2026, Cilt 3, Sayı 4, 315-318

OPEN ACCESS
ISSN: 3062-262X

Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)

Algorithmic Governance and the Rule of Law: Building Accountable Artificial Intelligence in Public Administration

Dr. Alexander Vance, Department of Law, European University Institute (EUI), Florence School of Regulation Florence, Italy, alexander.vance@eui.eu

Article History
Received: 02/05/2026; Accepted: 05/06/2026; Published: 01/09/2026

Abstract
Artificial intelligence is moving from experimental laboratories into the ordinary work of public administration. Governments increasingly use algorithmic systems to allocate benefits, detect fraud, assess risk, prioritize inspections, and support decisions affecting migration, policing, employment, and access to public services. These systems may improve consistency and administrative capacity, but they also create constitutional and democratic risks when their logic is opaque, their data reproduce historical inequalities, or their outputs are treated as neutral facts rather than contestable judgments. This article examines the relationship between algorithmic governance and the rule of law through a doctrinal and comparative analysis of European legal instruments and international principles. It argues that legality cannot be protected by transparency alone. Public-sector artificial intelligence requires a layered accountability model combining a clear legal basis, impact assessment before deployment, meaningful human responsibility, procedural rights for affected persons, independent oversight, and continuous auditing after implementation. The article compares the European Union Artificial Intelligence Act, the General Data Protection Regulation, the Council of Europe Framework Convention on Artificial Intelligence, and the UNESCO Recommendation on the Ethics of Artificial Intelligence. It concludes that the central policy question is not whether governments should use algorithmic systems, but under what institutional conditions automated assistance can remain subordinate to public reason, equality, and reviewable human judgment.

Keywords: algorithmic governance; rule of law; public administration; artificial intelligence; due process; accountability; fundamental rights.

1. Introduction

The contemporary state is becoming increasingly data-intensive. Public agencies collect, classify, and process information at a scale that exceeds the capacity of traditional administrative routines. Artificial intelligence (AI) promises to transform this capacity into faster decisions, targeted interventions, and more personalized public services. Yet the administrative use of AI is not merely a technical modernization project. It changes how public power is exercised, how discretion is distributed, and how citizens can challenge decisions.

The legal difficulty arises because algorithmic systems can influence outcomes without appearing to make decisions in the conventional sense. A system may rank applications, generate a risk score, identify an anomaly, or recommend an enforcement action while a public official formally signs the final decision. In practice, however, the official may rely heavily on the system, particularly where workload, institutional incentives, or technical complexity make independent verification difficult. The result may be a form of automation by deference: human involvement remains visible on paper, while the substantive reasoning is delegated to a model.

This development raises a classic rule-of-law concern. Public decisions must be attributable to a lawful authority, guided by intelligible standards, applied without arbitrary discrimination, and open to effective review. Algorithmic governance can support these objectives when it reduces inconsistency and exposes patterns that would otherwise remain hidden. It can

undermine them when the relevant data, model, or procurement arrangement prevents affected persons and reviewing institutions from understanding why a particular result occurred. The issue is therefore not simply whether an algorithm is accurate. A legally acceptable public decision must also be explainable at the level required for contestation, institutionally accountable, and compatible with equality and human dignity (Kroll et al., 2017; Yeung, 2018).

This article develops three claims. First, algorithmic governance should be treated as an institutional form of administrative power rather than as a neutral tool. Second, procedural safeguards must be designed around the full life cycle of an AI system, from procurement and data selection to deployment, monitoring, appeal, and retirement. Third, transparency is necessary but insufficient: an agency can disclose technical information while still denying individuals a meaningful opportunity to challenge the decision that affects them. The analysis is doctrinal and comparative. It draws on major European and international instruments and uses the rule of law as a normative framework for assessing their strengths and limits.

2. Algorithmic Governance and the Rule of Law

Algorithmic governance refers to the use of computational models, automated classification, and data-driven prediction to structure public decisions and conduct. It includes fully automated decisions, but it is broader than automation. A public body may use a model only to prioritize cases or advise an official, yet the model can still shape the distribution of attention and resources. This is important because administrative power is exercised not only through final orders but also through queues, inspections, eligibility thresholds, and the selection of people for closer scrutiny.

Bovens and Zouridis (2002) described a shift from street-level bureaucracies to system-level bureaucracies, in which discretion moves from individual officials toward information systems and organizational rules. AI intensifies that shift. Instead of eliminating discretion, it may relocate discretion to choices about labels, training data, proxy variables, objective functions, thresholds, and acceptable error. These choices are often made by a combination of civil servants, vendors, data scientists, and political decision-makers. If responsibility is dispersed across this chain, the citizen may encounter a decision without an identifiable decision-maker.

2.1 The rule-of-law benchmark

For present purposes, the rule of law has four connected dimensions. The first is legality: public bodies must have a valid legal basis and must act within the limits of their authority. The second is non-arbitrariness: decisions must be based on relevant reasons rather than hidden or impermissible proxies. The third is procedural fairness: affected persons must receive sufficient information and a genuine opportunity to be heard or to obtain reconsideration. The fourth is institutional accountability: an independent body must be able to investigate, correct, and, where necessary, stop an unlawful system. These dimensions apply whether the decision is made by a person, a model, or a person relying on a model.

3. Due Process, Transparency, and Contestability

The first safeguard is a legally intelligible basis for deployment. Agencies should identify the public purpose of an AI system, the categories of persons affected, the types of data used, the expected benefits, and the foreseeable rights impacts before procurement or implementation. A vague mandate to improve efficiency is not enough where a system can affect access to housing, social protection, education, immigration status, or criminal justice. The more intrusive the use, the more specific the legal authorization and safeguards should be.

The second safeguard is transparency, but transparency must be understood in layers. Institutional transparency concerns who owns the system, who procured it, who operates it, and which official is responsible for outcomes. Data transparency concerns the provenance, quality, representativeness, and retention of the data. Model transparency concerns the system's purpose, input variables, performance limits, and error patterns. Individual transparency concerns the reasons a particular person was affected. These layers serve different audiences and cannot be replaced by publishing a general statement that an agency uses AI.

A related distinction is the difference between explanation and justification. An explanation describes how a system produced an output. A justification addresses why the output should be accepted as legally and factually appropriate in the individual case. A feature-importance chart may explain that income, location, or prior contact with an agency influenced a prediction, but it does not by itself establish that the variable was lawful, reliable, or fair. Public administration requires reasons that can be connected to legal criteria and challenged by the affected person (Wachter, Mittelstadt, & Floridi, 2017).

3.1 Bias, equality, and administrative error

Algorithmic discrimination can arise even when protected characteristics are excluded. Geographic location, language, disability-related information, employment history, or patterns of service use may function as proxies. Historical data may also encode prior institutional bias. A system trained on unequal enforcement records can reproduce unequal enforcement with statistical efficiency. Therefore, equality review must examine both outputs and the institutional process that produced the training data. Accuracy metrics should be disaggregated across relevant groups, and agencies should document which errors are most harmful. In rights-sensitive settings, reducing false negatives may be more important than maximizing overall predictive accuracy.

4. Comparative Legal Responses

4.1 The European Union approach

The European Union has developed a layered framework rather than a single rule. The General Data Protection Regulation (GDPR) governs the processing of personal data and provides safeguards for certain forms of solely automated decision-making under Article 22, together with transparency and access rights. The GDPR does not create a simple universal right to receive the source code of a model. Its contribution is better understood as a set of controls over lawful processing, purpose limitation, data minimization, accuracy, and individual rights.

The Artificial Intelligence Act adds a risk-based framework. It prohibits selected uses, regulates high-risk systems, and creates obligations for providers and deployers. High-risk public-sector uses require attention to risk management, data governance, technical documentation, record-keeping, human oversight, accuracy, robustness, and cybersecurity. Article 27 also requires certain deployers to conduct a fundamental-rights impact assessment before using a high-risk system. These measures are significant because they move accountability upstream, before an individual decision is made.

Nevertheless, a risk-based model may leave gaps. A system can create substantial social harm through cumulative low-level decisions while falling outside a category that attracts the strongest obligations. Formal compliance may also become a checklist exercise if agencies treat impact assessments as procurement documents rather than as living instruments. Effective implementation therefore depends on supervisory capacity, public registers, internal expertise, and accessible remedies. The AI Act should be read together with data-protection, equality, administrative, and constitutional law rather than as a substitute for them.

4.2 International and regional principles

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law frames AI governance around public values and institutional duties. Its importance lies in connecting technical risk with democratic resilience, human rights, and the preservation of legal remedies. It encourages states to assess impacts, prevent discrimination, ensure accountability, and provide procedural guarantees. Similarly, the UNESCO Recommendation on the Ethics of Artificial Intelligence emphasizes proportionality, human oversight, transparency, explainability, accountability, and the protection of human dignity. Although soft-law instruments differ from binding legislation, they help articulate common principles across jurisdictions and can guide interpretation, procurement, and policy design.

5. A Public-Sector Accountability Model

A workable accountability model should follow the system's life cycle. The first stage is authorization and necessity. The public body should identify a lawful purpose and show that AI is necessary or proportionate compared with less intrusive alternatives. The second stage is design and procurement. Contracts should require access to documentation, audit cooperation, incident reporting, data governance, security controls, and the ability to suspend or terminate the system. Commercial confidentiality should not be allowed to erase the agency's legal responsibility to explain public decisions.

The third stage is pre-deployment assessment. An agency should map affected groups, test data quality, evaluate foreseeable discriminatory effects, define human-oversight duties, and specify the circumstances in which the system must not be used. The assessment should include a clear allocation of responsibility: a named official or unit must be empowered to question, override, or stop the model. Human oversight is meaningless if the person responsible lacks time, expertise, authority, or access to the information needed for independent judgment.

5.1 Individual remedies and institutional oversight

The fourth stage is operation and review. Individuals should be informed when an algorithm materially influences a public decision, unless a narrowly defined exception is justified by law. They should receive a comprehensible statement of the decisive reasons, the relevant evidence, and the available procedure for correction or appeal. Review must be capable of changing the outcome; a complaint channel that only records dissatisfaction is not a remedy. Agencies should also publish aggregate information about system performance, error rates, complaints, suspensions, and corrective actions, subject to privacy and security constraints.

The fifth stage is independent oversight. Data-protection authorities, equality bodies, ombuds institutions, courts, audit offices, and sectoral regulators each see different aspects of algorithmic power. Coordination among them is essential. A technical audit may identify drift or disparate error rates, while an administrative court may assess legal authority and reasons. No single institution can replace the others. Oversight should also extend to vendors and subcontractors, because outsourcing software does not outsource constitutional responsibility.

5.2 A minimum governance checklist

For public agencies, the following minimum questions operationalize the model: (1) What legal rule authorizes the use? (2) What public problem is the system intended to solve? (3) Who may be affected, directly or indirectly? (4) Are the data accurate, relevant, representative, and lawfully obtained? (5) Which variables may operate as proxies for protected characteristics? (6) What is the system's error profile across groups? (7) Who is accountable for each decision? (8) How can a person obtain reasons, correction, and human reconsideration? (9) Which independent body can audit or halt the system?

and (10) What conditions trigger retraining, suspension, or withdrawal? These questions should be documented before deployment and revisited throughout the system's operation.

6. Discussion

The central tension is between administrative scale and democratic justification. AI can help agencies manage complex tasks, but efficiency is not a constitutional value that overrides legality and equality. Nor is human decision-making automatically fair. Officials can be biased, inconsistent, or overwhelmed. The appropriate response is not to romanticize human discretion or to treat statistical prediction as objective. It is to design institutions in which computational assistance remains answerable to legal reasons, professional judgment, and public review.

7. Conclusion

Algorithmic governance will become an ordinary feature of the administrative state. Its legitimacy will depend less on whether systems are described as intelligent than on whether the institutions deploying them can explain, justify, monitor, and correct their effects. A rule-of-law approach requires clear authorization, rights-impact assessment, responsible human oversight, meaningful individual remedies, independent supervision, and continuous evaluation. The strongest framework is therefore layered: technical safeguards support, but cannot replace, legal and democratic accountability. Public authorities should adopt AI only when they can preserve the chain of responsibility from the model's design to the individual's right to challenge the decision. Under those conditions, AI may strengthen public administration without displacing the principles that make public power legitimate.

References

Bovens, M., & Zouridis, S. (2002). From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control. Public Administration Review, 62(2), 174-184. https://doi.org/10.1111/0033-3352.00168

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1-33.

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Council of Europe.

European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People-An ethical framework for a good AI society. Minds and Machines, 28, 689-707. https://doi.org/10.1007/s11023-018-9482-5

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633-705.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1-21. https://doi.org/10.1177/2053951716679679

OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD Publishing.

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. Fordham Law Review, 87(3), 1085-1139.

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76-99. https://doi.org/10.1093/idpl/ipy005

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. Regulation & Governance, 12(4), 505-523. https://doi.org/10.1111/rego.12158

Submission note: Replace all bracketed author and institutional placeholders, verify the target journal's author guidelines, and conduct a final originality, citation, and legal-update review before submission.