Interdisciplinary Studies in Society, Law, and Politics 2027; 6(1): 1-14

ISSLP

Original Research

Algorithmic Governance in Public Administration: An Analysis of the Challenges of Accountability, Transparency, and Responsibility in Artificial Intelligence–Based Decision-Making

Mohammad Reza. Karami[1*]

[1] M.A., Department of Political Science, Shahid Beheshti University, Tehran, Iran

*** Corresponding author email address**: karamitrade.ir@gmail.com

Received: 2026-05-06 **Revised:** 2026-10-14 **Accepted:** 2026-10-21 **Initial Publish:** 2026-10-21 **Final Publish:** 2027-01-01

The increasing use of artificial intelligence in public administration has transformed the structure of governmental decision-making and created new legal challenges concerning transparency, accountability, and responsibility. Algorithmic systems are increasingly employed to classify individuals, assess risks, allocate public resources, support regulatory enforcement, and assist or automate administrative decisions. Although these technologies may improve efficiency, consistency, and institutional capacity, they may also weaken traditional safeguards of administrative law when their operation is opaque, difficult to explain, or distributed among multiple public and private actors. This article examines the legal implications of algorithmic governance in public administration with particular emphasis on the principles of legality, procedural fairness, transparency, explainability, equality, human oversight, judicial review, and institutional responsibility. Using a descriptive-analytical legal approach, the study evaluates the extent to which existing public-law principles can address the challenges created by AI-based decision-making and identifies areas in which additional regulatory mechanisms are required. The analysis shows that transparency must extend beyond simple disclosure of algorithmic use and should include meaningful explanations of the factors influencing individual administrative decisions. It also argues that public authorities must remain legally responsible for decisions generated or materially influenced by artificial intelligence, even where systems are developed or supplied by private contractors. Effective human oversight, algorithmic impact assessments, continuous auditing, accessible complaint procedures, and meaningful judicial review are essential for preventing accountability gaps. The article concludes that a sustainable model of algorithmic governance requires the integration of technological innovation with established principles of public law. Artificial intelligence should support, rather than displace, legal responsibility, and the use of algorithmic systems must remain subject to identifiable lines of explanation, review, and institutional accountability.

Keywords: *Algorithmic Governance; Public Administration; Artificial Intelligence; Administrative Law; Transparency; Accountability; Legal Responsibility; Automated Decision-Making*

How to cite this article:

Karami, M. R. (2027). Algorithmic Governance in Public Administration: An Analysis of the Challenges of Accountability, Transparency, and Responsibility in Artificial Intelligence–Based Decision-Making. *Interdisciplinary Studies in Society, Law, and Politics, 6*(1), 1-14. https://doi.org/10.61838/kman.isslp.596

1. Introduction

The expansion of artificial intelligence into public administration has transformed the legal and institutional architecture of governmental decision-making. Public authorities increasingly rely on algorithmic systems to classify individuals, allocate public resources, detect fraud, assess eligibility for

© 2027 The authors. Published by KMAN Publication Inc. (KMANPUB). This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

benefits, prioritize inspections, evaluate risks, manage taxation, support policing, and assist regulatory enforcement. What distinguishes this development from earlier forms of administrative automation is not merely the growing computational capacity of public institutions but the increasing delegation of analytical, predictive, and sometimes decisional functions to systems whose internal processes may be difficult for officials, affected individuals, courts, and even technical designers to fully reconstruct. In this environment, the traditional administrative-law assumption that a public decision can be traced to an identifiable human decision-maker is progressively destabilized. Artificial intelligence systems may shape administrative choices through automated recommendations, risk scores, prioritization mechanisms, classifications, and predictive models long before a final decision is formally issued by a human official. The legal significance of this transformation lies in the fact that administrative law has historically developed around concepts such as legality, competence, reason-giving, procedural fairness, proportionality, reviewability, and individual responsibility. Algorithmic decision-making potentially modifies the factual conditions under which all of these principles operate. Contemporary legal scholarship has therefore increasingly emphasized that the incorporation of AI into governance cannot be treated as a purely technical modernization project because it directly affects the distribution of public power and the conditions under which that power may be challenged (Samiya & Bourane, 2025). The legal question is no longer whether public authorities may employ digital technologies, but under what institutional and normative conditions algorithmically assisted governance can remain compatible with the rule of law.

Algorithmic governance may be understood as the use of computational systems, data-driven models, machine learning tools, automated procedures, and predictive analytics in the exercise, organization, or support of public power. Such governance differs from ordinary digitization because algorithms may actively structure how information is interpreted and how administrative priorities are determined. In conventional public administration, legal rules are applied by officials who are expected to interpret evidence, weigh relevant factors, provide reasons, and remain accountable for the resulting decisions. By contrast, algorithmic systems may convert policy objectives into computational variables, rank individuals or cases, identify correlations, and generate outputs whose normative implications are not always visible. This is particularly important because algorithmic classifications may affect access to employment, welfare, education, public services, licensing, financial opportunities, regulatory treatment, or law-enforcement attention. As analyses of emerging AI regulation demonstrate, the legal treatment of artificial intelligence increasingly revolves around the recognition that algorithms can exercise a form of practical power over individuals even when they do not possess formal legal personality (He & Zhang, 2025). The concept of "algorithmic power" is therefore relevant to public law because it captures the ability of technical systems to influence legal positions, administrative outcomes, and opportunities through computational processes that are embedded within governmental institutions.

The expansion of AI governance has generated a parallel expansion of regulatory activity. Legislators and policymakers in multiple jurisdictions have attempted to define principles for risk management, transparency, human oversight, technical robustness, fairness, and accountability. One of the most significant legal developments has been the European Union's attempt to establish a comprehensive risk-based regulatory regime for artificial intelligence, reflecting the growing recognition that certain AI applications may create substantial threats to fundamental rights and institutional legitimacy (Nouralivand, 2024). The importance of such regulatory efforts extends beyond the European context because they illustrate a broader shift from voluntary ethical principles toward legally enforceable obligations. Legal scholars have similarly argued that AI governance requires a coherent legislative rationale rather than fragmented or purely sectoral interventions (Ghamami, 2024). This regulatory movement indicates that the principal challenge is not simply technological innovation but the integration of algorithmic systems into existing legal orders without weakening established protections against arbitrary power. The question of legal regulation becomes particularly urgent in public administration because the state possesses coercive powers unavailable to private actors. An erroneous recommendation generated by a commercial platform may cause economic

inconvenience, whereas an erroneous administrative algorithm may affect benefits, immigration status, taxation, licensing, policing, or access to public entitlements.

Within this emerging field, transparency is one of the most frequently invoked principles. However, algorithmic transparency is not a singular concept. It may refer to disclosure that an algorithm is being used, publication of the legal basis for its use, explanation of the variables or datasets employed, documentation of model design, provision of individual reasons for a particular outcome, or access to audit records and technical testing procedures. The complexity of these possibilities explains why transparency regulation has developed unevenly. A systematic examination of transparency laws in European jurisdictions has shown that legal transparency obligations often differ in scope, audience, enforceability, and technical specificity (Krook et al., 2025). This fragmentation creates a basic legal difficulty: formal disclosure may exist without genuine intelligibility. An administration could theoretically disclose the existence of an algorithm while remaining unable to explain why a particular individual received a particular score. Conversely, highly technical model documentation may be publicly available yet incomprehensible to ordinary citizens. Thus, effective legal transparency must be distinguished from mere informational disclosure. It must enable those affected by administrative action to understand the basis of decisions sufficiently to contest error, discrimination, or unlawful reasoning.

Accountability presents a second central challenge. In traditional administrative structures, responsibility can generally be assigned to a public body, an official, a minister, or another identifiable actor. AI systems complicate this architecture because algorithmic decisions are often produced through distributed chains of design, procurement, data collection, software development, deployment, institutional supervision, and human reliance. Public authorities may purchase AI systems from private contractors, use third-party datasets, or integrate models developed outside government. When harm occurs, each actor may claim that another part of the system was responsible. The developer may argue that the public authority misused the software; the public authority may argue that the system behaved unexpectedly; individual officials may claim that they reasonably relied on institutional tools. Comparable responsibility problems have already been identified in discussions of AI-related criminal responsibility, where conventional doctrines encounter difficulty when harmful outcomes arise from complex autonomous systems rather than direct human conduct (Ellamey & Elwakad, 2023). Although public administrative responsibility is doctrinally distinct from criminal responsibility, the underlying attribution problem is similar: law must determine who should answer for consequences produced through human-machine interaction.

The problem of responsibility is particularly important because administrative decision-making is not merely an operational activity; it is an exercise of legally authorized public power. Public agencies cannot avoid accountability simply by embedding legal judgments within technical infrastructures. Administrative discretion must remain subject to lawful purposes, relevant considerations, procedural requirements, and judicial review. This principle is closely related to contemporary debates concerning administrative justice and the use of AI, which emphasize that technological assistance must not erode legal guarantees such as fairness, equality, legality, and access to review (Rajaei & Amiri, 2024). From this perspective, algorithmic governance must be analyzed not as a replacement for legal administration but as a new modality through which administrative authority is exercised. The basic principles of administrative justice therefore remain applicable even when the factual process leading to a decision becomes technologically mediated.

Another important issue concerns the distinction between regulation and innovation. Overly restrictive legal controls may prevent public authorities from using AI to improve efficiency, detect administrative errors, reduce corruption, or enhance service delivery. Conversely, weak regulatory controls may create systems that are efficient but difficult to challenge, discriminatory in effect, or inconsistent with constitutional and administrative guarantees. This tension between control and innovation is widely recognized in contemporary AI regulatory scholarship (Hashemi, 2024). It is particularly acute in public administration because governments are simultaneously regulators and users of artificial intelligence. Public authorities may therefore face

conflicts between their interest in rapid technological modernization and their obligation to protect legal rights. The regulatory task is accordingly not to prohibit algorithmic tools but to establish institutional conditions under which efficiency does not become a justification for diminished accountability.

The legal debate also intersects with wider questions of governance. Research on corporate and organizational governance increasingly emphasizes that AI requires new structures of oversight, internal auditing, accountability, and risk management (Al-Mahameed, 2024). Although corporate governance operates within a different legal setting, its emphasis on institutional controls is relevant to public administration. The use of AI cannot be safely governed only through rules directed at the technical system itself. It also requires supervision of organizational processes such as procurement, testing, documentation, auditing, training, and decision review. Similarly, studies on information technology governance show that internal auditing plays an important role in ensuring that technological systems align with institutional objectives and accountability requirements (Tanbour et al., 2024). These insights suggest that algorithmic governance should be understood as an institutional phenomenon rather than as a narrow issue of software regulation.

The present study therefore examines algorithmic governance in public administration from a legal perspective, focusing specifically on the interrelated challenges of transparency, accountability, and responsibility in AI-based decision-making. It seeks to determine how established principles of public law can be preserved when administrative decisions are generated or substantially influenced by algorithmic systems, and it evaluates the legal mechanisms required to ensure that technological delegation does not become a means of escaping public responsibility.

2. Conceptual and Legal Foundations of Algorithmic Governance

The concept of algorithmic governance lies at the intersection of law, public administration, computer science, and institutional theory. In its broadest sense, it refers to the use of algorithms as instruments for organizing, directing, or influencing collective decision-making. In public administration, algorithmic governance can include systems used to automate routine tasks, assist officials in evaluating evidence, predict future events, rank cases according to risk, or directly generate administrative outcomes. These systems vary significantly in complexity. Some apply fixed rules encoded by programmers, while others use machine learning methods capable of identifying statistical relationships from large datasets. This distinction matters legally because the more adaptive and data-driven a system becomes, the more difficult it may be to identify precisely how a specific output was produced. Yet from the perspective of administrative law, the relevant issue is not whether a system is technically sophisticated but whether its use affects the exercise of public authority. When an algorithm influences access to benefits, taxation, public employment, licensing, enforcement, or another legally protected interest, its operation enters the domain of public law.

The legal foundation of algorithmic governance must begin with the principle of legality. Public authorities may act only within the scope of powers granted by law, and any use of AI must therefore possess a lawful institutional basis. This requirement is often overlooked when governments adopt new technologies through administrative procurement rather than explicit legislation. A public agency may possess general statutory authority to administer a welfare program, but this does not automatically answer whether it may delegate eligibility assessment to an opaque automated model. The doctrine of legality requires consideration of both substantive competence and procedural form. Legal scholars examining AI norm-setting have emphasized the need for dedicated regulatory frameworks capable of defining the legitimate scope of algorithmic activity rather than relying on uncertain analogies with older technologies (Ojaqi et al., 2024). The issue becomes particularly important when algorithms affect fundamental rights because the greater the impact of a decision, the stronger the argument that essential conditions governing its adoption should be determined by law rather than internal administrative policy.

The rule of law provides a second foundational principle. Rule-based government requires that administrative decisions be predictable, reviewable, and constrained by pre-existing legal norms. AI can support these objectives when used to increase consistency or identify departures from legal requirements. Indeed, research on the use of

AI for cyclical oversight of legal implementation suggests that artificial intelligence may strengthen rule-based governance by facilitating systematic monitoring of whether governmental practices comply with applicable legal standards (Bahadori-Jahromi & Fattahi-Zafargandi, 2025). At the same time, algorithms may undermine rule-of-law values if their internal logic is inaccessible, unstable, or based on correlations unrelated to legally relevant criteria. An algorithm may produce consistent outcomes while still applying unlawful criteria. Consistency is therefore not equivalent to legality. A legally compliant algorithm must not only behave predictably but must also operate according to norms that can be traced to lawful authority.

Administrative discretion presents a particularly difficult conceptual problem. Public administration frequently requires officials to interpret open-textured legal standards, assess individual circumstances, balance competing interests, and exercise judgment. Algorithms can formalize part of this process by converting administrative criteria into measurable variables. However, not every legally relevant factor can be easily quantified. Concepts such as reasonableness, necessity, proportionality, vulnerability, good faith, or exceptional hardship may require contextual judgment. If an algorithm reduces these concepts to standardized indicators, the apparent efficiency of automation may conceal a substantive transformation of legal meaning. The use of AI in administrative justice must therefore be evaluated according to whether it preserves the normative character of legal decision-making rather than merely reproducing numerical outputs (Rajaei & Amiri, 2024). A system that treats legal discretion as statistical prediction risks replacing judgment with correlation.

The relationship between algorithms and discretion can take several forms. In some cases, AI may merely provide information that officials are free to accept or reject. In other cases, institutional culture may create strong pressure to follow algorithmic recommendations, effectively converting advisory outputs into binding decisions. This phenomenon can generate "automation bias," whereby decision-makers defer to computational systems even when contrary evidence exists. The problem is especially significant when officials lack the technical expertise necessary to independently evaluate the model. In such circumstances, formal human involvement may become largely symbolic. The existence of a human signature at the end of a decision cannot by itself demonstrate meaningful human control if the official had neither the information nor the institutional authority required to challenge the algorithmic recommendation.

The principle of due process also constitutes a fundamental legal basis for algorithmic governance. Individuals affected by public decisions must ordinarily receive notice, an opportunity to respond, and a meaningful possibility of review where significant rights or interests are at stake. Algorithmic systems can interfere with these guarantees when individuals are unaware that automated methods have been used. If a person does not know that an adverse decision resulted from a risk-scoring model, that person cannot effectively challenge the model's data or reasoning. This problem is compounded when agencies treat algorithmic outputs as objective evidence rather than administrative judgments. Emerging AI laws increasingly attempt to address such issues through obligations relating to notice, explainability, risk assessment, and human oversight (Krook et al., 2025). Nevertheless, the practical adequacy of these safeguards depends on whether they provide information that is sufficiently specific to support legal challenge.

Equality and non-discrimination constitute another central foundation. Artificial intelligence systems operate on data derived from past patterns. If those patterns reflect historical inequalities, the system may reproduce or amplify them. The legal significance of this risk extends beyond intentional discrimination. Public law increasingly recognizes that apparently neutral procedures can create disproportionate effects on protected or vulnerable groups. Algorithmic systems may also rely on proxy variables that indirectly correlate with sensitive attributes. Contemporary scholarship on algorithmic power has therefore emphasized rights conflicts involving equality, autonomy, privacy, and procedural fairness (He & Zhang, 2025). In public administration, these concerns are especially serious because algorithmic classifications may determine access to essential services or increase exposure to enforcement.

Privacy and data protection are similarly integral. AI systems depend heavily on data collection, aggregation, and analysis. Government databases may contain

information about income, health, family relationships, employment, education, taxation, criminal history, or migration status. Linking such datasets can create highly detailed profiles of individuals. Even where individual datasets were lawfully collected, their reuse for algorithmic prediction may raise distinct legal questions concerning purpose limitation and proportionality. The governance challenge is therefore not simply whether data are accurate but whether the state is legally entitled to process them for the specific algorithmic purpose. The expansion of AI legislation reflects increasing recognition that data governance is inseparable from algorithmic governance (Ghamami, 2024).

The principle of proportionality provides an important analytical tool. Public authorities should not deploy intrusive or high-risk AI systems where less restrictive alternatives could achieve the same legitimate purpose. Proportionality requires evaluation of suitability, necessity, and the balance between public benefits and individual burdens. A system used to automate minor administrative tasks may require fewer safeguards than one used to identify individuals as high-risk for fraud or security purposes. Risk-based regulatory models attempt to reflect this logic by imposing stronger requirements on systems capable of producing serious legal effects (Nouralivand, 2024). The legal value of a risk-based approach lies in its capacity to differentiate governance obligations according to the potential severity of harm.

Institutional competence is also relevant. Public agencies using AI need technical expertise sufficient to understand the systems they procure and deploy. Dependence on private contractors creates the danger that agencies may exercise public power through tools they cannot independently evaluate. This challenge resembles problems identified in corporate AI governance, where organizational decision-makers must establish legal and managerial structures capable of supervising technologically complex systems (Al-Mahameed, 2024). In the public sector, the consequences are more significant because the state cannot transfer its constitutional or administrative responsibilities through contract. Outsourcing software development does not outsource legal accountability.

The increasing use of AI across legal domains confirms the need for coherent governance principles. Artificial intelligence has generated regulatory questions in contract law, including issues concerning the legal validity of transactions concluded through autonomous or semi-autonomous systems (Tajik Qaleh et al., 2025). It has also affected labor law, where automated systems may influence recruitment, workplace management, monitoring, and employment decisions (Ghasempour & Safaei, 2024). Competition law is similarly affected by algorithmic practices capable of influencing market structure and competitive behavior (Herati & Herati Ghavi, 2024). These developments demonstrate that AI regulation cannot be confined to a single branch of law. In public administration, however, the overarching principles of legality, due process, equality, proportionality, transparency, and judicial review provide a normative framework through which sector-specific technologies should be evaluated.

A further conceptual distinction must be drawn between machine autonomy and legal autonomy. An AI system may function autonomously in the technical sense that it produces outputs without immediate human intervention. This does not mean that it possesses legal autonomy equivalent to a public authority or natural person. Legal systems remain reluctant to attribute independent legal personality or responsibility to artificial intelligence. Discussions of AI responsibility in other contexts consistently emphasize the difficulties of assigning culpability or legal duties directly to machines (Ellamey & Elwakad, 2023). In public law, this reinforces a basic principle: algorithmic autonomy cannot dissolve institutional responsibility. Decisions produced through AI must remain attributable to legally recognized public bodies or officials.

Finally, algorithmic governance should be understood as a restructuring of administrative processes rather than a simple substitution of machines for humans. AI systems influence which information is considered relevant, how risks are defined, which cases receive priority, and how administrative objectives are operationalized. Regulation must therefore address the full lifecycle of algorithmic systems, including design, procurement, testing, deployment, monitoring, auditing, and withdrawal. Governance research in information technology demonstrates the importance of internal auditing and institutional oversight in ensuring that technological systems remain aligned with organizational standards (Tanbour et al., 2024). In public administration, such mechanisms must be supplemented

by legal safeguards because organizational effectiveness alone cannot guarantee respect for public rights.

3. Transparency, Explainability, and the Right to Know in Algorithmic Decision-Making

Transparency has become one of the central concepts in the legal governance of artificial intelligence because algorithmic decision-making challenges the traditional expectation that public authorities should be able to explain the basis of their actions. Administrative transparency historically serves several functions. It permits citizens to understand how governmental decisions are made, enables courts and oversight bodies to review administrative legality, discourages arbitrary action, and reinforces democratic legitimacy. When administrative systems become algorithmically mediated, these functions remain necessary, but the means of achieving them become more complex. Unlike a conventional written administrative file, an AI system may rely on thousands of variables, statistical relationships, technical parameters, and continuously updated datasets. The legal challenge is therefore not simply to disclose information but to determine what type of information is necessary for meaningful accountability.

The first level of transparency concerns notice. Individuals should ordinarily know when artificial intelligence is materially involved in a decision that affects their rights or interests. Without such notice, it may be impossible to identify relevant procedural protections. This requirement is conceptually straightforward but operationally difficult because public agencies may use AI at multiple stages of decision-making. A system may determine which applications receive additional scrutiny, identify which taxpayers are audited, or generate a risk score later considered by a human official. In such cases, the final decision may appear human even though the underlying process was algorithmically structured. The legal duty to disclose algorithmic involvement should therefore focus on material influence rather than formal authorship. The growing body of transparency legislation in Europe illustrates the movement toward legal obligations requiring organizations to inform individuals about certain forms of automated decision-making (Krook et al., 2025).

A second level concerns system-level transparency. Public authorities should disclose information about the purpose, legal basis, institutional owner, intended use, and risk classification of AI systems. This type of transparency allows citizens, legislators, journalists, and oversight bodies to understand how algorithmic governance is expanding across the public sector. It may also reveal whether agencies are using automated systems in sensitive areas without clear statutory authorization. Such disclosure is consistent with the broader regulatory logic that AI systems should be governed through explicit institutional rules rather than informal experimentation (Ojaqi et al., 2024). Public registers of government algorithms can therefore function as mechanisms of democratic oversight.

A third and more difficult level concerns technical transparency. This involves information about model architecture, training data, variables, validation methods, error rates, testing procedures, and performance metrics. Technical transparency is essential for experts who must evaluate whether a system is reliable or discriminatory. However, technical disclosure alone does not satisfy legal requirements. A citizen challenging an administrative decision may not benefit from access to source code or mathematical documentation without an explanation of how those materials relate to the specific decision. This distinction between technical transparency and legal intelligibility is crucial. Transparency laws that emphasize disclosure without considering comprehensibility may create the appearance of accountability without enabling meaningful contestation (Krook et al., 2025).

Explainability is therefore a separate but related requirement. An explanation should enable an affected individual to understand why a particular decision occurred, what information was considered, and whether the outcome can be challenged. In administrative law, this corresponds closely to the duty to give reasons. Reason-giving performs both procedural and substantive functions. It demonstrates that the authority considered relevant factors, facilitates judicial review, and allows the affected person to identify factual or legal errors. When AI is involved, the duty to give reasons should not be reduced to a generic statement that "the algorithm generated the result." Such a statement merely relocates opacity from the decision-maker to the technical system.

The difficulty of explainability varies according to the type of AI used. Rule-based systems may be relatively easy to explain because their logic can be expressed through identifiable conditions. Machine learning systems, particularly highly complex models, may produce outputs through patterns that are difficult to translate into human-readable reasons. This has led to debate over whether certain systems should be prohibited from high-stakes administrative use if adequate explanations cannot be provided. Rights-based approaches to algorithmic governance increasingly emphasize that opacity cannot be justified solely by technical complexity where significant legal interests are involved (He & Zhang, 2025). The burden should therefore fall on public authorities to select systems compatible with legal obligations, rather than on citizens to accept reduced procedural rights because the chosen technology is difficult to explain.

The right to know also interacts with access-to-information law. Public agencies may resist disclosure on grounds of security, confidentiality, intellectual property, trade secrets, or procurement agreements. These concerns are not trivial. Public disclosure of certain technical details could enable manipulation of systems or reveal proprietary information. Nevertheless, contractual confidentiality cannot automatically override administrative transparency. Governments should not be permitted to create zones of legal opacity by purchasing proprietary systems whose operation they are contractually prohibited from explaining. The tension between control and innovation in AI regulation is especially visible here (Hashemi, 2024). Protecting legitimate commercial or security interests may justify targeted confidentiality, but such restrictions must be balanced against the rights of individuals affected by public decisions.

Procurement law therefore becomes an important component of algorithmic transparency. Public authorities should require contractors to provide sufficient documentation, audit access, testing rights, and explanation capabilities as conditions of procurement. If a vendor refuses to disclose information necessary for legal review, the system may be unsuitable for governmental use. This requirement follows from the broader principle that public authority cannot contract away constitutional or administrative obligations. The same logic appears in discussions of AI governance in corporate settings, where governing bodies must retain effective oversight over systems provided by technical specialists (Al-Mahameed, 2024). In the public sector, oversight requirements are stronger because decisions may affect fundamental rights.

Data transparency is another critical issue. Algorithmic outputs depend not only on model design but also on the quality and representativeness of data. Errors, outdated records, biased datasets, and incomplete information can all produce unlawful administrative outcomes. Individuals should therefore have opportunities to challenge the accuracy of data used in decisions concerning them. The principle is particularly important when systems aggregate information from multiple databases. A person may not know that an outdated record from one administrative system has influenced a decision in another. Transparency must therefore include information about data sources and provide mechanisms for correction.

Bias creates additional complications. Algorithms may produce discriminatory outcomes without explicitly using protected characteristics. Variables such as postal code, employment history, consumption patterns, or educational background may operate as proxies for sensitive attributes. This illustrates why transparency must include not only disclosure of input variables but also analysis of their effects. Rights conflicts generated by algorithmic governance often arise from indirect forms of classification that are difficult to detect without systematic auditing (He & Zhang, 2025). Public authorities should therefore conduct regular impact assessments to identify whether ostensibly neutral models produce unequal outcomes.

Transparency also serves institutional accountability. Public officials need access to sufficient information to evaluate the systems they use. A serious governance failure occurs when government employees treat vendor-provided algorithms as authoritative without understanding their limitations. Research on information technology governance highlights the importance of internal auditing as a mechanism for ensuring that technological systems are subject to organizational control (Tanbour et al., 2024). Algorithmic transparency should consequently operate internally as well as externally. Officials, auditors, regulators, and courts require different levels of access,

but each must receive information appropriate to their role.

A comprehensive transparency regime should therefore be layered. General public transparency should disclose where and why AI systems are used. Individual transparency should provide affected persons with understandable explanations of decisions. Expert transparency should allow qualified auditors and regulators to inspect technical documentation and datasets. Judicial transparency should ensure that courts can obtain the information necessary for meaningful review. This layered approach avoids the false assumption that a single disclosure obligation can satisfy all legal purposes.

The European regulatory experience demonstrates the growing importance of such differentiated obligations (Nouralivand, 2024). Risk-based AI governance increasingly links transparency requirements to the potential severity of harm. High-risk systems are subject to stronger documentation, record-keeping, and oversight duties. This model reflects a broader legal principle: transparency obligations should correspond to the significance of the governmental power being exercised. An algorithm used to schedule appointments does not require the same scrutiny as one used to determine eligibility for essential social benefits.

Transparency is also linked to the prevention of arbitrary administration. A decision that cannot be explained cannot be effectively tested for relevance, proportionality, or consistency with statutory purpose. From this perspective, explainability is not simply a technical feature but a condition of lawful government. Administrative justice requires that public power remain intelligible to those who are subject to it (Rajaei & Amiri, 2024). Where the state cannot explain why an algorithm produced a legally significant result, reliance on that result should be treated with caution.

Finally, transparency should not be treated as an end in itself. Disclosure without remedies may reveal unlawful practices without correcting them. Effective algorithmic governance requires a connection between transparency, review, and institutional responsibility. Information must enable individuals to challenge decisions, oversight bodies to investigate systems, and public authorities to modify or withdraw defective models. Only when transparency is integrated into these broader accountability mechanisms can it fulfill its legal function.

4. Accountability and Legal Responsibility for AI-Based Public Decisions

Accountability is the institutional principle through which public power is connected to explanation, justification, supervision, and consequence. In conventional administrative systems, accountability operates through hierarchical supervision, parliamentary scrutiny, judicial review, disciplinary procedures, civil liability, ombuds institutions, audit mechanisms, and political responsibility. Artificial intelligence complicates these structures because it disperses decision-making across multiple actors and technical processes. An administrative outcome may reflect the combined influence of policymakers, software developers, data scientists, procurement officials, public servants, private contractors, and automated models. The central legal challenge is therefore to ensure that this diffusion of causation does not become a diffusion of responsibility.

The first principle should be institutional attribution. Decisions produced or materially influenced by AI must remain legally attributable to the public authority that deploys the system. A government agency should not be permitted to deny responsibility by arguing that an algorithm generated the result. This principle is necessary because only the public authority possesses the legal mandate to exercise administrative power. Technical autonomy does not create legal competence. Comparable debates in AI responsibility demonstrate the risks of allowing autonomous systems to create gaps in traditional attribution doctrines (Ellamey & Elwakad, 2023). In public law, the solution should be clearer: the agency using the system remains responsible for ensuring legality.

Institutional attribution does not mean that other actors should be exempt from responsibility. Developers and contractors may bear contractual, professional, or civil liability where defective design, negligent testing, inaccurate documentation, or failure to disclose known risks contributes to harm. The challenge is to distinguish external liability among multiple actors from the primary public-law responsibility owed to the individual. Citizens should not be required to determine which private vendor designed a model before

challenging an unlawful governmental decision. The public authority should remain the principal accountable actor, with separate mechanisms allowing it to seek contribution or indemnification from contractors where appropriate.

Responsibility must also extend to procurement decisions. Agencies should not acquire systems that they cannot lawfully operate, explain, or audit. Procurement officials therefore play an important role in algorithmic governance. Contracts should require suppliers to provide documentation, performance data, testing access, correction procedures, and cooperation with oversight bodies. The regulatory literature on corporate governance demonstrates that the introduction of AI requires organizational structures capable of assigning duties and monitoring risk (Al-Mahameed, 2024). Public institutions require even stronger frameworks because procurement decisions may directly affect the exercise of state power.

Human oversight is often proposed as the primary safeguard against algorithmic error. However, the concept must be defined carefully. Formal human presence does not necessarily create meaningful accountability. If an official lacks authority to depart from the algorithmic recommendation, lacks access to the model's reasoning, or lacks sufficient time to review individual cases, the human role may be purely ceremonial. Effective oversight requires competence, independence, access to information, and genuine decisional authority. This corresponds to wider concerns about preserving administrative justice when AI is incorporated into governmental processes (Rajaei & Amiri, 2024). A human reviewer must be able to question the output rather than merely confirm it.

Automation bias increases the importance of this requirement. Officials may place excessive confidence in computational outputs because they appear objective or scientifically sophisticated. Institutional design should therefore encourage critical review rather than passive reliance. Training programs should explain common algorithmic limitations, including data bias, false positives, model drift, and context sensitivity. Internal procedures should also document instances in which officials override automated recommendations. Such records can reveal whether human oversight is functioning in practice.

Algorithmic accountability must also address auditing. Regular audits should evaluate whether systems remain accurate, lawful, and proportionate after deployment. AI models may deteriorate over time as social conditions change or datasets become outdated. This phenomenon, often described as model drift, means that pre-deployment testing is insufficient. Continuous monitoring is necessary. Research on AI-supported oversight of legal implementation suggests that artificial intelligence itself can be used to strengthen compliance monitoring (Bahadori-Jahromi & Fattahi-Zafargandi, 2025). Nevertheless, automated oversight should supplement rather than replace independent human review.

Internal auditing is particularly important because many algorithmic risks may not be visible to courts until harm has already occurred. Information technology governance scholarship demonstrates that effective auditing can improve institutional control over complex technological systems (Tanbour et al., 2024). Public-sector algorithmic audits should examine data quality, error rates, disparate impacts, cybersecurity, compliance with statutory authority, and the adequacy of explanation mechanisms. High-risk systems should also be subject to external or independent audit to reduce conflicts of interest.

Judicial review remains a central accountability mechanism. Courts must be able to examine whether an algorithmic decision was lawful, procedurally fair, rational, and based on relevant considerations. This may require adapting evidentiary rules and standards of review. A court cannot meaningfully review a decision if the agency is unable or unwilling to explain the model that influenced it. Judicial access to technical information should therefore be treated as essential. In some cases, courts may require expert assistance to evaluate model design or statistical evidence. The objective should not be to transform judges into computer scientists but to ensure that technological complexity does not create immunity from legal scrutiny.

The burden of proof is another important issue. Individuals affected by algorithmic decisions often face severe informational asymmetry. The government controls the system, data, documentation, and technical expertise. Requiring claimants to prove the precise internal cause of an erroneous or discriminatory outcome may therefore be unrealistic. Procedural law

should consider presumptions or burden-shifting mechanisms where an individual demonstrates plausible evidence of algorithmic error or disparate impact. This approach is consistent with the broader objective of ensuring effective remedies rather than purely formal access to review.

Discrimination and bias require particularly strong accountability structures. AI systems may reproduce historical inequalities because they learn from existing data. Where public authorities use predictive tools in employment, welfare, policing, education, or regulatory enforcement, discriminatory patterns may have serious consequences. Legal analysis of AI in labor law has already identified concerns regarding automated decision-making and the protection of employee rights (Ghasempour & Safaei, 2024). Similar risks exist in public administration. Agencies should therefore conduct equality impact assessments before and after deployment.

Competition law scholarship also illustrates that algorithmic systems can produce structural effects that exceed the intentions of individual users (Herati & Herati Ghavi, 2024). This insight is relevant to public administration because algorithmic governance may create systemic patterns of exclusion or prioritization even where no single official intended such outcomes. Responsibility must therefore be capable of addressing structural harm rather than focusing exclusively on individual fault.

The question of liability is equally important. Administrative compensation regimes may need adaptation where unlawful algorithmic decisions cause financial or non-financial harm. Traditional liability rules often require proof of fault, causation, and damage. Yet algorithmic systems complicate these elements because causation may be distributed across datasets, model design, institutional procedures, and human reliance. In some high-risk contexts, strict or presumptive liability may be justified to ensure effective redress. Comparable debates in business law increasingly emphasize the need to adapt legal regulation to AI-related risks rather than assuming that conventional doctrines are always sufficient (Pasupuleti, 2024).

Accountability should also include regulatory supervision. Independent authorities may be necessary to inspect public-sector AI systems, investigate complaints, issue guidance, impose corrective measures, or prohibit unlawful deployments. The emergence of dedicated AI regulatory frameworks reflects recognition that decentralized self-regulation is inadequate for high-risk applications (Nouralivand, 2024). Such regulators should coordinate with existing bodies responsible for data protection, equality, administrative justice, auditing, and cybersecurity.

The doctrine of responsibility should furthermore recognize the distinction between technical error and legal error. A system can be technically accurate yet legally defective. For example, an algorithm may predict fraud with high statistical accuracy while relying on criteria that the law does not permit the administration to consider. Governance structures must therefore include legal review in addition to technical validation. AI regulation scholarship emphasizing the need for coherent legal frameworks supports this distinction (Ghamami, 2024).

The use of AI in different sectors confirms that responsibility questions cannot be solved through a single universal doctrine. Corporate governance focuses on duties of boards and managers (Inomovich, 2023). Contract law raises questions about the legal effect of autonomous transactions (Tajik Qaleh et al., 2025). Education may involve intellectual property and governance issues associated with generative AI (Mayana & Santika, 2024). Islamic finance may require alignment between technological innovation and normative principles derived from Maqasid al-Shariah (Najib et al., 2025). These examples demonstrate that AI governance must remain sensitive to the legal context in which systems operate. Public administration is distinctive because it involves coercive public authority and constitutional obligations.

A robust accountability framework should therefore combine ex ante and ex post mechanisms. Ex ante mechanisms include legislation, impact assessment, procurement rules, risk classification, testing, documentation, training, and human oversight. Ex post mechanisms include complaint procedures, audits, judicial review, compensation, regulatory enforcement, and system withdrawal. Neither category is sufficient alone. Prevention without remedies leaves individuals unprotected when failures occur, while remedies without prevention allow avoidable harms to persist.

The ultimate objective of legal responsibility in algorithmic governance is not to identify a single person

to blame for every technical failure. It is to ensure that public institutions remain answerable for the systems through which they exercise authority. Accountability must follow power. If algorithms influence decisions concerning rights, benefits, obligations, or enforcement, the legal system must preserve identifiable lines of responsibility from the technical process back to the public authority that authorized and used it.

5. Conclusion

Algorithmic governance has become an increasingly important feature of contemporary public administration, but its legal implications extend far beyond questions of technological efficiency. Artificial intelligence changes the institutional conditions under which public power is exercised by introducing systems capable of classifying individuals, predicting risks, prioritizing cases, generating recommendations, and in some circumstances producing decisions with minimal human intervention. These developments create significant opportunities for administrative modernization, yet they also place pressure on foundational principles of public law. The central challenge is to ensure that the use of sophisticated computational systems does not erode legality, procedural fairness, equality, reviewability, and institutional responsibility.

The analysis presented in this study demonstrates that algorithmic governance should be understood as a transformation in the structure of administrative decision-making rather than as a neutral technological tool. Algorithms influence which information is considered, how administrative objectives are translated into operational criteria, how risks are defined, and which individuals or cases receive governmental attention. These functions have direct legal significance because they shape the exercise of public authority. For this reason, the legal regulation of algorithmic administration must extend across the entire lifecycle of AI systems, including their design, procurement, training, testing, deployment, auditing, modification, and eventual withdrawal.

Transparency is a fundamental requirement of this regulatory framework. Public authorities should disclose when AI systems materially influence administrative decisions and should provide individuals with understandable explanations of how those systems affected particular outcomes. Transparency must be differentiated according to institutional purpose. General public disclosure should reveal where algorithms are used and under what legal authority. Individual transparency should provide reasons sufficient to support challenge and appeal. Technical transparency should enable qualified experts and regulators to evaluate system performance, while judicial transparency should guarantee that courts can obtain the information necessary for meaningful review. These obligations should not be undermined by commercial confidentiality or procurement arrangements. Where a proprietary system cannot be adequately explained or audited, its suitability for high-stakes governmental use should be questioned.

Explainability should be treated as an extension of the administrative duty to give reasons. The state cannot satisfy its legal obligations merely by informing an individual that an algorithm generated a result. Administrative decisions must remain intelligible enough to allow affected persons to identify relevant facts, challenge inaccurate information, contest discriminatory treatment, and understand the legal basis of the outcome. Technical complexity should not operate as a justification for reduced procedural protection. Public agencies should therefore select and design AI systems in a manner compatible with legal explainability requirements.

Accountability is equally essential. The use of artificial intelligence must not create responsibility gaps in which public authorities, officials, developers, and contractors each attribute harmful outcomes to another actor. The public authority deploying an AI system should remain the primary legally accountable entity because it possesses the statutory power exercised through that system. External contractors may bear additional contractual or civil responsibility, but citizens should not be forced to resolve complex chains of technological causation before challenging unlawful state action. Institutional responsibility must remain attached to the authority that authorized and relied upon the algorithmic process.

Meaningful human oversight must also be preserved. Human involvement cannot be reduced to the formal approval of algorithmic outputs. Officials must possess the competence, information, time, and authority necessary to question automated recommendations.

Institutions should actively address automation bias and create procedures that encourage critical review. Records of overrides, disagreements, and system errors should be maintained because they provide valuable evidence regarding the functioning of human oversight.

Algorithmic auditing should become a routine component of public-sector governance. High-risk systems require regular evaluation of accuracy, data quality, discriminatory effects, model drift, legal compliance, cybersecurity, and explanation capacity. Internal audits should be complemented by independent external review where systems significantly affect rights or public entitlements. Such mechanisms are necessary because many forms of algorithmic harm may become visible only after deployment.

Judicial review must remain fully effective in the algorithmic environment. Courts should not defer to technological systems simply because their operation is complex. Administrative authorities must be capable of explaining how AI influenced disputed decisions, and courts should have access to documentation, expert evidence, and relevant technical records. Procedural rules may also require adjustment to address the severe informational imbalance between individuals and public institutions. Burden-shifting mechanisms may be appropriate in cases where claimants can demonstrate plausible evidence of algorithmic error or discrimination but lack access to internal system information.

Responsibility for algorithmic harm should be addressed through a combination of preventive and remedial measures. Preventive regulation should include statutory authorization, risk assessment, procurement standards, testing requirements, documentation obligations, equality assessments, and human oversight. Remedial mechanisms should include administrative complaint procedures, judicial review, compensation, regulatory enforcement, and the suspension or withdrawal of defective systems. Effective governance requires both dimensions.

The broader normative principle emerging from this analysis is that public authority cannot become less accountable merely because it becomes more technologically sophisticated. Delegating analytical or decisional tasks to artificial intelligence cannot constitute a delegation of constitutional and administrative responsibility. Public institutions remain bound by the same legal obligations regardless of whether decisions are produced through traditional human deliberation, automated rules, machine learning systems, or combinations of human and algorithmic judgment.

A legally sustainable model of algorithmic governance should therefore be built around the principles of legality, proportionality, transparency, explainability, equality, reviewability, and institutional responsibility. These principles do not require the rejection of artificial intelligence in public administration. Rather, they establish the legal conditions under which technological innovation may legitimately be incorporated into government. Artificial intelligence may improve administrative efficiency, consistency, monitoring, and service delivery, but such benefits cannot justify systems that individuals cannot understand, challenge, or hold accountable.

Ultimately, the legitimacy of algorithmic governance will depend not on the sophistication of the technology employed but on the strength of the legal institutions surrounding it. Public administration should use AI as an instrument of lawful governance rather than as a mechanism for distancing decisions from human responsibility. The central legal imperative is therefore to ensure that wherever algorithmic systems influence the exercise of public power, there remains a clear chain of explanation, review, and responsibility connecting the technological process to legally accountable public institutions.

Author's Contribution

Not applicable.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Al-Mahameed, M. (2024). Towards a Legal Framework for Corporate Governance Amid Artificial Intelligence. *Corporate Law & Governance Review*, *6*(3), 113-121. https://doi.org/10.22495/clgrv6i3p12

Bahadori-Jahromi, A., & Fattahi-Zafargandi, A. (2025). Cyclical Oversight of Law Implementation Using Artificial Intelligence and the Promotion of Rule-Based Governance. *Biannual Journal of Research and Development in Public Law*, *2*(4).

Ellamey, Y., & Elwakad, A. (2023). The criminal responsibility of artificial intelligence systems: A prospective analytical study. *Corporate Law & Governance Review*, *5*(1), 92-112. https://doi.org/10.22495/clgrv5i1p8

Ghamami, S. M. M. (2024). An Introduction to the Rationale for Artificial Intelligence Legislation. *Law and Government*, *5*(1).

Ghasempour, A., & Safaei, N. Z. (2024). Legal Issues Arising from Artificial Intelligence in Labor Law. *Scientific Journal of Government and Law*, *5*(1(15)), 59-80.

Hashemi, S. H. (2024). Control or Innovation: Legal Requirements of Regulatory Policies on Artificial Intelligence. *Law and Government*, *5*(1).

He, J., & Zhang, Z. (2025). Algorithm Power and Legal Boundaries: Rights Conflicts and Governance Responses in the Era of Artificial Intelligence. *Laws*, *14*(4), 54. https://doi.org/10.3390/laws14040054

Herati, M., & Herati Ghavi, S. (2024). The impact of artificial intelligence on competition law. *Quarterly Journal of Law and Government*, *5*(1), 45-58.

Inomovich, Y. J. (2023). Legal Regulation of the Use of Artificial Intelligence in Corporate Governance. *Uzbek J. Law Digi. Policy*, *1*(3). https://doi.org/10.59022/ujldp.94

Krook, J., Winter, P., Downer, J., & Blockx, J. (2025). A systematic literature review of artificial intelligence (AI) transparency laws in the European Union (EU) and United Kingdom (UK): a socio-legal approach to AI transparency governance. *Ai and Ethics*, *5*(4), 4069-4090.

Mayana, R. F., & Santika, T. (2024). Generative Artificial Intelligence in Education and Its Governance: Perspective of Copyright Law. *Jurnal Pendidikan Terbuka Dan Jarak Jauh*, *25*(1), 1-14. https://doi.org/10.33830/ptjj.v25i1.7471.2024

Najib, N. M., Basarud-din, S. K., & Fazial, F. (2025). Artificial Intelligence (AI) in Islamic finance: A Maqasid Al-Shariah perspective. *International Journal of Law, Government and Communication*, *10*(40), 41-50. https://doi.org/10.35631/IJLGC.1040003

Nouralivand, Y. (2024). Analysis: The European Union Artificial Intelligence Act, the world's first law on artificial intelligence governance. *National Security Monitor*(142), 113-122.

Ojaqi, H., Soleimani Rouzbehani, F., & Zohourian Nadali, I. (2024). The Doctrine of Artificial Intelligence Norm-Setting and Regulation. *Law and Government*, *5*(1).

Pasupuleti, M. K. (2024). Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance. 19-35. https://doi.org/10.62311/nesx/66203

Rajaei, M., & Amiri, A. (2024). Principles Governing the Use of Artificial Intelligence in the Realization of Administrative Justice. *Interdisciplinary Studies in Society, Law, and Politics*, *4*(4), 1-8. https://doi.org/10.61838/kman.isslp.4.4.5

Samiya, K., & Bourane, A. (2025). Law in the Age of Artificial Intelligence: Challenges and Prospects. *Lex Localis - Journal of Local Self-Government*. https://doi.org/10.52152/fkhaga03

Tajik Qaleh, Z., Bahmani, M., & Moeir Mohammadi, M. A. (2025). Principles Governing the Validity of Contracts Concluded by Artificial Intelligence in Iranian and English Law. *Civil Law Knowledge*, *14*(28), 43-61.

Tanbour, K. M., Nour, A. I., & Halawa, S. M. A. (2024). The Impact of Internal Auditing on the Effectiveness of Information Technology Governance in Insurance Companies Listed on the Palestine Exchange. In *Artificial Intelligence and Economic Sustainability in the Era of Industrial Revolution 5.0* (pp. 359-377). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56586-1_28