ARTICLE

AI IN PUBLIC ADMINISTRATION: A COMPARATIVE ANALYSIS OF ACCOUNTABILITY & DUE PROCESS SAFEGUARDS IN EU & INDIA

Gouri Vijayvergiya[1]

Abstract

Governments worldwide are increasingly turning to artificial intelligence (AI) to transform public administration; improving efficiency, streamlining services, and supporting complex decision-making. Yet this technological shift brings thorny questions about accountability, transparency, and whether citizens receive fair treatment when algorithms make decisions that affect their lives. This paper compares how two very different democracies, the European Union and India are regulating AI-driven administrative decisions, zeroing in on accountability and due process protections.

What emerges is a striking contrast. The EU has built a comprehensive, legally binding framework through its AI Act 2024 and the General Data Protection Regulation (GDPR), creating enforceable rights to explanation, human oversight, and the ability to challenge automated decisions. India, meanwhile, has taken a different path. Its 2025 India AI Governance Guidelines articulate important principles but remain voluntary. While India's Constitution provides foundational rights protections, the country lacks dedicated laws specifically governing automated decision-making in public administration.

This gap matters. As AI systems become more embedded in welfare delivery, policing, and border control, India will need stronger, enforceable safeguards to ensure administrative decisions remain transparent, accountable, and faithful to due process principles.

Keywords – Artificial Intelligence, Automated Decision-Making (ADM), Public Administration, Accountability, Fundamental Rights, Algorithmic Governance, Artificial Intelligence Act, General Data Protection Regulation (GDPR), Digital Personal Data Protection Act, 2023, European Union, India.

I. INTRODUCTION

Artificial intelligence is reshaping public administration in profound ways. Governments now use AI to automate welfare eligibility checks, detect fraud, predict crime patterns, screen immigration applications, and deliver citizen services. These technologies promise real benefits: faster decisions, lower costs, and more efficient use of public resources. But they also raise uncomfortable questions

[1] LL.M Candidate, MIT WPU Pune

about who is accountable when algorithms make mistakes, how transparent these systems really are, and whether citizens get a fair hearing when machines decide their fate.[2]

The shift to AI-driven decision-making represents a fundamental change in how administrative power operates. Traditional bureaucratic decisions came from identifiable officials who could be questioned and held responsible. AI systems, by contrast, often rely on complex algorithms that even their creators struggle to fully explain. When an automated system denies someone welfare benefits, flags them as a fraud risk, or places them on a watchlist, determining who is responsible becomes far from straightforward. These concerns are especially acute in high-stakes areas like welfare, criminal justice, healthcare, and immigration, precisely where decisions can make or break people's lives.[3]

Different jurisdictions have responded in different ways. The European Union has embraced a rights-based regulatory model anchored in the AI Act 2024 and GDPR, establishing legally enforceable safeguards around transparency, human oversight, and the right to contest automated decisions. India has charted a more flexible course, relying on constitutional protections, sector-specific rules, and the voluntary India AI Governance Guidelines 2025.

This paper examines How do the European Union and India differ in their legal and institutional safeguards for accountability and due process in AI-driven public administration? Using comparative legal analysis, I have examined the regulatory frameworks, oversight institutions, and procedural protections each jurisdiction has developed.

While both the EU and India recognise the need for responsible AI governance, the EU has built a far more robust and enforceable framework for protecting accountability and due process. India's approach, though grounded in important constitutional principles, remains heavily dependent on voluntary guidelines and after-the-fact judicial intervention. As AI becomes more deeply woven into the fabric of governance, ensuring that administrative power stays transparent, accountable, and subject to legal scrutiny will be essential for maintaining public trust and upholding the rule of law.

II. CONCEPTUAL FRAMEWORK

Defining AI in Public Administration

When we talk about AI in public administration, we're referring to a wide array of technologies that help governments make decisions, analyse data, and deliver services. This includes automated decision-making (ADM) systems that process applications without human intervention, algorithmic risk assessment tools that flag individuals for scrutiny, predictive analytics that forecast crime or fraud patterns, and machine learning models that classify citizens for resource allocation or law enforcement purposes.[4]

These applications span a broad spectrum. On one end, you have relatively benign tools like chatbots that help citizens navigate government websites. On the other, you have high-stakes systems determining who gets welfare benefits, who crosses borders without additional screening, or which neighbourhoods receive heightened police patrols. The latter directly affect people's rights, opportunities, and life chances; making accountability and fairness non-negotiable.

---

[2] See Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015) (discussing opacity and accountability in algorithmic decision-making).

[3] See OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (adopted May 22, 2019, amended Nov. 8, 2023), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Accountability in Administrative Law

Accountability lies at the heart of democratic public administration. It means that decision-makers must explain their actions, own up to their choices, and face consequences when those choices cause harm or violate rules. This is how citizens keep governments in check.

AI complicates this picture considerably. When an algorithm produces a biased, inaccurate, or outright harmful outcome, who do we hold accountable? The government agency that deployed it? The private company that built it? The officials who oversaw its implementation? The lines blur quickly.

Scholars have found it helpful to break accountability into three interconnected pieces. First, answerability: the obligation to provide explanations and justify decisions. Second, responsibility: figuring out who is causally connected to a particular outcome. Third, liability: the legal or regulatory consequences that follow when rules are broken or harm occurs. Together, these dimensions help us think through how to maintain accountability when algorithms increasingly shape important public decisions.[5]

Due Process and Administrative Justice

Due process is the bedrock of fair administration. It ensures that decisions affecting individuals are made reasonably, transparently, and with proper safeguards. This includes the right to a fair hearing, the requirement that decisions be properly reasoned, protection against arbitrary action, and access to effective remedies when things go wrong.

These protections take on added urgency in the age of AI. People affected by automated decisions should be able to understand how and why a decision was reached, challenge outcomes before a human decision-maker, and seek review through judicial or administrative channels. Without these safeguards, algorithmic systems risk becoming impenetrable "black boxes" that operate beyond public scrutiny undermining procedural fairness and eroding trust in government.[6]

Theoretical Anchors

The EU-India comparison reflects two fundamentally different philosophies of AI governance. The EU follows a rights-based, precautionary model that puts fundamental rights protection front and centre. This approach relies on proactive safeguards: risk assessments, oversight mechanisms, and legally binding obligations designed to prevent harm before it occurs.

India has chosen a principle-based, innovation-friendly path. Rather than heavy-handed regulation, it promotes technological development through flexible frameworks, sector-specific adaptation, and voluntary adherence to broad ethical principles.[7]

---

[4] See Mark Bovens, Analysing and Assessing Accountability: A Conceptual Framework, 13 European Law Journal 447, 447–68 (2007) (conceptualising accountability in terms of an actor, a forum, and an obligation to explain and justify conduct).

[5] See Council of Europe, Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems (8 Apr. 2020), https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[6] Ministry of Electronics and Information Technology, India AI Governance Guidelines, supra note 13. Characterisations such as 'innovation-friendly' and 'developmental state model' are analytical interpretations and should be framed as the author's analysis rather than as direct statements of law.

These differences aren't accidental. They reflect deeper constitutional and political traditions. The EU's regulatory philosophy grows out of its post-war commitment to human rights constitutionalism. India's approach, meanwhile, is shaped by developmental priorities, economic growth objectives, and the pursuit of technological self-reliance.

Understanding these contrasting models matters because they shape how each jurisdiction balances innovation with accountability, efficiency with fairness, and technological progress with individual rights protection. These differences set the stage for the comparative analysis that follows.

III. EU FRAMEWORK: ACCOUNTABILITY & DUE PROCESS SAFEGUARDS

Legal Architecture

The European Union has constructed one of the world's most comprehensive AI regulatory frameworks. Its approach rests on three pillars: the AI Act 2024, the General Data Protection Regulation (GDPR), and a broader digital governance ecosystem that includes the Data Governance Act and Digital Services Act.[8]

The AI Act 2024 is the centrepiece. It adopts a risk-based classification system, banning certain applications outright like social scoring systems and some forms of real-time biometric surveillance in public spaces while imposing strict requirements on "high-risk" AI systems used in public administration, law enforcement, education, and critical services.[9]

Providers and deployers of high-risk AI face substantial obligations: conducting conformity assessments, maintaining detailed technical documentation and audit trails, ensuring meaningful human oversight, and registering systems in a central EU database. Non-compliance carries teeth: penalties can reach up to 4% of a company's global annual turnover.[10]

The GDPR complements this framework with robust data protection rights. Article 15 grants individuals the right to access information about how their data is processed. Article 22 protects against decisions based solely on automated processing when those decisions have legal or similarly significant effects. Recital 71 emphasises transparency, meaningful explanations, and the ability to challenge automated decisions.[11]

Together, these provisions translate abstract accountability principles into concrete legal obligations. Public authorities must demonstrate compliance and provide individuals with meaningful information about how algorithms influence decisions affecting them. By marrying data protection rights with AI-specific regulation, the EU aims to ensure that technological innovation remains compatible with transparency, accountability, and fundamental rights.

---

[7] Regulation (EU) 2024/1689, supra note 1; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 1 (4 May 2016); Regulation (EU) 2022/868 (Data Governance Act); Regulation (EU) 2022/2065 (Digital Services Act).

[8] Artificial Intelligence Act, supra note 1, arts. 5–6 and Annex III. The Act prohibits specified AI practices and classifies certain uses as high-risk; the exact scope depends on the statutory provisions and exceptions.

[9] Id. arts. 9, 11–15, 17, 26–27, 49, 99. Article 27 requires certain public-sector deployers of specified high-risk systems to conduct a fundamental-rights impact assessment; not every public-sector AI use is covered by that article.

[10] GDPR arts. 13(2)(f), 14(2)(g), 15(1)(h), 22 and recital 71. Article 22 is limited to decisions based solely on automated processing that produce legal effects or similarly significantly affect a person, subject to exceptions and safeguards.

Institutional Mechanisms

The EU's governance architecture features multiple layers of oversight. At the European level, the EU AI Office coordinates implementation, maintains the high-risk AI database, and issues regulatory guidance. National supervisory authorities monitor compliance and conduct investigations within member states. The European Data Protection Board promotes consistent GDPR application across borders.[12]

Judicial oversight adds another accountability layer. Article 8 of the European Convention on Human Rights has been interpreted to protect privacy, data protection, and aspects of algorithmic fairness. The Court of Justice of the European Union has repeatedly emphasised that automated decision-making must respect fundamental rights, including transparency and access to effective remedies.[13] These institutions create a dense web of accountability ensuring AI systems remain subject to legal scrutiny and public oversight.

Operational Safeguards

The AI Act embeds several concrete safeguards to protect accountability and due process:

- Human Oversight: High-risk AI systems must allow meaningful human intervention, enabling operators to review, modify, or override automated outputs.
- Duty to State Reasons: Public authorities must provide clear, understandable explanations for AI-assisted decisions, including the key factors influencing outcomes.
- Fundamental Rights Impact Assessments (FRIAs): Before deploying high-risk AI, organisations must assess potential risks to fundamental rights and implement mitigation measures.[14]
- Contestability: Individuals affected by AI-driven decisions can challenge outcomes, request human review, and seek redress through supervisory authorities.
- Audit Trails: Providers must maintain detailed technical documentation and system logs to support transparency and post-deployment investigations.

These safeguards work together to keep AI systems transparent, accountable, and rights-respecting.

Case Examples

Real-world cases show how these accountability mechanisms play out. In the Netherlands, courts struck down the SyRI welfare fraud detection system for lacking adequate transparency and proportionality safeguards. France now requires public authorities to disclose when AI assists decisions affecting individual rights. The iBorderCtrl pilot project faced sharp criticism over insufficient human oversight and potential bias in risk assessments.[15]

---

[11] Artificial Intelligence Act, supra note 1, arts. 64–70 (AI Office and governance) and arts. 74–77 (market surveillance and safeguards); GDPR arts. 51–59 (supervisory authorities) and arts. 63–76 (consistency mechanism and European Data Protection Board).

[12] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221; Case C-634/21, OQ v. Land Hessen (SCHUFA Holding AG), ECLI:EU:C:2023:957 (Dec. 7, 2023) (interpreting GDPR art. 22 in the context of credit scoring).

[13] Artificial Intelligence Act, supra note 1, art. 27. This provision applies to specified deployers and categories of high-risk AI; it is not a universal fundamental-rights impact assessment duty for every AI system.

[14] Rechtbank Den Haag [District Court of The Hague], NJCM c.s. v. State of the Netherlands, ECLI:NL:RBDHA:2020:1878 (Feb. 5, 2020) (holding the SyRI legislation incompatible with art. 8 ECHR). The separate assertions about France's

These examples demonstrate the EU's willingness to enforce accountability through judicial review and legislative refinement even as AI adoption accelerates.

IV. INDIA FRAMEWORK: ACCOUNTABILITY & DUE PROCESS SAFEGUARDS

Legal and Policy Architecture

India's AI governance landscape looks quite different. Rather than a dedicated AI law, India relies on constitutional protections, sector-specific regulations, and non-binding policy guidelines.

The India AI Governance Guidelines (2025) articulate seven core principles Trust, People First, Fairness, Accountability, Transparency, Reliability and Safety, and Inclusivity. While ethically important, these principles remain voluntary. Proposed institutions like the AI Governance Group and AI Safety Institute are still taking shape.[16]

The Digital Personal Data Protection Act, 2023 (DPDP Act) regulates personal data processing and grants rights to access, correction, and grievance redressal. But unlike the GDPR, it lacks specific safeguards for automated decision-making no right to explanation, no guaranteed human review.[17]

Constitutional protections under Articles 14 (equality), 19 (freedoms), and 21 (life and liberty, interpreted to include privacy) provide the primary safeguard against arbitrary state action. The Supreme Court's landmark Puttaswamy judgment (2017) reinforced this framework by recognising privacy as a fundamental right and emphasising proportionality in state data processing.[18]

Sector-specific measures like the RBI's FREE-AI framework for finance and MeitY advisories on deepfakes address particular risks but don't create comprehensive ADM accountability.[19]

Overall, India's approach remains principle-based, with limited statutory safeguards specifically targeting automated decision-making.

Institutional Mechanisms

India's AI governance architecture is still evolving. The proposed AI Governance Group (inter-ministerial) will coordinate policy, while the AI Safety Institute will focus on research and capacity-

disclosure requirements and the iBorderCtrl project require their own specific sources and are not established by this judgment.

[15] Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (Nov. 2025), https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2186639. The Guidelines set out seven guiding principles and recommendations; the legal status of each proposed institution and recommendation should be described with precision.

[16] Digital Personal Data Protection Act, No. 22 of 2023, §§ 11–14, 17, Gazette of India, Extraordinary, Aug. 11, 2023, https://www.meity.gov.in/data-protection-framework. The Act does not contain a GDPR Article 22 equivalent; however, the scope of its provisions and exemptions should be analysed separately rather than equated with the absence of all other legal safeguards.

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) (recognising privacy as a fundamental right and discussing legality, legitimate state aim, and proportionality).

[18] Reserve Bank of India, Report of the FREE-AI Committee / Framework for Responsible and Ethical Enablement of Artificial Intelligence (2025). The paper should cite the exact report or official RBI publication supporting the description of this framework.

building. The Data Protection Board of India, established under the DPDP Act, adjudicates data breach complaints but lacks explicit jurisdiction over algorithmic fairness or ADM disputes.[20]

In the absence of dedicated oversight, courts have stepped in. The Supreme Court's Aadhaar jurisprudence imposed proportionality limits on biometric authentication and mandated data minimisation. Several High Courts have scrutinised predictive policing and facial recognition deployments on privacy and discrimination grounds.[21]

But these interventions are reactive and case-specific—highlighting the absence of a comprehensive institutional framework for AI accountability.

Operational Gaps

Despite constitutional protections, India's framework exhibits significant accountability deficits:

- No Statutory ADM Rights: Unlike GDPR Article 22, the DPDP Act grants no right against solely automated decisions or mandatory human review.
- Voluntary Compliance: The 7 Sutras are non-binding, relying on corporate self-regulation rather than legal enforcement.
- Weak Transparency: No legal duty exists for public authorities to disclose AI use in decision-making or provide algorithmic explanations.
- National Security Exceptions: The DPDP Act grants broad exemptions to government agencies for national security and law enforcement, creating surveillance risks without adequate oversight.[22]
- Limited Contestability: Grievance mechanisms address data breaches but not algorithmic bias, errors, or unfair ADM outcomes.

These gaps underscore the urgent need for statutory ADM safeguards to complement constitutional litigation.

Case Examples

Aadhaar-enabled Direct Benefit Transfers (DBT) have streamlined welfare delivery but faced litigation over exclusion errors, lack of alternative authentication, and opaque algorithmic matching. Automated Facial Recognition Systems (AFRS) deployed by police in Delhi, Telangana, and elsewhere operate without statutory authorisation, raising concerns about misidentification and chilling effects on dissent. Predictive Policing Pilots in Hyderabad and Pune use historical crime data

[19] Ministry of Electronics and Information Technology, India AI Governance Guidelines, supra note 13 (recommending institutional arrangements including an AI Governance Group and AI Safety Institute). The manuscript should verify the operational status of these bodies as of the article's publication date.

[20] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (India). These decisions address privacy, proportionality, and Aadhaar's legal framework; they do not, by themselves, establish that High Courts have scrutinised all the predictive-policing and facial-recognition examples stated in the text.

[21] Digital Personal Data Protection Act, supra note 15, § 17. The Act contains specified exemptions, including provisions relating to national security and public order, but the paper should identify the exact clause and legal conditions rather than describe all government processing as broadly exempt.

to allocate patrols, risking reinforcement of biased enforcement patterns without independent audits.[23]

These examples highlight why India needs dedicated ADM legislation—not just constitutional remedies after harm occurs.

V. COMPARATIVE ANALYSIS

The table below captures key differences between EU and India approaches:

Dimension	European Union	India
Regulatory Model	Binding, risk-based (AI Act + GDPR)	Voluntary, principle-based (7 Sutras)
Legal Basis for ADM	Statutory authorisation required; FRIAs mandatory	No specific ADM law; relies on constitutional doctrines
Accountability Mechanisms	Clear duty-artefact-forum matrix; audit trails; fines up to 4% turnover	Diffused accountability; grievance redressal proposed but not enforced
Due Process Safeguards	Right to explanation, human review, contestability	Limited statutory rights; judicial remedies only post-harm
Institutional Oversight	AI Office, national authorities, EU database	Proposed AI Governance Group, Safety Institute (not yet operational)
Transparency & Disclosure	Mandatory registration, plain-language explanations	Voluntary transparency reports; no ADM-specific disclosure duty
Judicial Review	Strong (ECHR, CJEU precedents)	Evolving (Puttaswamy, Aadhaar cases)
Enforcement & Penalties	Fines up to 4% global turnover	No AI-specific penalties; DPDP Act fines limited to data breaches

[22] See Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (India). The claims about specific Aadhaar-enabled benefit-transfer exclusion cases, police facial-recognition deployments in Delhi and Telangana, and predictive-policing pilots in Hyderabad and Pune need separate case-specific or official documentary sources.

Key Analytical Points

Regulatory Philosophy: The EU's layered, enforceable framework reflects a precautionary commitment to fundamental rights. India's flexible, innovation-friendly approach prioritises economic growth and technological sovereignty. This divergence mirrors broader governance traditions: the EU's post-war rights constitutionalism versus India's developmental state model.

Due Process Embedding: The EU embeds due process within administrative procedure through statutory duties (explanations, human oversight, contestability). India relies on constitutional litigation to remedy violations after they occur leaving affected individuals without ex-ante protections.

Accountability Deficit Risk: India's voluntary framework creates an "accountability deficit" where no single actor is clearly responsible for algorithmic harms, and victims lack accessible redress pathways. The EU's duty-artefact-forum matrix (identifying who is accountable, for what, and before which body) provides a replicable model.

Procurement as Leverage: The EU uses public procurement rules to enforce AI accountability, requiring vendors to comply with conformity assessments and audit obligations. India's Digital India and IndiaAI Mission could similarly integrate accountability clauses but haven't yet done so.[24]

Implementation Gaps: Both jurisdictions face capacity challenges. The EU struggles with harmonising national implementation and ensuring SME/public authority compliance. India's proposed institutions remain unoperationalised, and bureaucratic capacity for AI oversight is limited.

VI. CHALLENGES AND RECOMMENDATIONS

Cross-Cutting Challenges

Both the European Union and India face several common challenges in implementing accountable and rights-compliant AI systems in public administration. First, the opacity of black-box algorithms, particularly proprietary models, limits the explainability and auditability of AI-driven decisions. Secondly, vendor lock-in, arising from public authorities' dependence on private AI providers, complicates accountability and makes it difficult to transition to alternative systems. Thirdly, capacity gaps within public bureaucracies, including a lack of technical expertise, hinder the effective oversight of AI deployments. Finally, the tension between administrative efficiency and the protection of individual rights creates a risk that the pressure to automate public services may overshadow due process requirements and procedural safeguards[25].

Recommendations for the EU

The European Union should strengthen Fundamental Rights Impact Assessments (FRIAs) by extending ex-ante assessment requirements to all high-risk AI systems deployed in the public sector and incorporating public consultation requirements as a proposed reform.[24] It should also enhance

[23] Artificial Intelligence Act, supra note 1, arts. 25–27 and 49, together with applicable EU and national public procurement law. The proposition that the EU 'uses public procurement rules' to enforce AI accountability needs a more specific procurement-law authority if retained as a statement of existing law.

[25] Retain the existing footnote, as it correctly clarifies that Article 27 of the EU AI Act does not itself impose a general public-consultation requirement.

the usability of the EU AI database to facilitate civil society monitoring and improve coordination in cross-border enforcement. Furthermore, technical assistance and compliance toolkits should be provided to small and medium-sized enterprises (SMEs) and public authorities to reduce implementation burdens and support effective compliance with the applicable regulatory framework.

Recommendations for India

India should enact legislation specifically governing automated decision-making (ADM), establishing a statutory framework that mandates algorithmic impact assessments, independent audit obligations, and meaningful human review mechanisms for high-stakes automated decisions. The Government should also expedite the operationalisation of the proposed AI Governance Group and AI Safety Institute, while strengthening the institutional capacity of the Data Protection Board to address complaints concerning algorithmic fairness, subject to an appropriate statutory mandate. Furthermore, the Digital India initiative should incorporate accountability clauses into government AI procurement contracts and require public authorities to publish transparency reports on their deployment of AI systems. Finally, judicial and regulatory capacity-building should be prioritised through specialised training on AI technologies, algorithmic decision-making, and associated legal risks to improve the quality of litigation and adjudication concerning algorithmic rights.

Global Lessons

A hybrid model combining binding core safeguards (e.g., rights to explanation, human oversight) with sectoral flexibility offers a promising middle path. South-South cooperation on AI governance capacity-building could help India and other emerging economies leapfrog implementation challenges.

VII. CONCLUSION

This comparative analysis reveals a stark divergence in accountability and due process safeguards between the EU and India. The EU's binding, risk-based framework embeds robust procedural protections within its administrative law tradition, enforceable through substantial penalties and judicial review. India, despite constitutional protections and principled guidelines, lacks statutory ADM-specific safeguards, creating an accountability deficit that risks undermining trust in AI-mediated governance.

The urgency of reform cannot be overstated. As AI systems scale in welfare delivery, policing, and border control, the absence of enforceable due process guarantees threatens to erode the rule of law and exacerbate inequalities. India must transition from voluntary principles to binding rules, drawing lessons from the EU's duty-artefact-forum matrix while adapting to its own institutional context. The EU, meanwhile, must ensure implementation fidelity and address capacity gaps to realise its rights-based vision.

Future research should empirically examine AI deployment outcomes in both jurisdictions, particularly in the Global South, to refine governance models and ensure that algorithmic administration serves democratic ends.