Artificial Intelligence and The Indian Constitution: Doctrinal, Structural, And Normative Challenges

Ms. Kiran Bala
Assistant professor, Rayat college of law, Railmajra

I. INTRODUCTION

Artificial intelligence (AI) has become central to India's governance infrastructure, from biometric authentication and welfare targeting to predictive policing and digital surveillance. India's public administration increasingly depends on algorithmic tools embedded within Aadhaar, the Digital Public Infrastructure (DPI) ecosystem, and emerging state-level predictive governance experiments. These systems alter the constitutional terrain because the Indian governance model assumes human accountability, reason-giving, and reviewability assumptions that do not neatly fit opaque algorithmic systems that learn from data rather than apply explicit legal reasoning.[1] AI-driven decisions are often inscrutable and non-explainable, raising significant tensions with Articles 14, 19, and 21, which collectively form the backbone of Indian constitutional rights jurisprudence.[2]

While the Constitution is technologically neutral, its doctrines were built around human decision makers capable of articulating reasons rooted in statutory interpretation and constitutional limits. AI challenges this structure by producing outputs based on correlations rather than legal norms, thereby complicating judicial review, administrative accountability, and democratic control. Global governance models including the EU AI Act, OECD AI Recommendation, and UNESCO AI Ethics Framework recognize these risks and place particular emphasis on transparency, proportionality, and human oversight.[3] India must develop its own constitutional framework that internalizes these principles while being sensitive to local conditions such as welfare governance, digital exclusion, and caste-based inequities.

II. RULE OF LAW, ADMINISTRATIVE REASONING, AND ALGORITHMIC LEGALITY

The rule of law requires state action to be non-arbitrary, predictable, and grounded in valid legal authority.[4] India's administrative law tradition from Maneka Gandhi to Ajay Hasia demands rational, reasoned decision-making.[5] AI systems complicate these obligations because machine-learning models often operate as "black boxes," making it difficult to trace decisions to statutory commands or policy objectives.[6] Judicial review depends on an intelligible record, but algorithmic systems frequently produce outputs without human-understandable justification. This contradiction undermines the rule of law and

[1] shoshana zuboff, the age of surveillance capitalism 85–112 (2019).
[2] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248.
[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence; OECD, Recommendation of the Council on Artificial Intelligence (2019); UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
[4] A.D.M. Jabalpur v. Shivkant Shukla, (1976) 2 S.C.C. 521.
[5] Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 S.C.C. 722.
[6] Jenna Burrell, How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms, 3 BIG DATA & SOC'Y 1 (2016).

procedural fairness as articulated by the Supreme Court.[7]

Moreover, allowing AI models to evolve through continuous learning raises concerns under the non-delegation doctrine. In re Delhi Laws Act prohibits the delegation of essential legislative functions, yet data-driven systems effectively generate substantive rules through pattern identification.[8] Without statutory limits, algorithmic delegation risks unconstitutional transfer of law-making power to automated systems. Comparative jurisdictions have flagged similar concerns; the EU AI Act explicitly restricts the deployment of self-learning AI in public decision-making without human oversight to prevent "normative drift."[9]

Algorithmic opacity also undermines reason-giving, which the Supreme Court has held is a natural component of administrative justice.[10] If an algorithm denies a welfare benefit or selects a taxpayer for audit, the absence of explainability directly violates the duty to provide reasons. The NITI Aayog Responsible AI for All report acknowledges this challenge and stresses the need for explainability in public-sector algorithms.[11]

III. EQUALITY, CLASSIFICATION, AND ALGORITHMIC BIAS UNDER ARTICLE 14

Article 14 prohibits arbitrary classification and discriminatory outcomes. Through E.P. Royappa, Maneka Gandhi, and Navtej Singh Johar, the Supreme Court has recognized both direct and indirect discrimination, including systemic disadvantages.[12] Algorithmic systems are especially susceptible to reproducing entrenched patterns of caste, class, gender, and religious inequality embedded in training datasets.[13]

For example, predictive policing systems trained on historical arrest data can disproportionately target Dalit or Muslim localities because past policing practices were themselves discriminatory.[14]International literature reinforces this concern; studies by the AI Now Institute and ProPublica show that predictive systems often amplify historical bias.[15] These findings align with Indian concerns about structural discrimination recognized in State of Kerala v. N.M. Thomas and later in Navtej.[16]

Global frameworks also emphasize anti-discrimination safeguards. The OECD AI Recommendation requires states to prevent algorithmic bias through audits and fairness assessments.[17] The UN Special Rapporteur on Racism has similarly warned that automated systems may constitute a form of "digital discrimination."[18] Such comparative insights reinforce the need for heightened scrutiny under Indian equality doctrine when the State uses AI.

IV. PRIVACY, SURVEILLANCE, AND DIGITAL CONSTITUTIONALISM

The landmark Justice K.S. Puttaswamy (Privacy) decision recognized privacy as a fundamental right grounded in dignity and autonomy.[19] AI intensifies

[7] Mohinder Singh Gill v. Chief Election Comm'r, (1978) 1 S.C.C. 405.In re Delhi Laws Act, A.I.R. 1951 S.C. 332.
[8] In re Delhi Laws Act, A.I.R. 1951 S.C. 332.
[9] EU Artificial Intelligence Act arts. 6–7.

[10] Kranti Assocs. Pvt. Ltd. v. Masood Ahmed Khan, (2010) 9 S.C.C. 496.
[11]NITI Aayog, Responsible AI for All: A Strategy for India (2021).
[12] Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1.
[13] Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 CALIF. L. REV. 671 (2016).
[14]amnesty int'l, automated apartheid (2021).

[15] Julia Angwin et al., Machine Bias, propublica (May 23, 2016).
[16] State of Kerala v. N.M. Thomas, (1976) 2 S.C.C. 310.
[17] OECD, Recommendation of the Council on Artificial Intelligence (2019).
[18] U.N. Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination in Emerging Digital Technologies (2020).
[19] Justice K.S. Puttaswamy (Privacy) v. Union of India, (2017) 10 S.C.C. 1.

privacy concerns because it depends on large datasets including biometric, behavioural, transactional, and geolocation data. India's growing use of facial recognition systems (FRS) by police forces in Delhi, Hyderabad, and other cities often lacks statutory basis.[20] Real-time FRS can track individuals across public spaces, creating pervasive surveillance that fails the Puttaswamy proportionality test.[21]

The Digital Personal Data Protection Act, 2023 (DPDP Act) provides a regulatory structure but contains wide government exemptions for national security and public order, raising concerns about disproportionate data processing.[22] Comparative systems offer stricter protections: the EU General Data Protection Regulation (GDPR) prohibits processing of biometric data without explicit safeguards, and the EU AI Act classifies real-time facial recognition as a "high-risk" system subject to intense scrutiny.[23]

Indian constitutional jurisprudence reinforces these comparative principles. In Anuradha Bhasin, the Supreme Court emphasized that digital restrictions must be necessary, proportionate, and time-bound.[24] The same logic applies to algorithmic surveillance: mass, indefinite, and opaque monitoring must be treated as constitutionally impermissible. International authorities echo this: the UN Office of the High Commissioner for Human Rights (OHCHR) has warned that AI-enabled surveillance may violate international human rights law.[25] UNESCO's 2021 Recommendation on the Ethics of AI similarly stresses that surveillance AI should be subject to strict proportionality and legislative oversight.[26]

V. PROCEDURAL DUE PROCESS AND ALGORITHMIC OPACITY

Article 21, interpreted through the "fair, just, and reasonable" standard of Maneka Gandhi, requires procedures consistent with due process.[27] When AI-based systems deny benefits, flag individuals for enforcement, or generate risk scores, affected persons often receive no explanation. Machine-generated codes or automated messages do not meet the due-process obligation of intelligible notice.

This violates principles from Kranti Associates, which treats reason-giving as integral to natural justice,[28]and Ridge v. Baldwin, which influences Indian due-process doctrine by requiring fair hearing before adverse decisions.[29] Algorithmic opacity also undermines the right to appeal, because individuals cannot meaningfully challenge a decision when its logic is inaccessible.

Comparative scholarship illustrates this problem. Danielle Citron and Frank Pasquale argue that automated decision-making creates "technological due process deficits," requiring transparency mandates.[30] The UK House of Lords' 2020 report on AI echoes similar concerns, warning that opaque algorithms risk creating an unaccountable "digital state."[31] These insights support an Indian constitutional requirement that AI-driven decisions include explainability, disclosure of error rates, and human-in-the-loop review.

VI. SEPARATION OF POWERS, DELEGATION, AND DEMOCRATIC ACCOUNTABILITY

AI deployment raises separation-of-powers concerns because algorithmic systems often perform functions traditionally exercised by humans within the legislative or judicial domains. When predictive models influence welfare eligibility or policing

[20] internet freedom found., face recognition in India: state of play (2023).
[21] Puttaswamy (privacy), supra note 19.
[22] Digital Personal Data Protection Act, No. 22 of 2023, India code.
[23] Council Regulation 2016/679, General Data Protection Regulation, art. 9; EU AI Act annex III.
[24] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637.
[25] OHCHR, The Right to Privacy in the Digital Age (2021).
[26]UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
[27] Maneka Gandhi, supra note 2.
[28] Kranti Assocs., supra note 10.
[29] Ridge v. Baldwin, [1964] A.C. 40 (H.L.).
[30] Danielle Keats Citron, Technological Due Process, 85 WASH. U. L. REV. 1249 (2008).
[31] UK House of Lords Select Comm. on Artificial Intelligence, AI in the UK: Ready, Willing and Able? (2018).

intensity, they effectively shape policy outcomes without parliamentary oversight. This risks violating the non-delegation principle and the democratic accountability framework inherent in Articles 73, 162, and 246.

In judicial contexts, algorithmic tools used for bail or sentencing recommendations risk undermining judicial independence. Although such practices are more common in the United States, comparative scholarship such as critiques of the COMPAS system illustrates how automated risk assessment can entrench racial bias and distort judicial reasoning.[32] Indian judges may similarly feel pressure to align their decisions with algorithmic outputs, compromising individualized justice.

Global institutions have flagged this risk. The Council of Europe's European Ethical Charter on the Use of AI in Judicial Systems rejects the replacement of judicial discretion with automated tools.[33] India's own Vidhi Centre for Legal Policy warns that judicial AI tools could undermine constitutional guarantees unless tightly regulated.[34]

Democratic accountability is further weakened when AI systems are developed by private vendors through opaque procurement contracts. Without transparency obligations, it becomes impossible for legislatures or citizens to verify whether the algorithmic logic complies with constitutional norms. This concern has been emphasized by the Indian Parliamentary Standing Committee on IT, which has called for stronger accountability mechanisms for algorithmic governance.[35]

VII. TOWARD AN INDIAN THEORY OF ALGORITHMIC CONSTITUTIONALISM

India requires an AI governance model grounded in constitutional rights and democratic accountability. Such a model should include:

1. Legality: AI systems must have explicit statutory authorization defining scope, purpose, safeguards, and oversight.[36]
2. Transparency and Explainability: Public authorities should disclose model architecture, accuracy metrics, training data characteristics, and error rates.
3. Proportionality: High-risk AI systems—especially in policing, welfare, and surveillance—must satisfy a strict necessity and minimal-intrusion test consistent with Puttaswamy and Anuradha Bhasin.
4. Anti-discrimination safeguards: Routine algorithmic bias audits, fairness assessments, and caste/gender impact evaluations must be mandatory.
5. Human accountability: AI may assist but cannot replace human decision-makers within the constitutional chain of responsibility.
6. Independent oversight: A national AI regulatory authority, similar to the EU's AI Office, should monitor deployment, audit compliance, and impose penalties.
7. Public participation: Inspired by UNESCO and OECD standards, AI policies should emerge through consultative democratic processes.

This framework constitutes an Indian theory of algorithmic constitutionalism—one that integrates global insights while grounding itself in India's unique constitutional commitments to dignity, equality, and social justice.

VIII. CONCLUSION

India stands at a constitutional crossroads. The rapid integration of AI into governance offers efficiency

[32] Julia Angwin et al., Machine Bias, PROPUBLICA (May 23, 2016).
[33] Council of Eur., European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems (2018).
[34] vidhi ctr. for legal pol'y, algorithmic decision-making and the law (2021).
[35] Parliamentary Standing Comm. on Info. Tech., Citizen Data Security and Privacy (2021).
[36] EU AI Act art. 29; OECD, supra note 17.

gains but risks undermining foundational constitutional norms. Articles 14, 19, and 21 require heightened scrutiny of algorithmic systems that may encode bias, enable pervasive surveillance, undermine due process, or erode human accountability. By drawing on comparative global standards while strengthening domestic constitutional doctrine, India can create an AI governance framework that is democratic, rights-protective, and faithful to the constitutional vision of liberty, equality, and dignity.