Data Protection Law (PDP Law). Organisational compliance with this law remains low. Lack of data security awareness and training among organisations and the public, resulting in a high risk of human error in data management.

Extensive data leaks threaten individual privacy and lower public trust in digital services and government. Operational disruption of public services due to cyberattacks such as ransomware that can hamper public services. Potentially large economic and social losses due to misuse of personal data.

Many Indonesian businesses lack understanding of AI technology, with 46% admitting limited knowledge of how AI-driven fraud works. This understanding gap makes them highly vulnerable to sophisticated fraud techniques such as social engineering, account takeover, and document and signature forgery. The attacks on public security published by IBM (International Business Machines, 2025) contain 67% phishing attacks, 51% have experienced smishing (SMS-based fraud), 47% have been victims of vishing (voice-based fraud), 97% reported account takeover attempts. Based on The Indonesian Internet Penetration Survey Report 2024 from the Indonesian Internet Service Providers Association (APJII) compiled a number of cases related to data security experienced by internet users in Indonesia. The following data is presented:



Source: Indonesian Internet Service Providers Association (APJII), 2024

Pic.3. Proportion of Data Security Vulnerability Cases Experienced in Public

AI-powered cyberattacks have fundamentally changed the cybersecurity landscape by allowing hackers to automate, scale and adapt their attacks with unprecedented speed and sophistication. Here's how AI is driving this change and the resulting consequences, Vulnerabilities through the misuse of AI allow cybercriminals to automate many phases of an attack, from reconnaissance (identifying vulnerabilities and targets) to execution (deploying malware, phishing or other exploits). This automation drastically reduces the time and effort required to launch large-scale campaigns, making attacks faster and more widespread than traditional methods.

AI can efficiently collect and analyse large amounts of data from public and private sources, allowing attackers to identify vulnerable targets and craft highly personalised phishing or social engineering attacks. This increases the likelihood of success and makes attacks harder to detect. AI-powered malware and attack tools can learn and evolve, adapting their behaviour in real time to evade traditional security measures such as signature-based detection or static firewalls. This makes them more resilient to conventional defences. With AI, attackers can orchestrate simultaneous attacks on multiple organisations or individuals, increasing the scale and impact of the campaign. AI-driven attacks can target sectors such as finance, healthcare and government, often with devastating consequences. AI-powered attacks have led to major data theft incidents, targeting sensitive financial and personal information. This includes bank details, social security numbers, and confidential business data, compromising individual privacy and organisational security. The theft and misuse of sensitive data results in direct financial losses for citizens, businesses, and government agencies. Indirectly, organisations face reputational damage, regulatory sanctions, and loss of customer trust. AI-based attacks can also penetrate

critical infrastructure, such as banking systems and government networks, raising concerns about national security and public safety.

Indonesia ranked 8th globally in data breaches in 2023, with over 3,300 cyber attacks reported each week at the beginning of the year. Significant incidents included ransomware attacks on the National Data Center and breaches affecting government agencies such as the National Civil Service Agency and the tax office, exposing millions of sensitive records. The financial, manufacturing, and transportation sectors were also targeted by ransomware, leading to operational disruptions and financial losses. Information manipulation and black campaign attacks via social media, driven by AI-generated misinformation, threaten political, economic, and social stability by manipulating public opinion and spreading false information. Repeated breaches and AI-supported attacks undermine trust in digital systems and technologies, potentially slowing the adoption of new innovations crucial for economic and social development. The leakage of sensitive data and AI-supported cyber espionage poses a threat to the political and economic stability of Indonesia. The existing cybersecurity framework and law enforcement are insufficient to effectively prevent cyber criminals, thus necessitating stronger legal measures and law enforcement to protect data privacy and enhance national cyber defense.

CONCLUSION

Indonesia currently lacks comprehensive laws and regulations specifically governing AI systems and ensuring the safety and protection of citizens' data. This regulatory gap makes public data vulnerable to misuse and cyber threats, undermining public trust and government legitimacy. The development and reuse of public data are hindered by infrastructure constraints and digital skills that are lacking among government workers. Many local governments struggle to fully implement basic e-government systems, which are a prerequisite for the successful adoption of AI. Although AI has the potential to enhance cybersecurity through advanced threat detection and automated responses, the increasing number of data breaches highlights the ongoing vulnerabilities. The recent enactment of the Personal Data Protection Act marks progress, but full implementation and enforcement remain challenging.

The application of AI in public administration must align with the principles of transparency, fairness, and accountability. Existing laws, such as Law No. 30 of 2014, have not accommodated automated or algorithmic decision-making, thus requiring legal reform to ensure the responsible use of AI in governance. Various efforts are being made to strengthen AI management through policy development, accountability frameworks, and collaboration among government, industry, academia, and society. However, operational cybersecurity measures such as infrastructure security and anonymization techniques need to be enhanced to protect sensitive data. Therefore, here are the recommendations: (1). Strengthening technical capabilities for early detection, response, and data encryption is crucial to counter AI-driven attacks. (2). Increasing education and awareness about AI cybersecurity threats among businesses and the public can enhance preparedness and reduce vulnerability. (3). Cooperation with global partners can enhance Indonesia's cybersecurity resources and strategies to combat advanced AI threats. (4). Updating data protection

laws and ensuring strict enforcement can help reduce risks and build public trust in data security.

REFERENCES

- Abel Uzoka, Emmanuel Cadet, & Pascal Ugochukwu Ojukwu. (2024). Leveraging AI-Powered chatbots to enhance customer service efficiency and future opportunities in automated support. *Computer Science & IT Research Journal*, 5(10), 2485–2510. <https://doi.org/10.51594/csitrj.v5i10.1676>
- Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, 57. <https://doi.org/10.1016/j.infoecopol.2021.100950>
- Adebola Folorunso, Temitope Adewumi, Adeola Adewa, Roy Okonkwo, & Tayo Nathaniel Olawumi. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances*, 21(1), 167–184. <https://doi.org/10.30574/gjeta.2024.21.1.0193>
- Alhosani, K., & Alhashmi, S. M. (2024). Opportunities, challenges, and benefits of AI innovation in government services: a review. In *Discover Artificial Intelligence* (Vol. 4, Issue 1). Springer Nature. <https://doi.org/10.1007/s44163-024-00111-w>
- Azzahra, A. (2023). Implementation Of Good Governance in Public Services at Local Government. *International Journal of Social Service and Research*, 3(7), 1899–1906. <https://doi.org/10.46799/ijssr.v3i7.594>
- Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial intelligence in healthcare: transforming the practice of medicine. *Future Healthcare Journal*, 8(2), e188–e194. <https://doi.org/10.7861/fhj.2021-0095>
- Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, 15(02), 245–278. <https://doi.org/10.4236/jis.2024.152015>
- Bokhari, S., & Myeong, S. (2017). The Influence of Artificial Intelligence on E-Government. *IEEE Access*, xx. <https://doi.org/10.1109/ACCESS.2023.3293480>
- Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering* (pp. 345–404). Springer International Publishing. https://doi.org/10.1007/978-3-319-95669-5_10
- Budiawan, F. P., Nuryati, T., Bhayangkara, U., & Raya, J. (2022). *Understanding the Implementation of Good Government Governance (GGG) on The Quality of Public Services*. <https://doi.org/10.38035/jafm.v3i3>
- 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>
- Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, 60. <https://doi.org/10.1016/j.jinfomgt.2021.102383>
- Committee on Artificial Intelligence of the National Science, S., & Council, T. (2019). *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*. <https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf>
- Dawson, C. D. (2019). *Artificial Intelligence*. <https://consult.industry.gov.au/>

- Dewi, S., & Hidayat, M. W. (2022). Protection of Data Privacy in The Era of Artificial Intelligence in The Financial Sector in Indonesia. *Journal of Central Banking Law and Institutions*, 1(2). <https://doi.org/10.21098/jcli.v1i2.18>
- Ejjami, R. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. *Journal of Next-Generation Research* 5.0. <https://doi.org/10.70792/jngr5.0.v1i1.5>
- Erman, E., & Furendal, M. (2024). Artificial Intelligence and the Political Legitimacy of Global Governance. *Political Studies*, 72(2), 421–441. <https://doi.org/10.1177/00323217221126665>
- European Commission. (2019). *High-Level Expert Group On Artificial Intelligence A Definition Of AI: Main Capabilities And Disciplines Definition developed for the purpose of the AI HLEG's*. <https://ec.europa.eu/digital-single->
- 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>
- Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. C., & Srikumar, M. (2020). *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*. <https://ssrn.com/abstract=3518482>
- Gandawidjaja, Y., Bunawan, P., Josua, C., & Purba, F. X. (2025). *The Role Of The State Towards Data Protection In The Use Of Artificial Intelligence Through The Cooperation Between Countries In Asean* (Vol. 13, Issue 6). <https://legal.isha.or.id/index.php/legal/index>
- George, M. (2008). *Elements of Library Research*. Princeton University Press. http://pustaka.unp.ac.id/file/abstrak_kki/EBOOKS/LIBRARY%20The%20Elements%20of%20Library%20Research.pdf
- Gerlich, M., Elsayed, W., & Sokolovskiy, K. (2023). Artificial intelligence as toolset for analysis of public opinion and social interaction in marketing: identification of micro and nano influencers. *Frontiers in Communication*, 8. <https://doi.org/10.3389/fcomm.2023.1075654>
- Guntur, M. (2017). *Implementation Of Good Governance Principles Based On Transparency, Accountability And Public Participation In Indonesia*. <https://eprints.unm.ac.id/5808/78/73-Guntur.pdf>
- Hartanto, M. B., Ikhwan, A., Eko, D., Pramono, H., Sukri, H., & Purnomo, R. F. (2024). Leveraging Artificial Intelligence to Combat Corruption: Innovative Solutions for Transparent Governance. *RISTEC: Research in Information Systems and Technology*, 5(2). <https://journal.institutpendidikan.ac.id/index.php/ristec/article/view/2177>
- Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 8(2). <https://doi.org/10.1016/j.dim.2023.100063>
- Jaiswal, U. (2022). The Political Justification of Global Governance in the Age of Artificial Intelligence. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 2(1). <https://doi.org/10.48175/568>
- Kabir, S. (2016). *Methods Of Data Collection*. <https://www.researchgate.net/publication/325846997>
- Kulal, A., Rahiman, H. U., Suvarna, H., Abhishek, N., & Dinesh, S. (2024). Enhancing public service delivery efficiency: Exploring the impact of AI. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(3). <https://doi.org/10.1016/j.joitmc.2024.100329>
- Leslie, D. (2019). *Understanding artificial intelligence ethics and safety*. <https://doi.org/10.5281/zenodo.3240529>
- Lim, W. M. (2024). What Is Qualitative Research? An Overview and Guidelines. *Australasian Marketing Journal*. <https://doi.org/10.1177/14413582241264619>
- Loi, M., & Spielkamp, M. (2021). Towards Accountability in the Use of Artificial Intelligence for Public Administrations. *AIES 2021 - Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 757–766. <https://doi.org/10.1145/3461702.3462631>
- Ma'rup, M., Tobirin, & Ali Rokhman. (2024). Utilization of Artificial Intelligence (AI) Chatbots in Improving Public Services: A Meta-Analysis Study. *Open Access Indonesia Journal of Social Sciences*, 7(4), 1610–1618. <https://doi.org/10.37275/oaijs.v7i4.255>
- Mensah, G. B. (2023). Artificial Intelligence and Ethics: A Comprehensive Review of Bias Mitigation, Transparency, and Accountability in AI Systems. *Africa Institute For Regulatory Affairs* LBG. <https://doi.org/10.13140/RG.2.2.23381.19685/1>
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data and Society*, 3(2). <https://doi.org/10.1177/2053951716679679>
- Müller Editor, V. C. (2017). *Studies in Applied Philosophy, Epistemology and Rational Ethics*. <http://www.springer.com/series/10087>
- Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: what it is and how it works. *AI and Society*, 39(4), 1871–1882. <https://doi.org/10.1007/s00146-023-01635-y>
- OECD. (2024). *Restricted Use- A usage restraint*. <http://www.oecd.org/termsandconditions>.
- Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. In *Journal of Strategic Information Systems* (Vol. 34, Issue 2). Elsevier B.V. <https://doi.org/10.1016/j.jsis.2024.101885>
- PDPC. (2018). *Discussion Paper On Artificial Intelligence (AI) And Personal Data-Fostering Responsible Development And Adoption Of AI*. <https://www.pdpc.gov.sg/help-and-resources/2020/03/discussion-paper-artificial-intelligence-and-personal-data>
- Pirozzoli, A. (2024). *The Human-centric Perspective in the Regulation of Artificial Intelligence; The Human-centric Perspective in the Regulation of Artificial Intelligence*. 9(1), 105–116. <https://doi.org/10.15166/2499-8249/745>
- Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4, 100005. <https://doi.org/10.1016/j.jrt.2020.100005>
- Rožman, M., Oreški, D., & Tominc, P. (2023). Artificial-Intelligence-Supported Reduction of Employees' Workload to Increase the Company's Performance in Today's VUCA Environment. *Sustainability (Switzerland)*, 15(6). <https://doi.org/10.3390/su15065019>
- Selten, F., & Klievink, B. (2024). Organizing public sector AI adoption: Navigating between separation and integration.

- Government Information Quarterly*, 41(1). <https://doi.org/10.1016/j.giq.2023.101885>
- Soori, M., Jough, F. K. G., Dastres, R., & Arezoo, B. (2024). AI-Based Decision Support Systems in Industry 4.0, A Review. *Journal of Economy and Technology*. <https://doi.org/10.1016/j.ject.2024.08.005>
- Taherdoost, H. (2021). Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects Hamed Taherdoost. Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. In *International Journal of Academic Research in Management (IJARM)* (Vol. 2021, Issue 1). <https://hal.science/hal-03741847v1>
- United Nation. (2024). *Governing AI For Humanity*. <https://digitallibrary.un.org/record/4062495>.
- United Nations Educational, S. and C. O. (2021). *Certified Copy of the Recommendation on the Ethics of Artificial Intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Wadipalapa, R. P., Katharina, R., Nainggolan, P. P., Aminah, S., Apriani, T., Ma'rifah, D., & Anisah, A. L. (2024). An Ambitious Artificial Intelligence Policy in a Decentralised Governance System: Evidence From Indonesia. *Journal of Current Southeast Asian Affairs*, 43(1), 65–93. <https://doi.org/10.1177/18681034231226393>
- WHO. (2021). *Ethics and Governance of Artificial Intelligence for Health : WHO Guidance*. World Health Organization. <https://www.who.int/publications/i/item/9789240029200>
- Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., Liu, X., Wu, Y., Dong, F., Qiu, C. W., Qiu, J., Hua, K., Su, W., Wu, J., Xu, H., Han, Y., Fu, C., Yin, Z., Liu, M., ... Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. In *Innovation* (Vol. 2, Issue 4). Cell Press. <https://doi.org/10.1016/j.xinn.2021.100179>
- Yuan, L. (2023). *CHINA Promoting the Artificial Intelligence for Science approach*. <https://doi.org/10.1007/s00146-020-00992-2>
- Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Telecommunications Policy*. <https://doi.org/10.1016/j.telpol.2024.102851>
- Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3). <https://doi.org/10.1016/j.giq.2021.101577>