Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 2, No. 3, September 2023, pp. 147-154
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v2i3.482

STATE DIGITAL SOVEREIGNTY IN THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE WITHIN INDONESIA'S GOVERNMENT SYSTEM

Wiredarme

Institut Pemerintahan Dalam Negeri, Indonesia
Email: wiredarme@ipdn.ac.id

(Received: October 16, 2023; Revised: October 25, 2023; Published: September 20, 2023)

Abstract

This study examines state digital sovereignty in the governance of artificial intelligence within Indonesia's government system. The main objective is to analyze how the state can maintain effective control over AI infrastructure, public-sector data, and government AI systems while preserving constitutional democracy, citizens' rights, and public accountability. This research applies a qualitative legal method with normative-juridical, conceptual, and socio-legal approaches. The analysis is based on constitutional principles, statutory regulations, policy documents, and recent scholarly debates on AI governance, digital sovereignty, data sovereignty, and public-sector digital transformation. The findings show that Indonesia has developed important foundations for digital government through the Electronic-Based Government System, One Data Indonesia, the Personal Data Protection Law, and the National Strategy for Artificial Intelligence 2020–2045. Yet these instruments have not fully established a comprehensive framework for sovereign AI governance. The main risks include infrastructure dependency, weak control over public-sector data, vendor dominance, limited algorithmic accountability, and unclear responsibility for AI-based administrative decisions. This study argues that state digital sovereignty in AI governance requires strategic infrastructure control, public-sector data sovereignty, algorithmic accountability, meaningful human authority, and democratic oversight. The contribution of this study lies in framing AI governance not merely as a matter of technological innovation or administrative efficiency, but as a constitutional issue concerning the state's capacity to govern digital power in the public interest.

Keywords: artificial intelligence governance; digital sovereignty; public administration; state sovereignty; Indonesia.

1. INTRODUCTION

The expansion of artificial intelligence in government administration has transformed the meaning of state authority in the digital era. AI is no longer limited to technical automation or administrative efficiency; it has become part of the infrastructure through which the state collects data, classifies citizens, predicts risks, allocates services, and designs public policy. In this context, digital sovereignty refers to the state's capacity to exercise meaningful control over digital infrastructure, data flows, computational systems, and algorithmic decision-making processes. The issue becomes more complex when government AI systems depend on foreign cloud services, privately owned platforms, imported models, external vendors, or data-processing infrastructures located outside national jurisdiction. Sovereignty is no longer exercised only through territorial borders, but also through the ability of the state to govern strategic digital resources.

Indonesia provides a relevant case for examining this issue because its public administration is undergoing rapid digital transformation. The legal and policy basis for digital government can be seen in the Electronic-Based Government System framework, the One Data Indonesia policy, the Personal Data Protection Law, and the National Strategy for Artificial Intelligence 2020–2045. Official regulatory sources record Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System and Presidential Regulation No. 39 of 2019 on One Data Indonesia as key instruments for integrating digital governance and public-sector data management in Indonesia. The National Strategy for Artificial Intelligence 2020–2045 also identifies ethics and policy, talent development, infrastructure and data, and industrial research and innovation as strategic foundations for Indonesia's AI development. These instruments show that Indonesia has begun to build the normative and institutional architecture for digital government. The central problem is whether this architecture is sufficient to secure state control over AI systems used in government administration.

The constitutional relevance of digital sovereignty lies in the relationship between state authority, public interest, and citizens' rights. When AI is used in government systems, data are not merely administrative records; they become strategic assets that determine the quality of public decision-making. Government AI may process population data, health records, education data, welfare data, tax information, mobility patterns, biometric identifiers, and other

sensitive datasets. If these data are stored, processed, or modelled through infrastructures beyond effective state control, the government may lose the ability to guarantee confidentiality, accountability, continuity of service, and legal protection. In a constitutional state, digital sovereignty should not be understood as a justification for excessive surveillance or centralized control. It should be understood as the state's responsibility to ensure that AI governance remains subject to law, democratic accountability, human rights, public oversight, and national public interest.

Recent scholarship on digital sovereignty has developed important conceptual foundations for this study. Hummel et al. define data sovereignty as meaningful control over data by relevant agents, ranging from individuals to states [1]. Fratini explains digital sovereignty as a multidimensional and contested concept involving political authority, technological autonomy, and institutional capacity [2]. Gordon links digital sovereignty with digital infrastructure and future technological dependency [3]. Paulsson and Fred show that public authorities may attempt to reclaim digital capacity by developing applications and data arrangements that reduce dependence on private actors [4]. Lehuedé expands the discussion by connecting digital sovereignty with decolonial critique and unequal global data relations [5]. Prasad's study on India shows that state claims over data may strengthen national digital power, yet such claims may also create new risks of data extraction and state surveillance [6]. These studies are relevant because they demonstrate that digital sovereignty cannot be reduced to data localization; it concerns the broader question of who controls digital infrastructure, who benefits from data, and who is accountable for algorithmic power.

A second body of literature discusses AI governance in public administration. Madan and Ashok show that AI adoption in public administration creates ethical tensions related to transparency, fairness, privacy, accountability, and human rights [7]. Criado, Sandoval-Almazán, and Gil-Garcia argue that AI in public administration must be analyzed through actors, governance levels, and policy arrangements [8]. De Almeida and Dos Santos Júnior emphasize that AI governance in public organizations requires organizational structures, risk management, data governance, and accountability mechanisms [9]. Ahn and Chen find that AI-augmented public administration depends not only on technology, but also on government employees' willingness, institutional readiness, and organizational adaptation [10]. Van Noordt and Tangi connect AI capability with public value creation, showing that AI must be governed according to public-sector objectives rather than private-sector performance metrics [11]. De Bruijn, Warnier, and Janssen warn that explainable AI may create new problems when explanations are oversimplified, strategic, or detached from real accountability [12]. Gesk and Leyer show that citizens' acceptance of AI in public services depends on trust, perceived usefulness, and perceived legitimacy [13]. Roehl, Roehl and Crompvoets, Carlsson, Hirvonen, and Rizk and Lindgren also emphasize that automated decision-making changes administrative discretion, legal certainty, good administration, accountability, and the decision space between citizens and public officials [14]–[18]. These studies provide a strong foundation for AI governance, yet they rarely place public-sector AI within the constitutional theory of state sovereignty in the digital domain.

This article fills that gap by examining state digital sovereignty in the governance of artificial intelligence within Indonesia's government system. Its novelty lies in connecting AI governance with the constitutional concept of state sovereignty in the digital space. Unlike studies that focus mainly on ethical AI, administrative efficiency, data protection, or technical accountability, this article argues that AI governance in Indonesia must be assessed through the state's ability to control three strategic domains: digital infrastructure, public-sector data, and government AI systems. The objective of this study is to analyze how Indonesia can maintain sovereign authority over AI-based government systems while still protecting constitutional democracy, citizens' rights, legal accountability, and public interest. This study positions digital sovereignty not as technological nationalism, but as a constitutional requirement for ensuring that AI used by the government remains lawful, accountable, secure, and aligned with the purposes of the Indonesian state.

2. RESEARCH METHODS

This study uses a qualitative legal research method with a normative-juridical, conceptual, and socio-legal approach. The normative-juridical approach is used to examine the legal foundations of digital government, public-sector data management, personal data protection, and artificial intelligence governance in Indonesia. The conceptual approach is applied to clarify the relationship between state sovereignty, digital sovereignty, data sovereignty, and AI governance. The socio-legal approach is used to understand how legal norms operate within the practical context of Indonesia's digital government transformation, especially when public services increasingly rely on data infrastructures, automated systems, and AI-based administrative tools.

This research does not employ a quantitative model, statistical testing, or a specific AI algorithm. It also does not develop or evaluate a technical AI system. Instead, the study is designed as a descriptive-analytical legal study that evaluates how the state should control AI infrastructure, public-sector data, and government AI systems from the perspective of constitutional law and public governance. The main analytical concern is not whether AI is technically effective, but whether AI governance in Indonesia is compatible with the principles of state sovereignty, constitutional democracy, public accountability, legal certainty, data protection, and citizens' rights.

The case study of this research is Indonesia's government AI governance framework. Indonesia is selected because the country has developed several legal and policy instruments that are directly relevant to digital sovereignty,

including the Electronic-Based Government System, One Data Indonesia, the National Architecture of Electronic-Based Government, the Personal Data Protection Law, and the National Strategy for Artificial Intelligence 2020–2045. Presidential Regulation No. 95 of 2018 establishes the Electronic-Based Government System as a framework for integrated digital administration, while Presidential Regulation No. 39 of 2019 provides the legal basis for One Data Indonesia as a national data governance policy. Presidential Regulation No. 132 of 2022 further regulates the National Architecture of the Electronic-Based Government System. Law No. 27 of 2022 on Personal Data Protection recognizes personal data protection as part of constitutional protection and regulates data processing, data-subject rights, data-controller obligations, cross-border transfer, and sanctions.

The study also uses Indonesia's National Strategy for Artificial Intelligence 2020–2045 as an important policy document. The strategy sets a national direction for AI development and identifies ethics and policy, talent development, infrastructure and data, and industrial research and innovation as strategic components of Indonesia's AI ecosystem. It also places AI development within long-term national transformation toward Indonesia 2045. These policy materials are analyzed not as binding statutes, but as indicators of the state's strategic orientation in governing AI. Their relevance lies in showing how Indonesia frames AI as a national development instrument, while the legal question examined in this article is whether that orientation is supported by sufficient sovereign control over infrastructure, data, and public-sector AI systems.

Data collection is conducted through documentary research. The primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, Law No. 30 of 2014 on Government Administration, Law No. 11 of 2008 as amended by Law No. 19 of 2016 and Law No. 1 of 2024 on Electronic Information and Transactions, Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System, Presidential Regulation No. 39 of 2019 on One Data Indonesia, and Presidential Regulation No. 132 of 2022 on the National Architecture of the Electronic-Based Government System. These legal materials are used to examine the extent to which Indonesia's positive law provides a normative basis for state control over government AI systems, public-sector data, and strategic digital infrastructure.

The secondary data consist of peer-reviewed journal articles published mainly within the last five years on digital sovereignty, data sovereignty, AI governance, public-sector AI, automated decision-making, digital infrastructure, data protection, and algorithmic accountability. These sources are used to construct the theoretical framework and to compare Indonesia's legal position with broader international debates. The study also uses policy reports, official government documents, and institutional publications related to Indonesia's digital government and AI policy. These materials are selected based on relevance, credibility, recency, and their contribution to the discussion of sovereign control over AI systems in government.

The data are analyzed using qualitative legal analysis through three stages. First, the study identifies constitutional and statutory norms related to sovereignty, state authority, digital government, public data governance, personal data protection, and administrative accountability. Second, it maps the strategic domains of AI governance in the Indonesian government system, namely digital infrastructure, public-sector data, AI models, procurement arrangements, cloud dependency, cross-border data processing, cybersecurity, and institutional oversight. Third, it evaluates whether the existing Indonesian framework is sufficient to ensure state digital sovereignty over AI systems used in government administration.

The analytical framework of this study is built on the concept of state digital sovereignty. In this research, state digital sovereignty is understood as the state's legal, institutional, and technological capacity to exercise effective control over digital infrastructure, public-sector data, and AI systems used for governmental purposes. This concept is operationalized through five indicators: control over strategic digital infrastructure, control over public-sector data, accountability of AI systems, protection of citizens' rights, and institutional capacity to regulate external technology providers. These indicators are used to assess whether Indonesia's AI governance framework enables the state to act as a sovereign public authority in the digital domain, rather than as a passive user of systems controlled by private or foreign actors.

To strengthen validity, this study applies source triangulation and conceptual triangulation. Source triangulation is carried out by comparing constitutional provisions, statutory regulations, policy documents, and recent academic literature. Conceptual triangulation is conducted by combining perspectives from constitutional law, administrative law, data protection law, AI governance, and digital sovereignty studies. This approach is necessary because the issue of AI governance cannot be adequately analyzed through one legal field alone. It involves the relationship between state power, technology dependence, data control, private-sector involvement, and citizens' constitutional rights.

The limitation of this research is that it does not conduct fieldwork, interviews, or technical audits of specific AI systems used by Indonesian government institutions. The study is limited to normative, conceptual, and policy-based analysis. This limitation is appropriate because the main objective of the article is to develop a constitutional and legal framework for understanding state digital sovereignty in government AI governance. Future empirical studies may further examine how government agencies procure, deploy, monitor, and audit AI systems in specific sectors such as health, taxation, social assistance, immigration, public security, and smart-city governance.

3. RESULTS AND DISCUSSION

3.1. Indonesia's AI Governance Architecture and the Question of State Digital Sovereignty

The findings of this study show that Indonesia has begun to develop a legal and policy architecture for digital government, but this framework has not yet fully established a comprehensive model of state digital sovereignty over artificial intelligence. The existing framework is still fragmented across several regulatory instruments, including the Electronic-Based Government System, One Data Indonesia, personal data protection, electronic information and transactions, and the National Strategy for Artificial Intelligence. Presidential Regulation No. 95 of 2018 provides the foundation for the Electronic-Based Government System, while Presidential Regulation No. 39 of 2019 establishes One Data Indonesia as a national policy for improving data governance across public institutions. These regulations demonstrate Indonesia's commitment to digital government integration, but they do not yet specifically regulate sovereign control over AI infrastructure, AI models, algorithmic decision-making, or external technology dependency.

This finding indicates that Indonesia's current digital governance framework is still more focused on administrative integration than on sovereign AI governance. The SPBE framework aims to improve efficiency, interoperability, and integration of electronic-based government services. One Data Indonesia seeks to produce accurate, accountable, and interoperable public-sector data. These instruments are important, but AI governance requires additional layers of control because AI systems do not merely store or transmit data. They process data, generate classifications, produce predictions, recommend decisions, and may influence the exercise of public authority. In this sense, AI changes digital government from an information-management system into a decision-influencing system.

The National Strategy for Artificial Intelligence 2020–2045 provides a more direct policy orientation for AI development in Indonesia. It identifies ethics and policy, talent development, infrastructure and data, and industrial research and innovation as strategic components of the national AI ecosystem. Recent policy discussions also show that Indonesia has continued to develop a broader AI roadmap to strengthen infrastructure, investment, and AI adoption in strategic sectors. This indicates that AI is increasingly viewed as a national development instrument. Yet from the perspective of constitutional law, the central issue is not only whether Indonesia can adopt AI, but whether the state can exercise effective legal, institutional, and technological control over AI used in government administration.

The results of this study support the argument of Hummel et al. that data sovereignty is closely related to meaningful control over data by relevant agents, including the state [1]. In Indonesia's government system, this control must include the ability to determine where public-sector data are stored, who may access them, how they are processed, which AI models are used, how systems are audited, and who is legally responsible for algorithmic outputs. Fratini's view that digital sovereignty is multidimensional is also relevant because Indonesia's challenge is not limited to data localization [2]. It includes cloud dependency, vendor dependency, cybersecurity readiness, algorithmic transparency, procurement governance, and the institutional capacity of public agencies to understand and supervise AI systems.

This study also finds that Indonesia's AI governance still lacks an explicit constitutional doctrine connecting AI, sovereignty, and public authority. Existing regulations regulate electronic government, data management, personal data, and digital transactions, but they have not fully addressed AI as an instrument of state action. This regulatory gap may create uncertainty when AI systems are used in administrative services, public security, taxation, health, education, social assistance, immigration, or smart-city governance. If public agencies rely on AI systems developed, trained, hosted, or maintained by private or foreign actors without sufficient state control, the exercise of public authority may become technologically dependent on non-state actors.

This finding is consistent with Madan and Ashok, who argue that AI adoption in public administration raises challenges related to transparency, privacy, accountability, fairness, and institutional readiness [7]. It also aligns with Criado, Sandoval-Almazán, and Gil-Garcia, who emphasize that AI in public administration must be understood across multiple governance levels, including policy, organizational, and operational dimensions [8]. In the Indonesian context, those governance levels must be connected with state digital sovereignty. AI governance is not only about making public services smarter; it is about ensuring that the state remains capable of controlling the digital systems through which public authority is exercised.

3.2. Infrastructure, Data, and Vendor Dependency as Strategic Sovereignty Risks

The second finding of this study is that state digital sovereignty in government AI depends on control over three strategic domains: digital infrastructure, public-sector data, and AI systems. These domains are interconnected. Without infrastructure control, the state may become dependent on external cloud providers or computational services. Without data control, the state may lose authority over strategic public-sector datasets. Without AI system control, the state may not be able to explain, audit, correct, or take responsibility for algorithmic outputs.

In the first domain, infrastructure control is essential because AI requires large-scale computing capacity, secure data centers, interoperable systems, cloud architecture, and cybersecurity resilience. Indonesia's digital

government transformation has encouraged integration, but integration may also increase systemic vulnerability if infrastructure governance is weak. A centralized or interconnected system may improve efficiency, but it may also create broader risks if external vendors dominate the architecture, if cloud services operate beyond effective jurisdictional control, or if public institutions lack technical capacity to monitor system performance. Gordon's study on digital sovereignty and digital infrastructure is relevant because it shows that sovereignty in the digital era is strongly shaped by infrastructural dependency [3]. For Indonesia, the issue is not isolation from global technology providers, but the capacity to negotiate, regulate, audit, and secure technological arrangements that support public authority.

The second domain is public-sector data. AI systems require data as training material, operational input, and validation resources. In government administration, these data may include civil registration data, health data, education data, tax data, mobility data, welfare data, biometric data, and public service records. Law No. 27 of 2022 on Personal Data Protection has strengthened the legal basis for protecting personal data in Indonesia, particularly through obligations imposed on data controllers and processors. Yet personal data protection alone is not sufficient to establish state digital sovereignty. The state also needs a clear framework for public-sector data classification, data-sharing limits, cross-border transfer control, access authorization, data audit, and accountability for AI training and deployment.

This finding strengthens Prasad's argument that state claims over data can become a key element of digital sovereignty, but they may also generate risks when the state treats people primarily as data resources [6]. In Indonesia, digital sovereignty must not be interpreted as unlimited state control over citizens' data. Sovereignty must be balanced with constitutional rights, privacy, proportionality, and public accountability. If government AI governance emphasizes state control without rights protection, digital sovereignty may shift into digital domination. For that reason, the state must control public-sector data not to expand unchecked power, but to guarantee lawful, secure, accountable, and rights-respecting public administration.

The third domain is control over AI systems. AI governance requires the state to know how models are developed, what data are used, what assumptions shape the model, what risks may arise, and how decisions can be reviewed. This is particularly important when AI systems are procured from private vendors or built through public-private partnerships. Paulsson and Fred show that public authorities may attempt to regain digital capacity by developing applications and data arrangements that reduce dependency on private actors [4]. This finding is relevant for Indonesia because public-sector AI may be difficult to control if government institutions only act as users of proprietary systems without sufficient access to documentation, audit mechanisms, source logic, or model performance reports.

The discussion also relates to the problem of explainability. De Bruijn, Warnier, and Janssen warn that explainable AI may create new risks if explanations are superficial or detached from accountability [12]. This study finds that explainability in Indonesia's government AI system should not be understood merely as a technical feature. It must become an administrative-law requirement. Public agencies must be able to explain why an AI system is used, what role it plays in the decision-making process, what data it processes, what risks it creates, and how affected citizens can challenge the output. A state that cannot explain AI systems used in government cannot fully claim digital sovereignty over those systems.

The findings also show that vendor dependency may weaken democratic accountability. When public institutions depend heavily on private technology providers, responsibility may become blurred. A government agency may claim that a decision follows the system output, while the vendor may claim that it only provides technical support. This diffusion of responsibility is constitutionally problematic because public authority must remain accountable to law. Hirvonen's argument regarding accountability structures in automated public-sector decision-making supports this finding [17]. For Indonesia, AI procurement should include mandatory clauses on audit access, data ownership, model documentation, cybersecurity standards, data localization when necessary, human oversight, and public-sector responsibility for final decisions.

3.3. Toward a Constitutional Model of Sovereign AI Governance in Indonesia

The third finding of this study is that Indonesia needs a constitutional model of sovereign AI governance that integrates state authority, public accountability, and citizens' rights. Digital sovereignty should not be reduced to technological nationalism or protectionism. It should be understood as the state's capacity to ensure that AI systems used in government remain lawful, secure, explainable, accountable, and aligned with constitutional values. In this model, the state must control AI systems not because the state owns all technology, but because the state is responsible for every exercise of public authority carried out through digital systems.

This study proposes five elements of sovereign AI governance for Indonesia. First, strategic infrastructure control must be strengthened. Government AI systems should operate on infrastructure that meets national cybersecurity, data protection, continuity, and auditability standards. This does not require rejecting foreign technology providers, but it requires enforceable legal control over data storage, system access, incident response,

cloud governance, and service continuity. The state must avoid a condition where critical government AI systems depend on infrastructures that cannot be audited or governed under Indonesian law.

Second, public-sector data sovereignty must be institutionalized. One Data Indonesia provides an important foundation for data standardization and interoperability, yet AI governance requires additional safeguards for data use in model training, profiling, prediction, and decision support. Data used for government AI must be legally obtained, accurate, representative, secure, and proportionate to the public purpose pursued. Hummel et al. emphasize meaningful control as the core of data sovereignty [1]. In Indonesia, meaningful control should include citizens' rights over personal data and the state's duty to prevent misuse of public-sector data.

Third, algorithmic accountability must become a legal requirement in government AI deployment. Every AI system used by public institutions should have a clear accountability chain covering design, procurement, testing, deployment, monitoring, audit, and redress. De Almeida and Dos Santos Júnior argue that AI governance in public organizations requires structures for risk management, data governance, and accountability [9]. This finding supports the need for Indonesia to develop mandatory algorithmic impact assessment for high-risk AI systems in government. Such assessment should evaluate legality, rights impact, discrimination risk, cybersecurity vulnerability, explainability, human oversight, and institutional responsibility.

Fourth, human authority and administrative responsibility must remain central. AI may support government decisions, but it should not replace lawful administrative judgment in matters affecting citizens' rights, obligations, or access to public services. Roehl's work on automated decision-making and good administration shows that automation must be assessed through transparency, fairness, accountability, and administrative capability [14]. Carlsson also emphasizes that automated welfare and public-service decisions may threaten legal certainty when the decision-making process becomes opaque [16]. In Indonesia, this means public officials must remain responsible for final decisions, and citizens must have access to reasons, correction mechanisms, and remedies.

Fifth, democratic and constitutional oversight must be strengthened. AI governance should involve not only executive agencies and technical experts, but also legislative oversight, judicial review, audit institutions, data protection authorities, civil society, academia, and affected communities. Public trust in government AI cannot be built only through claims of efficiency. Gesk and Leyer show that citizens' acceptance of AI in public services depends on perceived legitimacy and trust [13]. In Indonesia, legitimacy requires transparency, public participation, rights protection, and clear accountability for harm caused by AI systems.

Based on these findings, this study formulates the following proposition: state digital sovereignty in AI governance exists only when Indonesia can exercise effective legal, institutional, and technological control over government AI infrastructure, public-sector data, and algorithmic systems while preserving constitutional rights and democratic accountability. This proposition extends previous studies on AI governance by linking the debate to sovereignty theory in the digital domain. It also extends digital sovereignty literature by showing that sovereignty is not only about data control or infrastructure independence, but also about the constitutional accountability of AI-based public authority.

The main implication of this study is that Indonesia should develop a specific legal and institutional framework for government AI governance. Such a framework should regulate AI risk classification, public-sector AI procurement, data governance for AI training and deployment, algorithmic impact assessment, auditability, explainability, human oversight, citizen remedies, and accountability for public institutions using AI systems. Without this framework, Indonesia may adopt AI in government while remaining dependent on infrastructures, data arrangements, and algorithmic systems that are not fully subject to sovereign public control.

4. CONCLUSION

This study concludes that the governance of artificial intelligence in Indonesia's government system must be understood as a matter of state digital sovereignty, not merely as a question of technological adoption, administrative modernization, or public-service efficiency. AI systems used by government institutions are closely connected with the exercise of public authority because they may process public-sector data, support administrative decisions, classify citizens, predict social risks, and influence policy implementation. For this reason, the state must retain effective legal, institutional, and technological control over AI infrastructure, data, and algorithmic systems used in public administration.

The main finding of this study shows that Indonesia has developed several important foundations for digital government governance, including the Electronic-Based Government System, One Data Indonesia, the Personal Data Protection Law, and the National Strategy for Artificial Intelligence 2020–2045. These instruments demonstrate the state's commitment to digital transformation. Yet they have not fully formed a comprehensive framework for sovereign AI governance. Existing regulations remain fragmented and are still more focused on electronic administration, data integration, and personal data protection than on direct control over government AI systems, algorithmic accountability, infrastructure dependency, and vendor responsibility.

The novelty of this study lies in connecting AI governance with the concept of state sovereignty in the digital domain. Previous studies have discussed AI in public administration mainly through the perspectives of transparency,

accountability, fairness, explainability, and administrative efficiency [7]–[18]. Other studies have examined digital sovereignty through data control, infrastructure dependency, platform power, and geopolitical competition [1]–[6]. This article contributes to those debates by arguing that government AI governance requires a constitutional understanding of sovereignty. In this perspective, digital sovereignty is not limited to data localization or technological independence, but includes the state's ability to ensure that AI-based public authority remains lawful, accountable, auditable, secure, and subject to citizens' rights.

The findings also show that Indonesia's main challenge is not simply whether the government should use AI, but how the state can prevent dependency on external infrastructures, private vendors, proprietary systems, and cross-border data-processing arrangements that may weaken public control. If government AI systems are developed, hosted, trained, or maintained by actors beyond effective state supervision, the state may lose the ability to explain decisions, audit risks, protect strategic data, guarantee cybersecurity, and assign legal responsibility for algorithmic harm. Such dependency may gradually weaken the substance of sovereignty, even when formal legal authority remains in the hands of the state.

This study argues that sovereign AI governance in Indonesia should be built on five core elements: strategic infrastructure control, public-sector data sovereignty, algorithmic accountability, meaningful human authority, and democratic oversight. These elements must operate together. Infrastructure control without rights protection may lead to excessive state control. Data sovereignty without accountability may create risks of surveillance. AI innovation without human oversight may weaken administrative responsibility. Digital sovereignty must therefore be placed within the framework of constitutional democracy, where state control over AI is directed toward public interest, legal certainty, rights protection, and accountable governance.

The lack of this study is that it does not conduct empirical fieldwork or technical audits of specific AI systems currently used by Indonesian government institutions. The analysis is limited to normative, conceptual, and policy-based examination. Future research should investigate concrete AI implementation in specific sectors such as taxation, immigration, population administration, health services, social assistance, smart cities, public security, and judicial administration. Further studies may also examine public procurement contracts, cloud-service dependency, cross-border data processing, algorithmic impact assessments, and the institutional capacity of government agencies to audit AI systems. Comparative research with countries that have adopted specific public-sector AI regulations would also be valuable to develop a more operational model of sovereign, accountable, and rights-based AI governance for Indonesia.

REFERENCES

[1] P. Hummel, M. Braun, M. Tretter, and P. Dabrock, "Data sovereignty: A review," *Big Data & Society*, vol. 8, no. 1, 2021, doi: 10.1177/2053951720982012.

[2] S. Fratini, "Digital sovereignty: A descriptive analysis and a critical evaluation," *Digital Society*, vol. 3, 2024, doi: 10.1007/s44206-024-00146-7.

[3] G. Gordon, "Digital sovereignty, digital infrastructures, and quantum horizons," *AI & Society*, vol. 39, no. 1, pp. 125–137, 2024, doi: 10.1007/s00146-023-01729-7.

[4] A. Paulsson and M. Fred, "Making apps, owning data: Digital sovereignty and public authorities' arrangements to 'byte' back," *Organization*, vol. 32, no. 8, 2024, doi: 10.1177/13505084241246073.

[5] S. Lehuedé, "An alternative planetary future? Digital sovereignty frameworks and the decolonial option," *Big Data & Society*, vol. 11, no. 1, 2024, doi: 10.1177/20539517231221778.

[6] R. Prasad, "People as data, data as oil: The digital sovereignty of the Indian state," *Information, Communication & Society*, vol. 25, no. 6, pp. 801–815, 2022, doi: 10.1080/1369118X.2022.2056498.

[7] R. Madan and M. Ashok, "AI adoption and diffusion in public administration: A systematic literature review and future research agenda," *Government Information Quarterly*, vol. 40, no. 1, 101774, 2023, doi: 10.1016/j.giq.2022.101774.

[8] J. I. Criado, R. Sandoval-Almazán, and J. R. Gil-Garcia, "Artificial intelligence and public administration: Understanding actors, governance, and policy from micro, meso, and macro perspectives," *Public Policy and Administration*, vol. 40, no. 2, pp. 173–184, 2025, doi: 10.1177/09520767241272921.

[9] P. G. R. de Almeida and C. D. dos Santos Júnior, "Artificial intelligence governance: Understanding how public organizations implement it," *Government Information Quarterly*, vol. 42, no. 1, 102003, 2025, doi: 10.1016/j.giq.2024.102003.

[10] M. J. Ahn and Y.-C. Chen, "Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government," *Government Information Quarterly*, vol. 39, no. 2, 101664, 2022, doi: 10.1016/j.giq.2021.101664.

[11] C. van Noordt and L. Tangi, "The dynamics of AI capability and its influence on public value creation of AI within public administration," *Government Information Quarterly*, vol. 40, no. 4, 101860, 2023, doi: 10.1016/j.giq.2023.101860.

[12] H. de Bruijn, M. Warnier, and M. Janssen, "The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making," *Government Information Quarterly*, vol. 39, no. 2, 101666, 2022, doi: 10.1016/j.giq.2021.101666.
[13] T. S. Gesk and M. Leyer, "Artificial intelligence in public services: When and why citizens accept its usage," *Government Information Quarterly*, vol. 39, no. 3, 101704, 2022, doi: 10.1016/j.giq.2022.101704.
[14] U. B. U. Roehl, "Automated decision-making and good administration: Views from inside the government machinery," *Government Information Quarterly*, vol. 40, no. 4, 101864, 2023, doi: 10.1016/j.giq.2023.101864.
[15] U. Roehl and J. Crompvoets, "Inside algorithmic bureaucracy: Disentangling automated decision-making and good administration," *Public Policy and Administration*, vol. 40, no. 2, pp. 322–350, 2025, doi: 10.1177/09520767231197801.
[16] V. Carlsson, "Legal certainty in automated decision-making in welfare services," *Public Policy and Administration*, vol. 40, no. 2, 2025, doi: 10.1177/09520767231202334.
[17] H. Hirvonen, "Just accountability structures: A way to promote the safe use of automated decision-making in the public sector," *AI & Society*, vol. 39, pp. 155–167, 2024, doi: 10.1007/s00146-023-01731-z.
[18] A. Rizk and I. Lindgren, "Automated decision-making in public administration: Changing the decision space between public officials and citizens," *Government Information Quarterly*, 2025, doi: 10.1016/j.giq.2025.102061.
[19] T. Saheb and T. Saheb, "Topical review of artificial intelligence national policies: A mixed method analysis," *Technology in Society*, vol. 74, 102316, 2023, doi: 10.1016/j.techsoc.2023.102316.
[20] J. Laux, S. Wachter, and B. Mittelstadt, "Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk," *Regulation & Governance*, vol. 18, no. 1, pp. 3–32, 2024, doi: 10.1111/rego.12512.