Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 3, No. 3, September 2024, pp. 163-171
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v3i3.480

CONSTITUTIONAL ACCOUNTABILITY OF THE GOVERNMENT FOR MACHINE LEARNING-BASED SYSTEM ERRORS IN DIGITAL PUBLIC SERVICES

Wiredarme

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

(Received: October 12, 2024; Revised: October 27, 2024; Accepted: September 24, 2024)

Abstract

This study examines the constitutional accountability of the government for machine learning-based system errors in Indonesia's digital public services. The objective is to analyze how state responsibility should be formulated when digital systems misread data, reject applications, delay access, produce inaccurate classifications, or incorrectly process citizens' rights. This research applies a qualitative legal method with normative-juridical, conceptual, and socio-legal approaches. The analysis is based on constitutional norms, public service law, government administration law, personal data protection law, electronic-based government regulations, and recent scholarly debates on automated decision-making and public-sector AI governance. The findings show that machine learning-based errors cannot be treated as ordinary technical failures when they affect citizens' access to public services. Such errors must be understood as failures of public authority because the system operates within the institutional responsibility of the state. Indonesia already has legal foundations for public service, administrative responsibility, digital government, and personal data protection, but it lacks a specific accountability framework for machine learning-based public service errors. This study proposes the concept of state constitutional responsibility for governmental technology failure, consisting of preventive, explanatory, corrective, institutional, and remedial accountability. The contribution of this study lies in framing machine learning errors in public services as constitutional accountability issues, not merely as technical, administrative, or contractual problems.

Keywords: constitutional accountability; digital public services; machine learning; public administration; state responsibility.

1. INTRODUCTION

The use of machine learning in digital public services has transformed the relationship between citizens and the state. Public administration is no longer carried out only through direct bureaucratic judgment, written documents, and face-to-face verification, but also through automated systems that classify data, detect risks, verify applications, recommend decisions, and process access to public rights. In this context, machine learning may support faster, more consistent, and more efficient public services. At the same time, it may also create new forms of administrative failure when the system misreads citizen data, rejects valid applications, produces inaccurate classifications, or processes rights without adequate legal review. Such errors are not ordinary technical failures because they may affect citizens' access to identity documents, education, health care, social assistance, taxation services, licensing, population administration, and other constitutionally relevant public services.

In Indonesia, the constitutional dimension of this issue is closely related to the state's obligation to provide lawful, fair, accountable, and non-discriminatory public services. The 1945 Constitution guarantees equality before the law, legal certainty, protection of human dignity, and the right of citizens to obtain public services as part of the broader responsibility of the constitutional state. This obligation is strengthened by Law No. 25 of 2009 on Public Services, which regulates the rights and obligations of public service providers and users, including service standards, complaint mechanisms, public participation, and administrative sanctions. This framework becomes crucial when digital public services rely on machine learning because citizens may suffer harm not from direct human misconduct, but from system design, data errors, model bias, automation failure, or weak institutional supervision.

Indonesia's digital government transformation has created an institutional basis for technology-based administration. Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System establishes the framework for integrated digital administration, while Law No. 27 of 2022 on Personal Data Protection regulates personal data rights, data-controller obligations, data processing, cross-border transfer, sanctions, and dispute settlement. Law No. 30 of 2014 on Government Administration is also relevant because it provides the legal basis for government decisions and actions, good governance, protection for citizens, and responsibility for administrative errors. These instruments show that Indonesia already has norms on public service, digital government, personal data,

and administrative responsibility. The unresolved question is how these norms should apply when harm is caused by a machine learning-based public service system.

Recent literature has examined automated decision-making in public administration from the perspective of good administration, legality, and institutional governance. Roehl argues that automated administrative decision-making may support good administration, while also creating risks for carefulness, individual rights, professionalism, trustworthiness, responsiveness, and empowerment [1]. Roehl and Hansen further show that automated administrative decision-making produces both synergies and trade-offs with good governance values [2]. Roehl and Crompvoets explain that algorithmic bureaucracy changes how administrative discretion is organized inside public institutions [3]. Carlsson's study on automated decision-making in welfare services demonstrates that legal certainty becomes fragile when citizens cannot understand how automated systems influence administrative outcomes [4]. Hirvonen emphasizes the need for accountability structures to promote the safe use of automated decision-making in the public sector [5]. Rizk and Lindgren also show that automated decision-making changes the decision space between public officials and citizens [6]. These studies provide an important foundation, yet they mainly examine automated decision-making through administrative values and institutional governance rather than through the constitutional responsibility of the state for technological failure.

A second body of scholarship focuses on AI governance, trustworthiness, explainability, public-sector adoption, discretion, and liability. Madan and Ashok identify transparency, fairness, privacy, accountability, and human rights as central issues in AI adoption in public administration [7]. Criado, Sandoval-Almazán, and Gil-Garcia explain that AI in public administration must be understood through actors, governance levels, and policy arrangements [8]. De Almeida and Dos Santos Júnior show that public organizations require governance structures, risk management, and accountability mechanisms to implement AI responsibly [9]. Ahn and Chen highlight the role of institutional readiness and government employees' willingness in AI-augmented public administration [10]. Van Noordt and Tangi connect AI capability with public value creation in the public sector [11]. De Bruijn, Warnier, and Janssen warn that explainable AI may produce superficial explanations when not connected with real accountability [12]. Gesk and Leyer find that citizens' acceptance of AI in public services depends on trust and perceived legitimacy [13]. Agbabiaka, Ojo, and Connolly identify trustworthiness requirements for AI-enabled automated decision-making, including accountability, transparency, context sensitivity, feedback, and policy learning [14]. Montagnani, Najjar, and Davola examine AI liability debates and show that legal responsibility becomes complex when harm is produced through opaque and technically complex systems [15]. Guenduez and Mergel add that algorithmic systems in the public sector may reshape discretion and administrative values, especially when public officials rely on algorithmic recommendations in decision-making processes [16]. Tummers and Rocco further argue that artificial intelligence changes the meaning of discretion in public management because administrative judgment may become mediated by technical systems [17]. Veale and Brass also show that public-sector machine learning raises foundational questions about public management, accountability, and the institutional capacity of government to control algorithmic systems [18]. These studies are directly relevant, but they have not sufficiently developed a constitutional model of government responsibility for machine learning errors in Indonesia's digital public services.

This article fills that gap by examining constitutional accountability of the government for machine learning-based system errors in digital public services**.** Its novelty lies in offering the concept of state constitutional responsibility for governmental technology failure. Unlike studies that discuss AI mainly as an ethical, administrative, technical, or managerial governance issue, this article argues that errors in machine learning-based public services must be treated as failures of public authority when they affect citizens' rights. The objective of this study is to analyze how the Indonesian government should be constitutionally accountable when a digital system misreads, rejects, delays, or incorrectly processes citizens' rights. The study positions machine learning not as an autonomous actor that can absorb legal blame, but as an instrument of state administration whose risks must remain attached to public officials and public institutions. The core argument is that digital public service innovation is constitutionally legitimate only when citizens retain the right to explanation, correction, human review, complaint, remedy, and compensation for harm caused by machine learning-based administrative errors.

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 constitutional and statutory foundations of government responsibility in digital public services, especially when public authorities use machine learning-based systems to process citizens' rights. The conceptual approach is applied to construct the idea of state constitutional responsibility for governmental technology failure**.** The socio-legal approach is used to understand how legal responsibility should operate in the practical context of digital public service delivery, where administrative decisions may be influenced by data processing, algorithmic classification, automated verification, and machine learning-based recommendations.

This research does not employ a quantitative method, statistical testing, or technical experimentation with a specific machine learning algorithm. It also does not train, evaluate, or audit a particular AI model used by a

government institution. Instead, this study is designed as a descriptive-analytical legal research that examines how legal responsibility should be formulated when machine learning-based public service systems make errors that affect citizens. The central issue is not whether machine learning is technically accurate, but how the state must remain accountable when technological systems misread data, reject applications, delay services, generate inaccurate classifications, or process citizens' rights unlawfully.

The case study of this research is Indonesia's digital public service system, particularly public services that are increasingly connected with electronic-based government, personal data processing, and automated administrative mechanisms. Indonesia is selected because the country already has several relevant legal instruments for digital public administration. Law No. 25 of 2009 on Public Services regulates service standards, rights and obligations, public participation, complaint resolution, and sanctions in public service delivery. Presidential Regulation No. 95 of 2018 establishes the Electronic-Based Government System as the national framework for integrated digital government. Law No. 27 of 2022 on Personal Data Protection regulates data-subject rights, data-controller obligations, data processing, transfer of personal data, sanctions, and dispute settlement. Law No. 30 of 2014 on Government Administration provides the legal basis for government decisions, government actions, good governance principles, and legal protection for citizens in administrative processes.

Data collection is conducted through documentary research. The primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law No. 25 of 2009 on Public Services, Law No. 30 of 2014 on Government Administration, Law No. 27 of 2022 on Personal Data Protection, Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System, Presidential Regulation No. 132 of 2022 on the National Architecture of Electronic-Based Government System, and relevant regulations concerning electronic systems and public administration. Presidential Regulation No. 132 of 2022 is included because it regulates the national architecture of SPBE, including policy direction, strategic initiatives, architecture framework, architecture domains, and references for national digital government development.

Secondary legal materials consist of peer-reviewed journal articles published mainly within the last five years on automated decision-making, machine learning in public administration, algorithmic accountability, digital public services, explainable AI, public-sector AI governance, AI liability, administrative discretion, and good administration. These materials are used to build the theoretical foundation and to compare the Indonesian case with broader international debates. The study also uses official government documents, policy reports, and institutional publications to understand the direction of Indonesia's digital government transformation.

The data are analyzed using qualitative legal analysis through four stages. First, the study identifies constitutional norms and statutory provisions related to public service rights, legal certainty, equality before the law, government responsibility, personal data protection, and good administration. Second, it maps possible forms of machine learning-based system errors in digital public services, including data misreading, false rejection, inaccurate risk scoring, wrongful classification, delayed processing, and automated denial of access to public services. Third, it evaluates whether existing Indonesian legal instruments are sufficient to assign responsibility when such errors occur. Fourth, it formulates a constitutional accountability framework that places responsibility on public institutions rather than on technology as an autonomous actor.

The analytical framework is built on the concept of constitutional accountability for technological failure. In this study, this concept refers to the duty of the state to remain legally responsible when digital systems used in public administration cause rights-based harm to citizens. This responsibility includes the obligation to prevent errors through proper system design, data governance, human supervision, risk assessment, and audit mechanisms. It also includes the obligation to respond to errors through explanation, correction, complaint handling, administrative review, compensation, and institutional evaluation. The framework assumes that machine learning is only an instrument of public authority. For that reason, government institutions cannot avoid responsibility by arguing that harm was caused by technical error, vendor failure, model limitation, or system automation.

To maintain the validity of the analysis, this study applies source triangulation and conceptual triangulation. Source triangulation is conducted by comparing constitutional provisions, statutes, government regulations, official policy documents, and recent academic literature. Conceptual triangulation is conducted by combining constitutional law, administrative law, public service law, personal data protection, and AI governance perspectives. This combination is necessary because machine learning errors in digital public services involve more than one legal dimension. They concern the legality of administrative action, the protection of personal data, the quality of public service, the allocation of institutional responsibility, and citizens' access to remedies.

The limitation of this research is that it does not conduct empirical interviews with citizens, public officials, or technology providers. It also does not examine the source code or performance of a particular machine learning system used in Indonesian public administration. This limitation is acceptable because the study aims to develop a normative and conceptual model of government responsibility. Future empirical research may test this framework by examining specific digital public services in sectors such as population administration, licensing, taxation, health care, social assistance, immigration, education, or smart-city governance.

3. RESULTS AND DISCUSSION

3.1. Machine Learning-Based Errors as Failures of Public Authority

The first finding of this study shows that errors produced by machine learning-based systems in digital public services cannot be treated as ordinary technical defects. In the context of Indonesian public administration, digital systems used by government agencies are part of the exercise of public authority. When such systems misread citizen data, reject a valid application, classify a person incorrectly, delay the processing of public service rights, or generate an inaccurate administrative recommendation, the error has legal and constitutional consequences. The problem is not limited to software malfunction, but concerns the state's obligation to ensure lawful, fair, accountable, and rights-based public service delivery.

This finding is particularly relevant to Indonesia because public service delivery is legally framed as a state obligation. Law No. 25 of 2009 on Public Services regulates service standards, rights and obligations, public participation, complaint settlement, and sanctions in public service administration. In this framework, machine learning-based public service systems must be placed under the responsibility of public service providers. The state cannot separate digital errors from public accountability simply because the immediate cause of harm appears to be technical. If the system is used by a public institution, its consequences remain part of government responsibility.

This study also finds that machine learning changes the structure of administrative error. In conventional public services, error may arise from human negligence, abuse of authority, lack of information, or failure to follow procedure. In machine learning-based services, error may arise from biased training data, incorrect model assumptions, poor system integration, incomplete personal data, inaccurate risk scoring, weak validation mechanisms, or overreliance on automated outputs. This supports Roehl's argument that automated decision-making must be assessed through the principles of good administration because it may affect carefulness, individual rights, professionalism, responsiveness, and public trust [1]. Roehl and Hansen also show that automated administrative decision-making may create trade-offs between efficiency and good governance values [2].

The Indonesian case demonstrates that this issue is constitutionally important because public service errors may directly affect citizens' rights. A wrongful rejection in a population administration system may limit access to education, health care, banking, voting, or social assistance. An incorrect classification in a licensing system may prevent a citizen or business from obtaining lawful administrative approval. A misread record in taxation, immigration, health insurance, or social protection may create burdens that citizens cannot easily challenge. In such circumstances, machine learning error becomes a constitutional issue because it may interfere with legal certainty, equality before the law, personal data protection, and access to public services.

This study strengthens Carlsson's finding that automated decision-making may weaken legal certainty when citizens cannot understand how administrative outcomes are produced [4]. It also supports Rizk and Lindgren's argument that automation changes the decision space between citizens and public officials [6]. In Indonesia, this change may become more problematic when citizens face digital systems without clear explanation, human review, or effective complaint channels. Public officials may depend on system outputs, while citizens may not know how to correct the data or challenge the classification. The result is an imbalance of authority between the digital state and the citizen.

The main implication is that machine learning-based public service errors must be conceptualized as failures of public authority when they affect rights, obligations, or access to services. The government remains constitutionally accountable because machine learning is only an instrument of administration. It does not possess legal authority, public mandate, or constitutional responsibility. Public institutions that design, procure, deploy, or rely on machine learning systems must remain responsible for their consequences.

3.2. Legal Gaps in Assigning Responsibility for Machine Learning Errors in Indonesia

The second finding of this study shows that Indonesia already has important legal instruments for public service, administrative responsibility, digital government, and personal data protection, but these instruments have not yet produced a specific accountability model for machine learning-based system errors. Law No. 30 of 2014 on Government Administration provides the legal basis for government decisions, government actions, good governance, and legal protection for citizens in administrative processes. The official legal database describes this law as a foundation for improving good governance and providing legal protection for citizens and government officials. Yet this law was not designed specifically for algorithmic or machine learning-based decision support systems.

Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System provides the framework for digital government integration in Indonesia. Presidential Regulation No. 132 of 2022 further regulates the national architecture of SPBE, including policy direction, architecture framework, architecture domains, and strategic initiatives for national digital government development. These regulations are significant because they create the institutional basis for digital public administration. Yet they remain primarily oriented toward integration, interoperability, architecture, and digital transformation. They do not explicitly regulate how responsibility should be assigned when machine learning-based systems produce harmful administrative errors.

Law No. 27 of 2022 on Personal Data Protection also provides an important foundation. It regulates personal data principles, types of personal data, rights of data subjects, obligations of data controllers and processors, data transfer, sanctions, institutional arrangements, dispute settlement, and criminal provisions. The official legal database also explains that personal data protection is intended to guarantee the constitutional rights of data subjects. This law is highly relevant because many machine learning errors originate from inaccurate, incomplete, excessive, or unlawfully processed data. Yet data protection alone cannot fully answer the problem of public service error. A citizen may suffer harm not only because personal data are misused, but because the government uses flawed data or automated classification to process a public right.

This study identifies four accountability gaps in the Indonesian framework. First, there is no explicit obligation for public agencies to disclose when machine learning is used in digital public services. Citizens may not know whether their application, complaint, eligibility, or administrative status has been influenced by algorithmic processing. Second, there is no specific standard requiring algorithmic impact assessment before machine learning systems are deployed in rights-sensitive public services. Third, there is no clear legal rule requiring meaningful human review when a machine learning output negatively affects a citizen. Fourth, there is no specific remedial mechanism for citizens harmed by algorithmic error, especially where harm arises from a combination of data error, system design, vendor failure, and administrative reliance.

These findings are consistent with Madan and Ashok, who identify transparency, fairness, privacy, accountability, and human rights as major challenges in AI adoption within public administration [7]. They also align with De Almeida and Dos Santos Júnior, who argue that public organizations need governance structures, risk management, and accountability mechanisms to implement AI responsibly [9]. In the Indonesian case, the challenge is not the absence of legal norms altogether, but the absence of a specific bridge between existing administrative-law responsibility and machine learning-based public service failure.

The study also finds that vendor involvement may complicate accountability. Public institutions may procure digital systems from private technology providers, including vendors that design models, manage infrastructure, process data, or maintain platforms. When harm occurs, the government may argue that the error originated from the system, while the vendor may argue that it only followed technical specifications. This diffusion of responsibility is constitutionally unacceptable because citizens interact with the state, not with an invisible algorithm or private contractor. Hirvonen's argument on the need for just accountability structures in automated public-sector decision-making is directly relevant here [5]. Accountability must remain attached to the public institution, even when technical work is outsourced.

The discussion also relates to the problem of discretion. Guenduez and Mergel show that algorithms in the public sector can reshape administrative discretion and public values [16]. Tummers and Rocco also argue that artificial intelligence changes the meaning of discretion in public management [17]. In Indonesia, machine learning may shift discretion from frontline public officials to system designers, data engineers, procurement teams, and institutional managers. If this shift is not regulated, responsibility becomes difficult to locate. The state may appear to act through a digital system, while no official actor clearly owns the consequences of the system's output.

3.3. Constitutional Accountability Framework for Governmental Technology Failure

The third finding of this study is that Indonesia needs a constitutional accountability framework for machine learning-based errors in digital public services. This framework should be built on the principle that technology used by the government is never outside constitutional responsibility. Machine learning may support public administration, but it cannot replace legal authority, human judgment, institutional accountability, or citizens' right to remedy. The government remains responsible because the system operates within the state's administrative structure and affects citizens through public power.

This study proposes five elements of constitutional accountability for governmental technology failure. First, preventive accountability must be established before machine learning systems are deployed. Public agencies should be required to conduct legal risk assessment, data quality assessment, bias testing, cybersecurity review, and algorithmic impact assessment for systems that affect citizens' rights or access to essential public services. This element responds to Agbabiaka, Ojo, and Connolly's finding that trustworthy AI-enabled automated decision-making requires accountability, transparency, context sensitivity, feedback mechanisms, and policy learning [14].

Second, explanatory accountability must be guaranteed. Citizens should have the right to know whether machine learning was used, what role the system played, what data were processed, and why a particular output affected their service result. This does not require the government to disclose every technical detail of a model, but it requires understandable reasons that allow citizens to identify possible errors and seek correction. De Bruijn, Warnier, and Janssen warn that explainable AI may become superficial when explanation is not connected to real accountability [12]. For Indonesia, explainability must be treated as an administrative-law requirement, not merely as a technical feature.

Third, corrective accountability must be built into every machine learning-based digital public service. Citizens must be able to correct personal data, submit additional evidence, request human review, and challenge

automated or semi-automated classifications. This is essential because machine learning systems may misread social context, local conditions, identity changes, household status, health conditions, economic vulnerability, or administrative records. Gesk and Leyer show that public acceptance of AI in public services depends on trust and perceived legitimacy [13]. A system that does not provide correction and review mechanisms will be perceived not as efficient, but as arbitrary.

Fourth, institutional accountability must remain with the public agency. Even when a machine learning system is developed or maintained by a private vendor, the government institution using the system must remain legally responsible to citizens. Vendor contracts may regulate internal liability between the state and private provider, but they cannot eliminate the state's public responsibility. This point is consistent with Montagnani, Najjar, and Davola's discussion of the complexity of AI liability in technically opaque systems [15]. In public administration, such complexity cannot be used to weaken citizens' remedies. The state must ensure that procurement contracts contain audit rights, documentation duties, data ownership rules, cybersecurity obligations, error-reporting mechanisms, and liability clauses.

Fifth, remedial accountability must provide effective remedies for citizens. Remedies should include explanation, correction, administrative review, restoration of service, compensation where harm is proven, and institutional evaluation to prevent repeated failure. Public service complaint mechanisms under Law No. 25 of 2009 are a necessary starting point, but they should be adapted to digital and machine learning-based public service contexts. Without a specific remedial pathway, citizens may face a procedural dead end: the system rejects them, the officer cannot explain why, and the institution treats the output as final.

This framework extends previous studies on automated decision-making and AI governance. Roehl and Crompvoets explain how algorithmic bureaucracy changes administrative structures [3], while Veale and Brass show that public-sector machine learning raises foundational questions about public management and institutional capacity [18]. This study contributes by arguing that those administrative and managerial questions must be elevated into constitutional accountability. When digital public service failure harms citizens, the issue is not only whether the system should be improved. The deeper issue is whether the state has fulfilled its constitutional duty to protect citizens from unlawful, opaque, and unreviewable exercises of public power.

Based on these findings, this study formulates the following proposition: machine learning-based errors in digital public services constitute governmental accountability problems when they affect citizens' rights, obligations, or access to public services. The state cannot avoid responsibility by attributing harm to system error, model limitation, data defect, or vendor failure. A constitutional state must ensure that every digital public service system remains explainable, reviewable, correctable, and accountable. In Indonesia, this requires the development of specific regulations on algorithmic impact assessment, human oversight, administrative remedies, and institutional responsibility for machine learning-based public services.

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 machine learning-based errors in Indonesia's digital public services must be understood as a matter of constitutional accountability, not merely as technical malfunction or administrative inconvenience. When a public service system misreads data, rejects an application, delays access, produces inaccurate classification, or incorrectly processes citizens' rights, the consequences are directly connected with the exercise of public authority. Since machine learning systems used in public services operate within the institutional authority of the state, their errors remain part of government responsibility. Technology cannot be treated as an autonomous actor that absorbs legal blame.

The main finding of this study shows that Indonesia already has several important legal foundations for public service, government administration, digital government, and personal data protection. Law No. 25 of 2009 on Public Services, Law No. 30 of 2014 on Government Administration, Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System, and Law No. 27 of 2022 on Personal Data Protection provide a normative basis for legality, service standards, complaint mechanisms, data protection, and administrative responsibility. Yet these instruments have not fully established a specific accountability model for machine learning-based errors in digital public services. The existing framework still lacks explicit rules on algorithmic disclosure, impact assessment, meaningful human review, correction mechanisms, and remedies for citizens harmed by system-based decisions.

The novelty of this study lies in offering the concept of state constitutional responsibility for governmental technology failure. Previous studies have discussed automated decision-making and AI governance mainly through the perspectives of good administration, transparency, explainability, institutional readiness, public trust, and legal liability [1]–[18]. This article contributes to that debate by placing machine learning-based public service errors within the constitutional relationship between the state and citizens. In this perspective, the main issue is not only whether AI systems are accurate or efficient, but whether citizens remain protected when those systems affect their rights, obligations, and access to public services.

The findings also show that machine learning changes the structure of administrative responsibility. Errors may no longer originate only from individual officers, but also from biased data, flawed model design, poor system integration, vendor dependency, weak institutional supervision, or excessive reliance on automated outputs. This condition may blur responsibility if the legal framework does not clearly assign accountability to public institutions. For that reason, the government cannot avoid responsibility by arguing that harm was caused by technical error, data defect, model limitation, or third-party vendor failure. In a constitutional state, public institutions remain responsible because they decide to procure, deploy, supervise, and rely on digital systems in delivering public services.

This study proposes that constitutional accountability for governmental technology failure should include five elements: preventive accountability, explanatory accountability, corrective accountability, institutional

accountability, and remedial accountability. Preventive accountability requires legal risk assessment, data-quality assessment, bias testing, cybersecurity review, and algorithmic impact assessment before machine learning systems are used. Explanatory accountability requires the government to provide understandable reasons when system outputs affect citizens. Corrective accountability requires mechanisms for data correction, human review, and objection. Institutional accountability ensures that responsibility remains with public agencies, even when systems are developed by private vendors. Remedial accountability requires effective remedies, including service restoration, administrative review, compensation where appropriate, and institutional evaluation.

The practical implication of this study is that Indonesia needs a more specific legal and institutional framework for machine learning-based public services. Such a framework should regulate the use of AI in rights-sensitive public services, require algorithmic impact assessments, mandate human oversight, clarify institutional responsibility, and guarantee citizens' access to explanation, correction, complaint, and remedy. Digital public service innovation must not weaken citizens' constitutional protection. It must strengthen public accountability, legal certainty, and trust in government.

The limitation of this study is that it does not conduct empirical fieldwork or technical audits of specific machine learning systems used by Indonesian government institutions. The analysis is limited to normative, conceptual, and policy-based examination. Future research should examine concrete cases of machine learning or automated systems in Indonesian public services, such as population administration, taxation, social assistance, health insurance, licensing, immigration, education, and smart-city governance. Further studies may also involve interviews with citizens, public officials, system developers, and oversight institutions to assess how accountability mechanisms operate in practice. Comparative studies with countries that have adopted AI liability rules or public-sector algorithmic accountability frameworks would also help develop a more operational model for Indonesia.

REFERENCES

[1] 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.

[2] U. B. U. Roehl and M. B. Hansen, "Automated, administrative decision-making and good governance: Synergies, trade-offs, and limits," *Public Administration Review*, vol. 84, no. 6, pp. 1185–1198, 2024, doi: 10.1111/puar.13799.

[3] 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.

[4] V. Carlsson, "Legal certainty in automated decision-making in welfare services," *Public Policy and Administration*, vol. 40, no. 2, pp. 302–321, 2025, doi: 10.1177/09520767231202334.

[5] 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.

[6] 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.

[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] O. Agbabiaka, A. Ojo, and N. Connolly, "Requirements for trustworthy AI-enabled automated decision-making in the public sector: A systematic review," *Technological Forecasting and Social Change*, vol. 215, 124076, 2025, doi: 10.1016/j.techfore.2025.124076.
[15] M. L. Montagnani, M.-C. Najjar, and A. Davola, "The EU regulatory approach(es) to AI liability, and its application to the financial services market," *Computer Law & Security Review*, vol. 53, 105984, 2024, doi: 10.1016/j.clsr.2024.105984.
[16] A. Guenduez and I. Mergel, "Algorithms in the public sector: A review of discretion and administrative values," *Government Information Quarterly*, vol. 41, no. 1, 101894, 2024, doi: 10.1016/j.giq.2023.101894.
[17] L. Tummers and P. Rocco, "Discretion in the age of artificial intelligence," *Public Management Review*, vol. 26, no. 3, pp. 450–472, 2024, doi: 10.1080/14719037.2023.2211556.
[18] M. Veale and I. Brass, "Administration by algorithm? Public management meets public sector machine learning," *Public Management Review*, vol. 21, no. 8, pp. 1193–1216, 2019, doi: 10.1080/14719037.2018.1495832.