

Regulating Autonomous AI for Transparent and Accountable Digital Public Services

Agung Rizky¹ , Nasrul Hidayat² , Maulana Arif Komara³ , Aulia Wellington^{4*} 

¹Faculty of Sains and Technology, Universitas Raharja, Indonesia

^{2,3}Faculty of Economics and Business, Universitas Raharja, Indonesia

⁴Department of Law and Autonomous Systems Governance, Eesp Incorporation, Samudra Hindia Britania

¹agungrizky@raharja.info, ²nasrul.hidayat@raharja.info, ³maulana.arif@raharja.info, ⁴walington.aul@eesp.io

*Corresponding Author

Article Info

Article history:

Submission March 11, 2026

Revised September 21, 2026

Accepted September 25, 2026

Published September 30, 2026

Keywords:

AI

Digital Public Services

AI Governance

Human Oversight

Digital Governance



ABSTRACT

The increasing deployment of autonomous Artificial Intelligence (AI) in digital public services is transforming administrative decision-making, service delivery, and interactions between governments and citizens. However, greater computational autonomy creates regulatory challenges concerning transparency, accountability, human oversight, and the allocation of legal responsibility when AI-driven decisions produce adverse consequences. **This study aims** to examine the adequacy of existing legal governance principles for autonomous AI in digital public services and to formulate an integrated legal framework that strengthens transparency and accountability while preserving human-centered governance. **This study employs** normative legal research using a conceptual and regulatory approach. Relevant legal principles, regulatory instruments, and scholarly literature concerning AI governance, algorithmic accountability, transparency, data protection, and digital public administration are critically analyzed to identify regulatory gaps and formulate governance principles applicable to autonomous AI systems. **The analysis demonstrates** that conventional administrative and digital governance frameworks remain insufficient to address accountability gaps arising from autonomous decision-making, particularly where responsibility is distributed among public institutions, technology developers, and system operators. The proposed framework integrates algorithmic transparency, traceability, meaningful human oversight, institutional accountability, risk-based regulation, and rights protection as interconnected regulatory requirements. **Effective regulation** of autonomous AI in digital public services requires a human-centered and risk-sensitive legal governance model that reconciles technological autonomy with legal certainty, public accountability, and citizens' fundamental rights. The framework provides a foundation for developing sustainable and trustworthy digital public services.

This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

1. INTRODUCTION

Artificial Intelligence (AI) has increasingly become an integral component of digital government, transforming how public institutions process information, allocate resources, make administrative decisions, and deliver services to citizens [1]. The integration of AI into public administration offers substantial opportunities to improve efficiency, responsiveness, personalization, and the scalability of government services [2].

Recent evidence indicates that AI adoption in government is expanding rapidly, particularly in internal administrative processes and public service delivery, although its application in higher-stakes decision-making remains constrained by concerns regarding data quality, transparency, assurance, and accountability [3]. This development signals a transition from conventional digital government toward increasingly automated and potentially autonomous forms of public administration [4].

For the purposes of this study, autonomous AI refers to AI systems that can perform decision-related functions with a degree of operational independence, including processing information, generating outputs, adapting to changing circumstances, and influencing or initiating actions with limited direct human intervention [5]. This distinguishes autonomous AI from conventional automated systems that primarily execute predetermined rules and from AI-assisted decision-making in which AI mainly provides recommendations or analytical support while a human decision-maker retains direct control over the final decision [6]. The distinguishing characteristic of autonomous AI is therefore not the mere use of AI, but the degree to which the system can independently perform decision-related functions within an administrative process [7]. This distinction is legally significant because increasing operational autonomy may complicate the allocation of authority, responsibility, oversight, and accountability [8].

Transparency represents a further challenge. Citizens interacting with AI-enabled public services may not know whether a decision has been generated or substantially influenced by an algorithm, what data informed the decision, which criteria were applied, or how the decision can be challenged [9]. The problem becomes particularly significant when AI systems operate as complex or partially opaque computational models [10]. The OECD identifies insufficient transparency as a factor that can weaken accountability and public trust, while excessive reliance on AI may amplify errors and deepen existing inequalities [11]. Consequently, transparency in digital public services should not be understood merely as disclosure of technical information, but as a legal and institutional mechanism enabling citizens to understand, contest, and seek review of AI-mediated administrative decisions [12].

Procedural protection should therefore provide affected citizens with a clear pathway to review and contest an AI-mediated decision [13]. At a minimum, this pathway should enable citizens to receive understandable information about the AI system's role, the general grounds of the decision, the responsible institution, and the available procedure for requesting human review [14]. Where an AI-mediated decision adversely affects an individual's rights or access to public services, the individual should have an opportunity to contest the decision before an authorized human reviewer and to obtain an effective remedy where an error, unlawful treatment, or procedural violation is identified [14]. These safeguards ensure that transparency is translated into an actionable procedural right rather than remaining limited to information disclosure [15].

International AI governance principles increasingly recognize these concerns. United Nations Educational, Scientific and Cultural Organization (UNESCO) recommendation on the Ethics of AI places human rights and human dignity at the center of AI governance and identifies transparency, explainability, responsibility, accountability, and human oversight as fundamental principles. It further emphasizes that AI systems should remain auditable and traceable and that ultimate responsibility should not be displaced from human actors to AI systems [16]. These principles establish an important normative foundation for regulating AI in public administration [17]. Nevertheless, translating high-level principles into operational legal requirements remains challenging, particularly where autonomous systems interact with administrative authority and directly affect citizens' rights and access to public services [18]. Existing scholarship and policy frameworks have addressed AI accountability, algorithmic transparency, responsible AI, and automated decision-making from different legal and governance perspectives [19]. However, these approaches frequently examine transparency, accountability, human oversight, or risk management as relatively separate governance requirements [20]. A more integrated legal perspective is necessary because autonomous AI creates interdependent regulatory problems:

- Transparency enables traceability.
- Traceability supports accountability.
- Accountability requires identifiable human or institutional responsibility.
- Effective human oversight provides a mechanism through which automated decisions can be reviewed, challenged, or overridden.

The absence of an integrated relationship among these elements may leave significant gaps in the governance of autonomous AI within digital public services [21].

This study therefore addresses a research gap concerning the formulation of an integrated legal governance framework specifically designed for autonomous AI in digital public services [22]. Rather than treating AI regulation solely as a matter of ethical principles or technological risk management, this research conceptualizes regulation as a mechanism for reconnecting computational autonomy with legal responsibility and human-centered administrative governance [23]. The study particularly focuses on how transparency, accountability, human oversight, traceability, risk-based regulation, and fundamental rights protection can operate as interconnected legal safeguards throughout the AI lifecycle [24].

Accordingly, this study aims to examine the adequacy of existing legal governance principles in addressing the challenges posed by autonomous AI in digital public services and to formulate an integrated legal framework for strengthening transparency and accountability [25]. The study contributes to the LAW Journal scope by connecting autonomous AI regulation with four closely related areas: AI governance and algorithmic regulation, digital governance and web-based public administration, technology law and digital policy, and ethical and human-centered AI governance [26]. In the area of AI governance and algorithmic regulation, the framework establishes interconnected requirements for transparency, traceability, risk assessment, and accountability [27]. In digital governance and web-based public administration, it provides a governance structure for AI-mediated administrative decisions that affect citizens and public services [28]. From a technology law and digital policy perspective, the framework clarifies how technological autonomy can remain subject to legal authority, institutional responsibility, and effective remedies. Finally, its human-centered orientation places human oversight, fundamental rights, and meaningful intervention at the center of autonomous AI governance [29]. By integrating these dimensions, the study advances legal knowledge beyond principle-based discussion toward a structured governance model for autonomous AI in digital public services [30].

2. LITERATURE REVIEW

2.1. Autonomous AI in Digital Public Services

The integration of AI into public administration has transformed conventional digital government by enabling automated data processing, prediction, classification, recommendation, and decision-making [31]. AI adoption can improve administrative efficiency, responsiveness, and service delivery, but it may also create tensions with fundamental public administration values, particularly accountability, equality, fairness, privacy, rule of law, and transparency [32]. A systematic review of automated administrative decision-making confirms that these values may experience both synergies and trade-offs as governments increasingly delegate administrative functions to computational systems [33].

The emergence of increasingly autonomous AI introduces a more complex regulatory dimension because the system may perform decision-related functions with reduced direct human intervention [34]. For the purposes of this study, autonomous AI refers to AI systems that can perform decision-related functions with a degree of operational independence, including processing information, generating outputs, adapting to changing circumstances, and influencing or initiating actions with limited direct human intervention [35]. This distinguishes autonomous AI from conventional automated systems that primarily execute predetermined rules and from AI-assisted decision-making in which AI mainly provides recommendations or analytical support while a human decision-maker retains direct control over the final decision [36]. The distinguishing characteristic of autonomous AI is therefore not the mere use of AI, but the degree to which the system can independently perform decision-related functions within an administrative process. This distinction is legally significant because increasing operational autonomy may complicate the allocation of authority, responsibility, oversight, and accountability [37].

This characteristic challenges conventional assumptions concerning who exercises administrative authority and who should bear responsibility for resulting decisions. In digital public services, such challenges become particularly important where AI-generated outputs influence citizens' access to public services or otherwise affect their rights and interests [38]. Research on AI innovation in government services similarly identifies accountability and clearly defined responsibilities as fundamental requirements when analytical and decision-making functions are increasingly delegated to AI systems. Accordingly, autonomous AI should not be understood merely as an efficiency-enhancing technology. Its deployment represents a transformation in the relationship between computational systems, public institutions, and citizens [39]. The regulatory question

therefore extends beyond whether AI can perform administrative functions effectively to whether its autonomy can remain subject to legal authority, institutional control, and meaningful avenues for citizen review [40].

2.2. Transparency, Accountability, and Human Oversight

Transparency is a fundamental requirement for legitimate AI-based public services because citizens need sufficient information to understand when and how automated systems influence administrative decisions. However, meaningful transparency involves more than simply disclosing the existence of an AI system [41]. It may require information concerning the system's role, relevant decision criteria, data inputs, responsible institutional actors, and mechanisms through which affected individuals can seek explanation or review. Recent research specifically conceptualizes algorithmic transparency in digital public services as an administrative-law concern involving transparency, accountability, procedural rights, and the right to explanation [42]. The relationship between transparency and accountability is particularly important because transparency without traceability may not establish responsibility [43]. Autonomous AI systems require mechanisms that allow relevant actors and authorities to reconstruct how an output was produced and identify the institutional or human actors responsible for its design, deployment, supervision, and consequences [44]. Research on semi-autonomous AI systems emphasizes the importance of preserving operational records and contextual information to clarify the boundaries between human and system agency. Thus, traceability functions as a bridge between transparency and accountability.

Human oversight provides a further safeguard by ensuring that computational autonomy does not eliminate human responsibility [45]. Contemporary regulatory developments increasingly recognize that oversight should correspond to both the level of autonomy and the risks associated with an AI system. The EU AI Act, for example, requires appropriate human oversight for high-risk AI systems and provides that designated persons should be able to understand system limitations, monitor operation, and, where appropriate, disregard, override, or reverse AI outputs [46]. This demonstrates a shift from merely having a human present within an automated process toward meaningful human oversight supported by actual authority and competence. These elements should therefore be understood as an integrated governance chain: transparency enables understanding, traceability enables reconstruction, human oversight enables intervention, and accountability establishes legal responsibility. Such integration is particularly important in public services because automated decisions can directly affect citizens and the legitimacy of public administration [47].

2.3. Risk-Based and Rights-Based AI Governance

The increasing diversity of AI applications has encouraged regulators to adopt risk-based approaches rather than imposing identical obligations on every AI system. A risk-based model allows regulatory requirements to correspond to the potential severity and probability of harm associated with particular applications [48]. The EU AI Act exemplifies this approach by differentiating regulatory obligations according to levels of risk and imposing stronger requirements on high-risk systems, including requirements concerning risk management, data quality, logging, documentation, human oversight, and transparency [49].

Nevertheless, risk-based regulation alone may be insufficient for digital public services because government AI operates within a context of public authority and may directly affect fundamental rights. Therefore, AI governance should also incorporate a rights-based dimension encompassing privacy, non-discrimination, procedural fairness, human dignity, and access to effective remedies [50]. Recent research on AI and social equity in public services highlights the risks of reduced transparency, exclusion, algorithmic bias, and diminished human discretion, while emphasizing the importance of legal frameworks, monitoring, citizen participation, and appeal mechanisms. This combination of risk-based and rights-based governance is particularly relevant to autonomous AI. Greater autonomy should correspond to stronger safeguards where decisions have greater consequences for individuals. Consequently, regulation should not simply ask whether an AI system is technically safe but also whether its deployment preserves citizens' legal rights and whether affected individuals retain meaningful opportunities to understand, challenge, and obtain review of AI-mediated decisions. This approach is consistent with emerging human-centered AI governance frameworks that seek to operationalize human oversight, data accountability, documentation, and bounded algorithmic autonomy.

2.4. Research Gap and Conceptual Proposition

The literature shows that autonomous AI can improve public-sector efficiency while raising concerns about transparency, accountability, fairness, privacy, and the rule of law. Although existing studies address transparency, human oversight, accountability, risk-based regulation, and citizens' rights, these elements are

often treated separately rather than as an integrated legal structure for autonomous AI in public services. The Integrated Human-Centered Legal Governance Framework addresses this gap by linking transparency to traceability, traceability to institutional accountability, and human oversight to enforceable intervention throughout the AI lifecycle. Transparency requires appropriate documentation and disclosure; traceability requires logs that enable significant decisions to be reconstructed; human oversight requires competent and authorized personnel to monitor, intervene, override, or review AI outputs; and risk assessment determines safeguards according to potential impacts. Thus, the framework translates broad AI governance principles into an operational legal structure that enables controlled AI autonomy while preserving human legal responsibility.

The framework positions transparency as the foundation of traceability, traceability as the basis of accountability, human oversight as the mechanism for meaningful intervention, and rights protection and risk-based regulation as boundaries for legitimate AI autonomy. This integrated approach strengthens LAW's interdisciplinary contribution by connecting autonomous technology with digital governance, administrative law, accountability, and human-centered rights protection.

3. RESEARCH METHOD

3.1. Research Design and Legal Approaches

This study employs a normative legal research design to examine the regulation of autonomous AI in digital public services, focusing on transparency and accountability. This approach analyzes legal norms, principles, regulations, and governance concepts rather than empirically measuring institutional or user behavior. Recent AI governance studies in public administration have similarly applied normative analysis to identify gaps in supervisory authority, algorithmic auditing, compliance, and institutional accountability.

Three complementary approaches are applied. First, the statutory approach examines laws and regulations on AI, digital public administration, electronic systems, personal data protection, transparency, accountability, and administrative decision-making. Second, the conceptual approach analyzes algorithmic transparency, traceability, accountability, human oversight, risk-based regulation, and rights protection. Third, the comparative approach examines regulatory developments in selected jurisdictions and international AI governance instruments as relevant models for AI-enabled public services. The methodological structure is presented in Figure 1, which illustrates the sequence from the regulatory problem through legal approaches, regulatory gap analysis, and framework formulation.

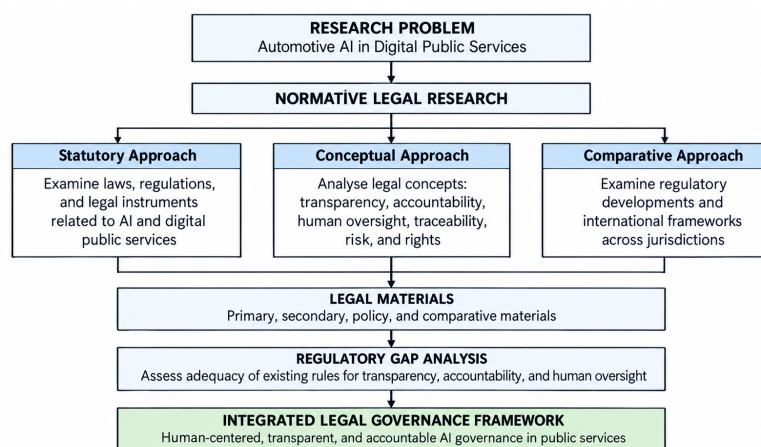


Figure 1. Research Design for the Normative Legal Analysis of Autonomous AI

Figure 1 illustrates the analytical sequence used in this research. The study begins with the regulatory problem created by the increasing autonomy of AI in digital public services and subsequently applies statutory, conceptual, and comparative legal approaches. The resulting legal materials are examined through regulatory gap analysis to determine whether existing legal mechanisms adequately address transparency, accountability, and human oversight. These findings are then synthesized into an integrated legal governance framework. This structure is consistent with contemporary normative research on AI governance, which combines statutory, conceptual, and comparative approaches to reconstruct administrative oversight mechanisms.

3.2. Legal Materials and Data Collection

The legal materials are classified into primary and secondary legal materials. Primary legal materials consist of legislation, regulations, official regulatory instruments, and international legal or governance frameworks relevant to AI, digital public services, administrative decision-making, data protection, transparency, accountability, and human oversight. Secondary legal materials consist of peer-reviewed journal articles, scholarly books, academic studies, and authoritative policy publications addressing AI governance, algorithmic decision-making, digital government, administrative law, and digital rights.

The selection of legal materials is guided by their legal relevance, institutional authority, topical relevance, and applicability to autonomous AI in public services. Particular attention is given to regulatory instruments that establish concrete obligations concerning risk management, transparency, traceability, and human oversight. For example, the EU AI Act provides a significant comparative reference because its regulatory framework links risk classification with requirements concerning documentation, logging, transparency, and human oversight.

Table 1. Materials Examined and Their Functions in the Research

Category	Materials Examined	Function in the Research
Primary legal materials	Legislation, regulations, AI regulatory instruments, administrative regulations, international governance instruments	Identify binding legal obligations and regulatory principles
Secondary legal materials	Peer-reviewed journal articles, academic books, scholarly studies	Develop theoretical and doctrinal arguments
Policy and institutional materials	Official AI governance frameworks, regulatory guidelines, institutional reports	Identify emerging governance standards and implementation principles
Comparative materials	Selected foreign AI regulations and international frameworks	Identify transferable regulatory principles and comparative gaps

Table 1 demonstrates how each category of legal material contributes to the analysis. Primary materials establish the normative foundation, secondary materials support doctrinal and conceptual interpretation, while policy and comparative materials provide broader regulatory perspectives. The combination is particularly important because AI regulation is developing rapidly and remains fragmented across jurisdictions. Recent research on Indonesia's AI governance, for example, identifies the absence of an integrated administrative framework concerning regulatory authority, algorithmic audits, certification, compliance oversight, and accountability.

3.3. Legal Analysis and Framework Development

The collected materials are analyzed using normative legal analysis, regulatory gap analysis, and normative synthesis. The analysis begins by identifying the existing legal principles applicable to AI-enabled public services. These principles are then compared with the specific characteristics of autonomous AI, particularly its capacity to perform decision-related functions with reduced direct human intervention.

The second stage identifies regulatory gaps by assessing whether existing legal mechanisms adequately safeguard transparency, traceability, accountability, human oversight, risk management, and fundamental rights. Particular attention is given to the relationship between these principles rather than treating them as independent requirements. For example, transparency provides information about AI involvement and decision processes, traceability enables decisions to be reconstructed, human oversight enables intervention, and accountability establishes responsibility for the consequences of AI-mediated decisions.

The third stage applies comparative analysis to identify regulatory principles that can strengthen the governance of autonomous AI. The EU AI Act is particularly relevant because its human-oversight requirements require high-risk AI systems to permit meaningful human monitoring and intervention, including the ability to disregard, override, or reverse system outputs where appropriate. Its framework also connects risk management with transparency, documentation, record-keeping, and human oversight. The integrated analytical relationship is presented in Figure 2, while Table 2 summarizes the corresponding legal dimensions and regulatory functions.

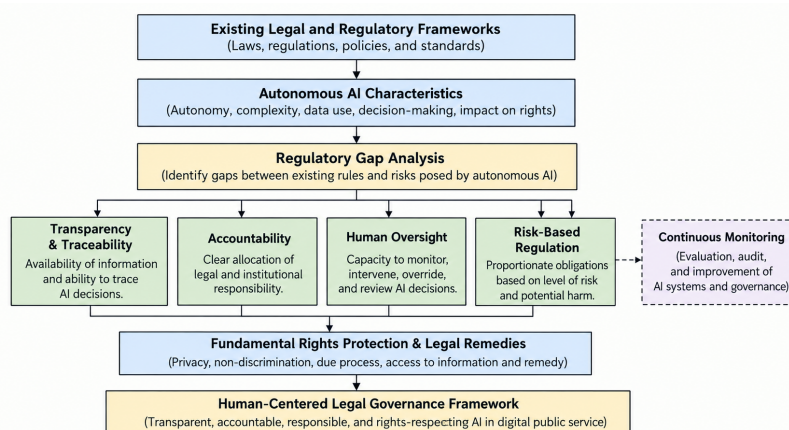


Figure 2. Integrated Legal Analysis Framework

Figure 2 shows the central analytical proposition of the study. Existing legal frameworks are assessed against the characteristics and risks of autonomous AI to identify regulatory deficiencies. Transparency and traceability establish the informational basis for accountability, while human oversight preserves meaningful human intervention. These mechanisms operate within a risk-based regulatory structure and are ultimately constrained by fundamental rights and access to legal remedies. The synthesis produces a human-centered legal governance framework designed to ensure that increasing technological autonomy does not result in the displacement of human and institutional legal responsibility.

The integrated legal analysis framework presented in Figure 2 provides the analytical basis for identifying the key legal requirements for governing autonomous AI in digital public services. The framework connects existing legal and regulatory instruments with the specific characteristics and risks of autonomous AI, followed by an assessment of regulatory gaps and the formulation of interconnected governance requirements. To further operationalize the proposed framework, Table 2 summarizes the principal analytical dimensions and their corresponding legal functions in ensuring transparent, accountable, and human-centered AI governance.

Table 2. Analytical Dimensions of the Proposed Legal Governance Framework

Dimension	Core Legal Question	Expected Regulatory Function
Transparency and traceability	Can citizens and regulators understand and reconstruct AI-mediated decisions?	Disclosure, documentation, logging, and explainability
Accountability	Who is legally responsible for AI deployment and its consequences?	Clear allocation of institutional and human responsibility
Human oversight	Can authorized humans monitor, intervene in, or override AI decisions?	Meaningful human control and intervention
Risk management	Are regulatory obligations proportionate to the potential level of harm?	Risk classification, assessment, mitigation, and monitoring
Rights protection	Are citizens protected from unlawful, discriminatory, or harmful AI decisions?	Privacy, equality, due process, and access to remedy

Table 2 forms the analytical basis for the Results and Discussion section. Rather than assuming that autonomy itself should be prohibited, the study examines the legal conditions under which autonomous AI can legitimately operate in public services. The resulting framework therefore seeks to reconcile technological autonomy with human accountability, administrative legality, transparency, and citizens' fundamental rights. These dimensions provide a structured basis for assessing the legal implications of autonomous AI in public services. They also highlight the importance of ensuring that technological autonomy remains subject to appropriate legal safeguards and institutional responsibilities.

4. RESULTS AND DISCUSSION

4.1. Regulatory Challenges of Autonomous AI in Digital Public Services

The analysis indicates that the increasing use of autonomous AI in digital public services creates regulatory challenges that cannot be adequately addressed through conventional administrative and information technology regulations alone. Autonomous AI systems may perform functions such as data classification, prediction, recommendation, prioritization, and decision-making with limited direct human intervention. While these capabilities can improve administrative efficiency and service responsiveness, they also introduce uncertainty regarding who should be legally responsible when an AI-supported decision produces an error, discriminatory outcome, or other adverse consequence. Recent research on automated administrative decision-making similarly identifies tensions between efficiency and core public administration values, including accountability, fairness, privacy, rule of law, and transparency.

A central finding of this study is that autonomy should not be interpreted as a transfer of legal responsibility from human actors to the AI system itself. Instead, legal responsibility must remain attributable to identifiable natural or legal persons involved in the AI lifecycle. This position is consistent with the UNESCO Recommendation on the Ethics of AI, which emphasizes that AI systems should remain subject to human responsibility and accountability and that accountability should be supported through auditability and traceability. The regulatory problem therefore arises not simply from the existence of AI, but from the distribution of responsibility across multiple actors. Public institutions may determine the purpose and conditions of deployment, technology providers may design and maintain the system, and operators may supervise or implement AI-generated outputs. Without explicit legal allocation of responsibilities, the resulting governance structure may create accountability gaps, particularly when the decision-making process is difficult to reconstruct or when institutions rely excessively on automated outputs.

Consequently, autonomous AI used in public services requires a governance model that connects technological autonomy with legally identifiable responsibility. This finding provides the basis for the integrated framework proposed in this study, in which transparency and traceability function as mechanisms for establishing accountability rather than merely as general ethical principles.

4.2. Legal Requirements for Transparency, Traceability, and Human Oversight

The analysis further demonstrates that transparency in autonomous AI governance should be understood as a functional legal requirement, rather than merely an obligation to disclose technical information. Citizens affected by AI-supported public services should be able to understand whether an AI system is being used, the general role it performs, the categories of data involved, the responsible institution, and the mechanisms available to challenge or review an AI-assisted decision. This interpretation is consistent with international AI governance principles that connect transparency and explainability with accountability, human rights, and meaningful oversight.

However, transparency alone is insufficient when an AI decision cannot be reconstructed after it has been made. Traceability therefore becomes the operational dimension of transparency. To make an AI-mediated administrative decision reconstructable, the system should preserve appropriate records of the decision context, relevant data inputs or data categories, model or system version, applicable decision criteria, processing or workflow stages, generated outputs, timestamps, human interventions, overrides, and subsequent administrative actions. The scope of record-keeping should be proportionate to the significance and risk of the decision, while respecting applicable data protection and confidentiality requirements. These records enable authorized reviewers, auditors, and responsible institutions to reconstruct the decision-making process, identify where an error or intervention occurred, and determine which actors exercised relevant authority. Traceability therefore transforms transparency from information disclosure into an evidentiary mechanism that supports administrative review, accountability, and legal remedies.

Human oversight is a key requirement for responsible autonomous AI governance. It should involve active human capacity to monitor, interpret, intervene in, override, and review AI outputs, supported by adequate authority, competence, and information. The EU AI Act similarly emphasizes effective human oversight for high-risk AI systems according to their autonomy and associated risks. Transparency, traceability, and human oversight therefore function as mutually reinforcing safeguards: transparency enables scrutiny, traceability preserves evidence, and human oversight enables intervention. Together, they strengthen the reviewability of autonomous AI decisions and support clear institutional accountability for adverse outcomes.

4.3. Integrated Human-Centered Legal Governance Framework

Based on the regulatory gap analysis, this study proposes an Integrated Human-Centered Legal Governance Framework consisting of six interconnected dimensions: algorithmic transparency, traceability, institutional accountability, human oversight, risk-based regulation, and fundamental rights protection. Rather than treating these principles as independent requirements, the framework positions them as mutually reinforcing components across the AI governance lifecycle. First, algorithmic transparency and traceability establish the informational foundation of accountability. Public institutions should maintain appropriate documentation concerning the purpose, function, data use, and decision-making role of autonomous AI systems. Traceability mechanisms should additionally ensure that significant AI-supported actions can be reconstructed and audited. Second, institutional accountability requires clear allocation of legal responsibility among public authorities, system providers, and operators. The institution deploying autonomous AI should not avoid responsibility merely because a decision was generated by an automated system. Responsibility should instead be allocated according to each actor's function, authority, control, and contribution throughout the AI lifecycle.

Third, human oversight provides a safeguard against excessive technological autonomy. Human intervention should be proportionate to the potential impact of the AI system. For low-impact administrative services, such as routine informational or administrative support functions, human oversight may primarily involve monitoring and periodic review. For medium-impact services that may influence eligibility, prioritization, or access to non-essential administrative benefits, human review should be available when relevant concerns or adverse outcomes arise. For high-impact decisions affecting legal rights, essential public services, social benefits, permits, or other significant individual interests, meaningful human review should occur before or immediately following the decision, with sufficient authority to question, override, or reverse the AI output. Proportionality therefore requires the intensity of human oversight to increase with the potential severity, reversibility, and rights implications of the decision. Fourth, risk-based regulation allows regulatory obligations to correspond to the potential harm and level of autonomy of the AI system. This prevents both under-regulation of high-risk applications and unnecessary regulatory burdens for low-risk systems. The OECD similarly emphasizes that government use of AI requires governance mechanisms capable of managing risks associated with biased data, insufficient transparency, overreliance, and diminished public trust. Finally, fundamental rights protection and legal remedies provide the normative boundary of autonomous AI deployment. Privacy, non-discrimination, due process, access to information, and the right to challenge adverse decisions should remain protected throughout the AI lifecycle. UNESCO's framework similarly emphasizes privacy, fairness, accountability, transparency, human oversight, and access to appropriate governance mechanisms as interconnected elements of responsible AI.

The framework moves beyond a technology-oriented approach toward legal governance in which AI autonomy operates within clear boundaries of transparency, accountability, human control, proportionality, and rights protection. It is primarily applicable to digital public services where AI influences administrative decisions affecting rights, eligibility, benefits, permits, licensing, or other significant services. Low-risk applications with limited impact on individual rights may require lighter governance. Thus, the framework applies proportionately according to the system's autonomy, potential impact, and implications for individual rights.

4.4. Legal and Policy Implications for Sustainable Digital Public Services

The sustainability dimension of the framework is closely aligned with SDG 16, Peace, Justice and Strong Institutions, by promoting transparent, accountable, reviewable, and rights-respecting AI governance. It also supports SDG 9, Industry, Innovation and Infrastructure, by encouraging responsible technological innovation within appropriate legal and institutional safeguards. Thus, sustainable digital public services should be understood not only in terms of technological efficiency but also institutional integrity, responsible innovation, and long-term protection of citizens' rights.

The framework proposes a continuous lifecycle governance model for autonomous AI in digital public services. Before deployment, risk and impact assessments should determine potential harms, appropriate levels of autonomy and human oversight, institutional responsibilities, and documentation requirements. During operation, monitoring and logging should track system performance, decisions, human interventions, and emerging risks. Periodic audits should evaluate continued legal and governance compliance, while identified errors or rights violations should trigger corrective action, system modification, suspension, or other appropriate measures. These processes should continuously inform subsequent risk assessments and governance adjustments.

The main contribution of the framework is its integration of transparency, accountability, human oversight, risk management, and rights protection into a single governance structure. Greater AI autonomy and potential impact should correspond to stronger requirements for traceability, oversight, accountability, and legal remedies. However, implementation may vary across emerging economies due to differences in technical expertise, infrastructure, financial resources, and regulatory capacity. A proportionate approach should therefore be adopted while maintaining minimum safeguards for transparency, accountability, human oversight, and rights protection. Capacity building, technical training, and inter-institutional cooperation can support effective implementation.

5. MANAGERIAL IMPLICATIONS

For public managers, governance responsibility should begin before deployment through the definition of the AI system's purpose, scope, level of autonomy, responsible institutional actors, and accountability arrangements. Regulators should establish risk-based requirements, minimum documentation and logging standards, audit mechanisms, reporting obligations, and accessible procedures for reviewing or challenging AI-mediated decisions. AI developers should incorporate transparency, traceability, documentation, testing, risk assessment, and appropriate human-control mechanisms into system design and maintenance. System operators should conduct continuous monitoring, document significant AI actions and human interventions, identify anomalous or harmful outputs, and escalate high-impact decisions when human review is required. Across these roles, responsibility should remain institutionally identifiable and should not be displaced by the autonomous operation of the AI system. This division of responsibilities can strengthen monitoring, auditing, intervention, and accountability while enabling public institutions to benefit from AI-enabled efficiency without compromising legal certainty and citizens' rights.

6. CONCLUSION

The increasing deployment of autonomous AI in digital public services creates legal challenges concerning transparency, accountability, traceability, human oversight, risk management, and fundamental rights protection. This study finds that conventional administrative and technological governance mechanisms are insufficient when AI systems can process information, generate outputs, and influence public decisions with limited human intervention. Importantly, technological autonomy cannot transfer or eliminate legal responsibility, which must remain attributable to identifiable human and institutional actors.

Based on the normative legal analysis, this study proposes an integrated human-centered legal governance framework comprising six interconnected dimensions: algorithmic transparency, traceability, institutional accountability, meaningful human oversight, risk-based regulation, and fundamental rights protection. Transparency enables understanding of AI-mediated processes, traceability allows decisions to be reconstructed, accountability establishes responsibility, and human oversight preserves the capacity for intervention and review. Risk-based regulation determines the proportional intensity of safeguards, while fundamental rights protection establishes substantive and procedural boundaries for autonomous AI. These dimensions should operate continuously throughout the AI lifecycle rather than as isolated regulatory requirements.

The central normative principle of this study is that greater AI autonomy and potential public impact should require stronger legal safeguards. Before deployment, institutions should conduct appropriate risk and impact assessments and establish clear responsibilities and transparency requirements; during operation, monitoring, logging, human oversight, and accountability should be maintained; and following significant incidents, audit, review, remediation, and improvement mechanisms should be available. Through this integrated approach, autonomous AI can support innovation and efficiency in digital public services while preserving human responsibility, legal certainty, public trust, equality, and fundamental rights.

7. DECLARATIONS

7.1. About Authors

Agung Rizky (AR)  <https://orcid.org/0009-0006-7046-8639>

Nasrul Hidayat (NH)  <https://orcid.org/0009-0006-1498-5586>

Maulana Arif Komara (MK)  <https://orcid.org/0009-0005-8906-3132>

Aulia Wellington (AW)  <https://orcid.org/0009-0004-4536-4729>

7.2. Author Contributions

Conceptualization: AR; Methodology: AW; Software: MK; Validation: NH, AW and MK; Formal Analysis: AR and MK; Investigation: NH; Resources: MK; Data Curation: AR and NH; Writing Original Draft Preparation: MK and AW; Writing Review and Editing: NH and AR; Visualization: MK; All authors, AR, NH, MK, and AW have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- [1] K. Alhosani and S. M. Alhashmi, "Opportunities, challenges, and benefits of ai innovation in government services: a review," *Discover Artificial Intelligence*, vol. 4, no. 1, p. 18, 2024.
- [2] B. Attard-Frost, A. Brandusescu, and K. Lyons, "The governance of artificial intelligence in canada: Findings and opportunities from a review of 84 ai governance initiatives," *Government Information Quarterly*, vol. 41, no. 2, p. 101929, 2024.
- [3] A. Batool, D. Zowghi, and M. Bano, "Ai governance: a systematic literature review," *AI and Ethics*, vol. 5, no. 3, pp. 3265–3279, 2025.
- [4] E. Bracci, "The loopholes of algorithmic public services: An "intelligent" accountability research agenda," *Accounting, Auditing & Accountability Journal*, vol. 36, no. 2, pp. 739–763, 2023.
- [5] M. A. Camilleri, "Artificial intelligence governance: Ethical considerations and implications for social responsibility," *Expert systems*, vol. 41, no. 7, p. e13406, 2024.
- [6] Y. Chandra and N. Feng, "Algorithms for a new season? mapping a decade of research on the artificial intelligence-driven digital transformation of public administration," *Public Management Review*, vol. 28, no. 3, pp. 620–654, 2026.
- [7] Y. Fan, "The role of artificial intelligence in the digital transformation of government: opportunities and ethical challenges," *Frontiers in public health*, vol. 13, p. 1694996, 2025.
- [8] T. Chen, M. Gasco-Hernandez, and J. R. Gil-Garcia, "Understanding accountability in ai use within the public sector: Insights from state governments in the united states," *Public Administration*, 2026.
- [9] J. C. Covilla, "Artificial intelligence and administrative discretion: Exploring adaptations and boundaries," *European Journal of Risk Regulation*, vol. 16, no. 1, pp. 36–50, 2025.
- [10] Bhima, A. R. A. Zahra, and T. Nurtino, "Enhancing organizational efficiency through the integration of artificial intelligence in management information systems," *APTISI Transactions on Management (ATM)*, vol. 7, no. 3, pp. 282–289, 2023.
- [11] P. M. A. R. Correia, R. L. D. Pedro, I. d. O. Mendes, and A. D. Serra, "The challenges of artificial intelligence in public administration in the framework of smart cities: reflections and legal issues," *Social sciences*, vol. 13, no. 2, p. 75, 2024.

- [12] U. Fischer-Abaigar, C. Kern, N. Barda, and F. Kreuter, "Bridging the gap: Towards an expanded toolkit for ai-driven decision-making in the public sector," *Government Information Quarterly*, vol. 41, no. 4, p. 101976, 2024.
- [13] Mustam, A. Rizky, and J. Edwards, "Technology innovation adoption for business performance in the digital economy," *APTISI Transactions on Management (ATM)*, vol. 10, no. 3, pp. 332–345, August 2026.
- [14] 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, p. 101704, 2022.
- [15] S. Grimmelikhuijsen and A. Meijer, "Legitimacy of algorithmic decision-making: Six threats and the need for a calibrated institutional response," *Perspectives on Public Management and Governance*, vol. 5, no. 3, pp. 232–242, 2022.
- [16] S. Hidayat, K. Kusrini, E. Utami, A. Setyanto, and K. Vaher, "Artificial intelligence driven predictive risk management in green technology investment," *APTISI Transactions on Management (ATM)*, vol. 10, no. 2, pp. 203–214, May 2026.
- [17] M. P. Hauer, T. D. Krafft, and K. Zweig, "Overview of transparency and inspectability mechanisms to achieve accountability of artificial intelligence systems," *Data & Policy*, vol. 5, p. e36, 2023.
- [18] I. T. Hjaltalin and H. T. Sigurdarson, "The strategic use of ai in the public sector: A public values analysis of national ai strategies," *Government Information Quarterly*, vol. 41, no. 1, p. 101914, 2024.
- [19] A. R. Aruan, K. Toha, and A. R. Nurdin, "Digital governance for confiscating crypto-assets to settle tax liabilities in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 1066–1079, 2025.
- [20] M. S. Khan, A. Shoaib, and E. Arledge, "How to promote ai in the us federal government: Insights from policy process frameworks," *Government Information Quarterly*, vol. 41, no. 1, p. 101908, 2024.
- [21] I. B. M. P. Dharmika and I. N. Subanda, "The effectiveness of public services in realizing good governance," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 1Sp, pp. 77–83, 2023.
- [22] G. Lazcoz and P. De Hert, "Humans in the gdpr and aia governance of automated and algorithmic systems. essential pre-requisites against abdicating responsibilities," *Computer Law & Security Review*, vol. 50, p. 105833, 2023.
- [23] 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, p. 101774, 2023.
- [24] S. Kosasi, C. Lukita, M. H. R. Chakim, A. Faturahman, and D. A. R. Kusumawardhani, "The influence of digital artificial intelligence technology on quality of life with a global perspective," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 240–250, 2023.
- [25] M. Mäntymäki, M. Minkinen, T. Birkstedt, and M. Viljanen, "Defining organizational ai governance," *AI and Ethics*, vol. 2, no. 4, pp. 603–609, 2022.
- [26] I. Mergel, H. Dickinson, J. Stenvall, and M. Gasco, "Implementing ai in the public sector," *Public Management Review*, pp. 1–14, 2024.
- [27] J. Juanda, R. J. Riansyah, A. Arsadi, and L. Bethany, "Towards entrepreneurial campus sustainability: Integrating artificial intelligence for resource allocation in business management," *Aptisi transactions on technopreneurship (ATT)*, vol. 6, no. 3, pp. 314–323, 2024.
- [28] J. Mišić, R. van Est, and L. Kool, "Good governance of public sector ai: A combined value framework for good order and a good society," *AI and Ethics*, vol. 5, no. 5, pp. 4875–4889, 2025.
- [29] J. Mökander and L. Floridi, "Operationalising ai governance through ethics-based auditing: an industry case study," *AI and Ethics*, vol. 3, no. 2, pp. 451–468, 2023.
- [30] A. Kiseleva, D. Kotzinos, and P. De Hert, "Transparency of ai in healthcare as a multilayered system of accountabilities: between legal requirements and technical limitations," *Frontiers in artificial intelligence*, vol. 5, p. 879603, 2022.
- [31] N. Nuryani, A. B. Mutiara, I. M. Wiryana, D. Purnamasari, and S. N. W. Putra, "Artificial intelligence model for detecting tax evasion involving complex network schemes," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 339–356, 2024.
- [32] O. Neumann, K. Guirguis, and R. Steiner, "Exploring artificial intelligence adoption in public organizations: a comparative case study," *Public Management Review*, vol. 26, no. 1, pp. 114–141, 2024.
- [33] C. Novelli, M. Taddeo, and L. Floridi, "Accountability in artificial intelligence: what it is and how it works," *Ai & Society*, vol. 39, no. 4, pp. 1871–1882, 2024.
- [34] D. Novitasari, F. S. Goestjahjanti, U. Rahardja, S. Santoso, S. V. Sihotang, N. A. Santoso, and G. P. Cesna,

- “Optimizing msme performance through marketing capabilities and digital marketing adoption,” in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2025, pp. 1–7.
- [35] P. G. R. De Almeida and C. D. dos Santos Junior, “Artificial intelligence governance: Understanding how public organizations implement it,” *Government information quarterly*, vol. 42, no. 1, p. 102003, 2025.
- [36] U. B. 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. 1184–1199, 2024.
- [37] U. Rahardja, Q. Aini, D. Manongga, I. Sembiring, and I. D. Girinzio, “Implementation of tensor flow in air quality monitoring based on artificial intelligence,” *International Journal of Artificial Intelligence Research*, vol. 6, no. 1, p. 23, 2023.
- [38] F. Selten and B. Klievink, “Organizing public sector ai adoption: Navigating between separation and integration,” *Government Information Quarterly*, vol. 41, no. 1, p. 101885, 2024.
- [39] V. J. Straub, D. Morgan, J. Bright, and H. Margetts, “Artificial intelligence in government: Concepts, standards, and a unified framework,” *Government Information Quarterly*, vol. 40, no. 4, p. 101881, 2023.
- [40] Cabinet Secretariat of the Republic of Indonesia. (2026, Jun.) President prabowo pushes acceleration of ai-based govtech to strengthen state governance and budget. Cabinet Secretariat of the Republic of Indonesia. [Online]. Available: <https://setkab.go.id/en/president-prabowo-pushes-acceleration-of-ai-based-govtech-to-strengthen-state-governance-and-budget/>
- [41] D. Manongga, U. Rahardja, I. Sembiring, Q. Aini, and A. Wahab, “Improving the air quality monitoring framework using artificial intelligence for environmentally conscious development,” *HighTech and Innovation Journal*, vol. 5, no. 3, pp. 794–813, 2024.
- [42] C. Van Noordt and G. Misuraca, “Artificial intelligence for the public sector: results of landscaping the use of ai in government across the european union,” *Government information quarterly*, vol. 39, no. 3, p. 101714, 2022.
- [43] G. Wang, Y. Guo, W. Zhang, S. Xie, and Q. Chen, “What type of algorithm is perceived as fairer and more acceptable? a comparative analysis of rule-driven versus data-driven algorithmic decision-making in public affairs,” *Government Information Quarterly*, vol. 40, no. 2, p. 101803, 2023.
- [44] N. Lutfiani, I. Sembiring, I. Setyawan, A. Setiawan, U. Rahardja, and S. Sulistio, “Exploring the relationship between artificial intelligence and business performance,” *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 19, no. 1, pp. 1–12, 2025.
- [45] J. Willems, M. J. Schmid, D. Vanderelst, D. Vogel, and F. Ebinger, “Ai-driven public services and the privacy paradox: do citizens really care about their privacy?” *Public Management Review*, vol. 25, no. 11, pp. 2116–2134, 2023.
- [46] S. Misra, B. Katz, P. Roberts, M. Carney, and I. Valdivia, “Toward a person-environment fit framework for artificial intelligence implementation in the public sector,” *Government Information Quarterly*, vol. 41, no. 3, p. 101962, 2024.
- [47] C. Li, “Ai-driven governance: Enhancing transparency and accountability in public administration,” *Digital Society & Virtual Governance*, vol. 1, no. 1, pp. 1–16, 2025.
- [48] M. Stankovich, E. Behrens, and J. Burchell, “Toward meaningful transparency and accountability of ai algorithms in public service delivery,” *Government Information Quarterly, early access*, 2023.
- [49] F. A.-H. Al-Shawabkeh and K. Al-Jasmi, “Artificial intelligence and transparency management in the public sector: A comparative legal study on accountability and oversight in european and american laws,” *Journal of Posthumanism*, vol. 5, no. 5, pp. 2326–2340, 2025.
- [50] Z. Wang, “Transparent governance in an automated age: Challenges and solutions in public authorities ai deployment,” *International Journal of Ethical AI Application*, vol. 1, no. 4, pp. 31–36, 2025.