



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

ARTIFICIAL INTELLIGENCE AND CONSTITUTIONAL RIGHTS IN INDIA: REGULATING ALGORITHMIC DECISION-MAKING, BIAS AND ACCOUNTABILITY

~ SATHVIKA.J

ABSTRACT

Artificial Intelligence (AI) is increasingly being integrated into policing, welfare administration, employment, credit, education, healthcare, judicial and legal systems, and public administration. Algorithmic systems may improve efficiency, consistency and the processing of large quantities of information, but they may also reproduce or amplify discriminatory patterns embedded in historical data and institutional practices. Where governmental decisions affecting individuals are informed or generated by algorithms, constitutional concerns arise regarding equality, non-discrimination, privacy, dignity, autonomy, freedom, procedural fairness and access to remedies. India does not presently possess a single comprehensive AI-specific constitutional accountability framework. Nevertheless, Articles 14, 19 and 21 of the Constitution, together with administrative-law principles and the emerging data-protection and responsible-AI framework, provide a substantial foundation for regulating rights-affecting AI. This paper argues for a rights-based, risk-sensitive Indian framework incorporating algorithmic impact assessment, transparency, meaningful explanation, human oversight, independent auditing, institutional accountability and effective remedies.

1. INTRODUCTION

1.1 Background

Decision-making by public authorities has traditionally been associated with identifiable human decision-makers who collect information, apply legal standards, consider relevant circumstances and provide a decision capable of being reviewed. Digitalisation has progressively altered this model. Contemporary administrative systems increasingly use computational tools to classify individuals, predict risks, prioritise cases and recommend or determine outcomes. The transformation may be represented as a continuum: human decision-making, algorithm-assisted decision-making and automated decision-making. The constitutional significance of the distinction lies not merely in the technology used, but in how technological systems redistribute discretion and affect the ability of individuals to understand and challenge decisions.

Examples include facial-recognition systems, predictive policing, automated welfare eligibility, recruitment algorithms, credit scoring, insurance risk assessment, AI-based surveillance, automated content moderation and government databases that facilitate profiling. Similar technologies are used by private actors in employment, finance, education and healthcare. Their increasing deployment creates a new form of governance in which decisions can be generated from large datasets and statistical models rather than from an individually articulated chain of human reasoning.

1.2 The Constitutional Problem

The central constitutional issue is therefore not simply whether AI is technologically reliable. It is whether a State decision affecting an individual's rights or legally significant interests can be constitutionally legitimate when the individual cannot understand, challenge or obtain meaningful human review of the algorithmic process behind it. An algorithm may produce an apparently objective output while relying on historical data, proxy variables or assumptions that reproduce existing inequalities. Conversely, a technically sophisticated system may create accountability problems because responsibility is distributed between a government department, software vendor, data provider, developer and individual officer.

1.3 Problem Statement

Three interconnected problems emerge. First, algorithmic bias may produce direct or indirect discrimination. Secondly, opacity or black-box decision-making may prevent affected persons from understanding the basis of adverse outcomes. Thirdly, an accountability gap may arise when no actor accepts responsibility because the decision is attributed to the algorithm itself.

These problems become more serious when AI systems operate at scale and affect vulnerable populations.

1.4 Research Question

The central research question is: Can a State decision affecting an individual's rights be constitutionally legitimate when the individual cannot understand, challenge or obtain meaningful human review of the algorithmic process behind it?

1.5 Objectives

The paper seeks to examine the constitutional rights implicated by AI; analyse algorithmic discrimination under Article 14; examine privacy and autonomy under Article 21; assess procedural fairness and natural justice; evaluate India's existing legislative, regulatory and policy framework; identify accountability gaps; and propose constitutional safeguards for high-impact governmental AI.

1.6 Methodology

The research adopts a doctrinal and comparative legal methodology. It analyses constitutional provisions, legislation, judicial decisions, regulatory materials, policy documents and selected international regulatory frameworks. Comparative materials are used not to prescribe wholesale transplantation, but to identify regulatory principles capable of adaptation to India's constitutional structure.

2. UNDERSTANDING AI DECISION-MAKING AND ALGORITHMIC GOVERNANCE

2.1 What is Algorithmic Decision-Making?

An algorithm is a defined sequence of computational instructions used to process inputs and produce an output. Artificial Intelligence is a broader technological field involving systems capable of performing tasks associated with human cognitive functions, while machine learning enables systems to identify patterns from data and generate predictions or classifications. Automated decision-making refers to decisions made wholly or substantially through automated processing, while predictive analytics uses historical and current data to estimate future outcomes.

A crucial distinction is between AI-assisted and AI-generated decision-making. In AI-assisted decision-making, the system supplies information, recommendations or classifications

while a human remains responsible for the final decision. In AI-generated or fully automated decision-making, the system may determine the outcome with little or no meaningful human intervention. This distinction is central to responsibility because the presence of a human interface does not necessarily establish meaningful human judgment.

2.2 How Algorithmic Decisions Work

A simplified model is: Data → Training → Algorithm/Model → Prediction or Classification → Decision → Consequence. Bias may enter at every stage. Data collection may underrepresent certain populations; historical datasets may contain institutional discrimination; measurement choices may capture outcomes inaccurately; model designers may select variables that act as proxies for protected characteristics; deployment may occur in circumstances different from those in which a model was developed; and decision-makers may misunderstand or over-trust outputs.

2.3 Algorithmic Bias

Algorithmic bias can take several forms, including historical bias, sampling bias, measurement bias, proxy discrimination, automation bias and feedback loops. A system need not explicitly use caste, religion, sex or another protected characteristic to produce discriminatory effects. A variable such as location, occupation, educational institution or purchasing behaviour may correlate with a protected characteristic and reproduce existing structural inequalities. A feedback loop can further entrench the problem when earlier algorithmic predictions influence future data, causing the system to learn from its own historically biased outputs.

2.4 Algorithmic Governance

Algorithms increasingly govern both State and private activity. State AI directly engages constitutional law because governmental action is constrained by fundamental rights and judicial review. Private AI raises a different question: how far constitutional values can influence private technological actors through horizontal application of fundamental rights, statutory regulation and the State's positive obligations to prevent rights violations. The distinction should therefore run throughout the analysis.

3. CONSTITUTIONAL FRAMEWORK IN INDIA

3.1 Article 14 — Equality and Non-Arbitrariness

Article 14 guarantees equality before the law and equal protection of the laws. Indian equality doctrine has developed beyond formal classification to include scrutiny of arbitrary State action. In *E P Royappa v State of Tamil Nadu*, the Supreme Court connected equality with non-arbitrariness, while *Maneka Gandhi v Union of India* strengthened the requirement that State action affecting liberty must satisfy standards of fairness. *Ajay Hasia v Khalid Mujib Sehravardi* reinforced Article 14 review of State action, and *Shayara Bano v Union of India* recognised manifest arbitrariness as a constitutional ground in the appropriate context.

Applied to AI, these principles raise a significant question: can an algorithmic decision be challenged as arbitrary where the decision-maker cannot explain why a particular individual received a particular outcome? Algorithmic opacity does not automatically establish arbitrariness, but it can make it difficult to demonstrate that relevant considerations were used, irrelevant considerations excluded and like cases treated alike.

3.2 Article 15 — Discrimination

Article 15 prohibits discrimination by the State on specified grounds including religion, race, caste, sex and place of birth. Algorithmic systems create a difficult problem of indirect discrimination because apparently neutral criteria may produce disproportionate disadvantages for protected groups. *Lt Col Nitisha v Union of India* is significant for its treatment of substantive equality and indirect discrimination. Its reasoning provides a doctrinal basis for asking whether neutral algorithmic criteria reproduce structural disadvantage even where protected characteristics are not explicitly entered into the model.

3.3 Article 19

AI may affect Article 19(1)(a) through automated content moderation, recommendation systems, algorithmic censorship and surveillance that produces chilling effects on expression. Article 19(1)(g) may be implicated where automated recruitment, occupational classification or platform-based systems affect access to employment or professional activity. Restrictions must remain within constitutionally permissible limits, and the use of technology does not remove the need to justify governmental interference with protected freedoms.

3.4 Article 21

Article 21 provides the strongest foundation for analysing privacy, dignity, autonomy and fair procedure. Maneka Gandhi requires procedure affecting personal liberty to satisfy constitutional standards of fairness. Justice K S Puttaswamy (Retd) v Union of India recognised privacy as a fundamental right, including interests in informational privacy and decisional autonomy. Puttaswamy (Aadhaar) demonstrates the importance of proportionality when State systems collect and process personal information. The legality of an intrusive AI system may therefore be assessed through legality, legitimate aim and proportionality, together with appropriate safeguards.

3.5 Articles 32 and 226

Articles 32 and 226 provide constitutional remedies. Algorithmic opacity, however, can make remedies ineffective if the affected person cannot identify the basis of the decision or obtain sufficient information to challenge it. This creates a direct connection between constitutional remedies and explainability: meaningful judicial review requires sufficient information to assess legality, relevance, fairness and proportionality.

4. ALGORITHMIC BIAS AND CONSTITUTIONAL EQUALITY

4.1 Why Algorithmic Bias is Constitutionally Significant

Algorithmic neutrality is not necessarily constitutional neutrality. A mathematical model may apply the same formula to every person while still producing discriminatory outcomes because the underlying data reflects historical inequality. The constitutional inquiry must therefore focus not only on formal neutrality but also on whether the decision-making process and its effects are compatible with substantive equality.

4.2 Direct Discrimination

Direct discrimination presents the clearest case. If an AI recruitment system expressly uses sex as a factor in selecting candidates, the use of the protected characteristic immediately raises Article 14 and Article 15 concerns. Similar issues arise where a governmental system explicitly uses caste, religion or another protected characteristic in determining access to public benefits or services without a constitutionally sufficient justification.

4.3 Indirect Discrimination

The more difficult case occurs where a neutral criterion disproportionately disadvantages a protected group. Lt Col Nitisha is particularly relevant because constitutional equality may require attention to structural effects rather than only the formal wording of a rule. In algorithmic systems, variables that appear neutral may operate as proxies for caste, sex, socioeconomic status or other protected characteristics. The constitutional question should therefore include whether the criterion reproduces an unjustified discriminatory disadvantage.

4.4 Historical Data and Structural Inequality

AI systems frequently learn from historical data. If historical decision-making was discriminatory, the dataset may encode those patterns; the model may then learn them and reproduce them; subsequent decisions generate new data that reinforces the pattern. The resulting sequence can be expressed as: historical discrimination → biased dataset → algorithmic prediction → reproduced discrimination → new data → reinforced prediction. Algorithmic governance must therefore examine not only the model but also the social conditions from which its training data emerged.

4.5 AI in Policing

Predictive policing, facial recognition and crime-risk prediction create particular constitutional concerns. Errors can affect individuals who have committed no offence, while profiling may concentrate surveillance on communities already subject to heightened policing. Article 14 concerns arise from unequal treatment; Article 21 concerns arise from privacy, dignity and personal liberty; and procedural concerns arise when individuals cannot effectively challenge a risk classification. Presumption of innocence and safeguards against arbitrary surveillance are therefore relevant to the design and use of high-impact policing systems.

4.6 AI in Welfare and Public Administration

Automated beneficiary identification, fraud detection, welfare eligibility systems and biometric authentication may improve administrative efficiency but can also generate wrongful exclusion. Data errors, authentication failures and model misclassification may deprive individuals of essential benefits. Because welfare decisions may directly affect dignity and basic conditions of life, procedural safeguards must ensure notice, reasons, correction mechanisms and meaningful human review.

5. AI, PRIVACY, AUTONOMY AND PROCEDURAL FAIRNESS

5.1 Privacy

Puttaswamy provides the constitutional foundation for assessing data collection, profiling, biometric processing, behavioural prediction and surveillance. AI increases the scale and inferential power of data processing: information collected for one purpose may be combined with other datasets to infer characteristics not expressly supplied by an individual. The constitutional concern therefore extends beyond collection to the use, combination and inference of personal information.

5.2 Informational Self-Determination

Individuals have a significant interest in knowing what information is collected, why it is collected, how it is processed, who can access it and how it affects consequential decisions. Transparency is particularly important where data is used to create profiles or predictions. Data protection and constitutional privacy therefore intersect, although privacy compliance alone cannot guarantee non-discrimination or procedural fairness.

5.3 Autonomy

AI classifications can influence employment, credit, education, healthcare and access to public benefits. Automated classification may narrow meaningful opportunities where individuals are treated according to inferred probabilities rather than their individual circumstances. Autonomy requires that consequential decisions remain capable of being understood and contested, especially where the system's output significantly affects a person's choices or legal position.

5.4 Natural Justice

The principle of audi alteram partem requires that a person affected by a decision receive a meaningful opportunity to be heard. Algorithmic decision-making raises the question whether a person can meaningfully participate if the decisive reasoning is hidden inside a model. Likewise, reasoned decision-making requires more than a statement that an algorithm has determined an outcome. A public authority should be able to articulate the legal and factual basis of the decision in a manner that permits meaningful challenge.

5.5 Right to Explanation

Indian constitutional and administrative principles can support a requirement for decision-level explanation. The explanation need not necessarily require disclosure of source code. Depending on the circumstances, it may require disclosure of the fact that AI was used, the material factors considered, relevant data, the basis of the outcome, significant limitations and the route for human review. The constitutional purpose is intelligibility and contestability rather than technological disclosure for its own sake.

6. ACCOUNTABILITY, TRANSPARENCY AND EXPLAINABILITY

6.1 The Accountability Gap

Responsibility for an AI decision may be distributed among a developer, technology vendor, data provider, government department, human officer and the AI system itself. This fragmentation can create an accountability gap. The affected person, however, experiences a single decision and a single consequence. A rights-based framework must therefore identify a legally responsible institution even where technological responsibility is distributed.

6.2 Transparency

Transparency can be understood at three levels. Technical transparency concerns how the model operates. Procedural transparency concerns how the particular decision was reached. Institutional transparency concerns who is responsible for deployment, monitoring and review. For constitutional accountability, procedural and institutional transparency may sometimes be more important than complete technical transparency.

6.3 Explainability

Model interpretability, individual decision explanation and disclosure of relevant factors are distinct. A highly complex model may not be fully interpretable in technical terms, but a person may still receive an intelligible explanation of why a consequential decision was made. Full disclosure of source code should not automatically be treated as the constitutional standard. The relevant question is whether sufficient information is available to evaluate legality, discrimination, error and fairness.

6.4 Human Oversight

High-impact governmental decisions should generally retain meaningful human oversight. However, a human-in-the-loop model is inadequate if the official simply rubber-stamps the

algorithmic output. Meaningful oversight requires authority to question the result, examine relevant evidence, depart from the model where justified and provide reasons for the final decision.

6.5 Liability

Potential responsibility may arise through constitutional remedies, administrative law, data-protection law, sectoral regulation, civil liability and contractual mechanisms. The allocation of contractual risk between a government department and a vendor cannot extinguish constitutional obligations owed to individuals. A public authority that deploys an AI system remains responsible for ensuring that the exercise of public power complies with constitutional standards.

7. EXISTING INDIAN LEGAL AND REGULATORY FRAMEWORK

7.1 Constitution of India

Articles 14, 15, 19, 21 and 32, together with Article 226, provide the principal constitutional framework for addressing AI-related State action. They establish standards of equality, non-discrimination, freedom, privacy, dignity, fair procedure and judicial remedies. These provisions demonstrate that India does not begin from a constitutional vacuum even though there is no single AI-specific constitutional statute.

7.2 Digital Personal Data Protection Framework

The Digital Personal Data Protection Act 2023 regulates the processing of digital personal data and establishes obligations for Data Fiduciaries and rights for Data Principals. The Digital Personal Data Protection Rules 2025 provide the detailed regulatory framework and implementation architecture. The framework is important for consent, notice, processing obligations, data security, individual rights and institutional enforcement.

Nevertheless, privacy compliance is not equivalent to algorithmic fairness. Data may be lawfully processed and still be used in a model that produces discriminatory outcomes. Data protection primarily regulates the processing of personal data; constitutional algorithmic governance must additionally examine the legality, fairness and effects of consequential decisions. This distinction is central to the argument for AI-specific accountability safeguards.

7.3 Information Technology Framework

The Information Technology Act 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 form important parts of India's digital regulatory architecture. They address areas including intermediary obligations, online information and platform accountability. However, they were not designed as a comprehensive framework for high-risk algorithmic decision-making across governmental and private sectors. They therefore provide relevant components but do not resolve all questions of algorithmic discrimination, explainability, impact assessment and human oversight.

7.4 Government AI Policy

NITI Aayog's National Strategy for Artificial Intelligence and its Responsible AI documents demonstrate an emerging Indian policy emphasis on responsible and ethical AI. The Responsible AI framework addresses principles such as safety, reliability, inclusivity, non-discrimination, privacy, transparency and accountability. The IndiaAI Mission, including its Safe and Trusted AI pillar, further demonstrates the government's effort to combine AI innovation and infrastructure with responsible deployment.

7.5 Regulatory Gap

India therefore has a fragmented framework composed of constitutional principles, data-protection law, information-technology regulation, sectoral rules and AI policy initiatives. The principal gap is not the total absence of legal controls, but the absence of a single comprehensive regime specifically governing high-risk algorithmic decision-making, algorithmic discrimination, mandatory impact assessment, explainability, human oversight and institutional constitutional accountability.

8. JUDICIAL ROLE AND EMERGING CONSTITUTIONAL QUESTIONS

Indian courts already possess doctrinal tools capable of addressing many AI-related disputes even though AI-specific constitutional jurisprudence remains developing. Article 14 provides a basis for reviewing arbitrary and discriminatory State action; Article 21 provides a framework for privacy, dignity and autonomy; proportionality can be used to assess intrusive State technologies; natural justice and reasoned decision-making can address procedural deficiencies; and Articles 32 and 226 provide constitutional remedies.

Several questions are likely to arise. Can an algorithmic governmental decision be challenged under Article 14? Does opacity become constitutionally significant where it prevents

effective review? Can automated profiling violate Article 21? Can an individual demand reasons explaining the material factors that produced an adverse decision? Can apparently neutral algorithmic criteria amount to indirect discrimination? What degree of human review is necessary? Who should bear the evidentiary burden where the relevant data and model are controlled by the government or vendor? Can courts order disclosure of algorithmic criteria, and how should that be balanced against trade secrets and cybersecurity concerns?

These questions should be approached through existing doctrine rather than by assuming that every AI dispute requires an entirely new constitutional test. *E P Royappa* and *Shayara Bano* support non-arbitrariness analysis; *Puttaswamy* and *Modern Dental College* support privacy and proportionality analysis; *Maneka Gandhi* supports fair procedure; *Kranti Associates* and *Mohinder Singh Gill* support reasoned decision-making; *Nitisha* provides an important foundation for indirect discrimination; and Articles 32 and 226 enable judicial review and remedies. The challenge is therefore one of doctrinal adaptation: translating established constitutional standards into an environment where decision-making is computational, probabilistic and potentially opaque.

9. COMPARATIVE PERSPECTIVE

9.1 European Union

The European Union's Artificial Intelligence Act provides a prominent risk-based regulatory model. It distinguishes prohibited practices and high-risk AI systems and imposes enhanced obligations concerning risk management, data governance, documentation, transparency, accuracy, robustness and human oversight. The significance for India is not that the EU model should simply be copied, but that differentiated regulatory intensity can be matched to the potential impact of an AI system.

9.2 United States

The United States provides a contrasting model characterised by constitutional constraints on government and a substantial body of sector-specific anti-discrimination and regulatory law. Title VII addresses employment discrimination, the Equal Credit Opportunity Act addresses credit discrimination, and constitutional due process and equal-protection principles constrain governmental action. The NIST AI Risk Management Framework provides a voluntary risk-

management framework rather than a single comprehensive federal AI statute comparable to the EU AI Act.

9.3 Comparative Question

The relevant comparative question is therefore which regulatory principles can be constitutionally adapted to India. The EU demonstrates the utility of risk-sensitive classification and mandatory safeguards for high-impact systems; the US demonstrates how existing rights and sectoral regulation can address particular forms of algorithmic harm. India can draw from both approaches while grounding its framework in Articles 14, 19 and 21, administrative law and constitutional remedies.

10. PROPOSED RIGHTS-BASED AI REGULATORY FRAMEWORK FOR INDIA

This paper proposes an Indian Constitutional Algorithmic Accountability Framework for high-impact governmental AI. The framework is not presented as existing Indian law; it is a normative synthesis designed to operationalise constitutional principles in an algorithmic environment.

10.1 Algorithmic Impact Assessment

Before deployment of high-risk AI, a public authority should conduct an Algorithmic Impact Assessment addressing equality, discrimination, privacy, accuracy, security, affected populations, foreseeable harms, human oversight and remedies. The assessment should occur before deployment and be periodically reviewed after implementation.

10.2 Risk Classification

AI systems should be classified as Low Risk, Moderate Risk, High Risk and Prohibited or Unacceptable Risk. Regulatory intensity should increase with potential impact on fundamental rights. Systems affecting welfare, policing, employment, credit, education, healthcare or access to public services should ordinarily receive enhanced scrutiny where their outputs have consequential effects.

10.3 Mandatory Human Oversight

High-impact decisions should not be entirely automated. A human official should have genuine authority to review evidence, question the system, depart from its recommendation and provide reasons. Human oversight must not become a formal rubber-stamping exercise.

10.4 Right to Notice

Individuals should be informed when AI materially contributes to a decision affecting their rights or legally significant interests. Notice should identify the responsible authority, the general purpose of the system and the availability of review or challenge.

10.5 Right to Explanation

Individuals should receive understandable reasons for consequential decisions. The explanation should identify relevant factors and the basis of the outcome without necessarily requiring unrestricted disclosure of source code or sensitive technical architecture. The objective is meaningful contestability.

10.6 Right to Contest

Individuals should be able to challenge the decision, correct inaccurate data, request human review and obtain an effective remedy. These mechanisms should be accessible and should not impose an unrealistic technical burden on individuals who lack access to the underlying system or data.

10.7 Algorithmic Audit

Independent audits should examine accuracy, discriminatory effects, data quality, security, robustness and compliance. Auditing should occur both before deployment and periodically thereafter, especially where the system is adaptive or where its outputs influence future training data.

10.8 Government Algorithm Registry

Public authorities should maintain a registry identifying the purpose of each high-impact AI system, responsible authority, risk classification, categories of data used, audit status and oversight mechanism. Sensitive technical or security information may be protected where justified, but the existence and institutional responsibility for a system should not ordinarily be concealed.

10.9 Allocation of Responsibility

The framework should reject the proposition that 'the algorithm made the decision' automatically removes institutional responsibility. The public authority deploying the system should remain accountable for constitutional compliance. Contracts with developers and vendors

may allocate commercial responsibility, but they should not transfer away the State's constitutional obligations.

10.10 Algorithmic Constitutional Compliance Test

The paper proposes an Algorithmic Constitutional Compliance Test for high-impact State AI: Legality → Legitimate Aim → Necessity → Proportionality → Non-discrimination → Explainability → Human Oversight → Effective Remedy. A system should not be deployed, or should be modified or withdrawn, where it cannot satisfy the applicable constitutional requirements. This test combines existing Indian doctrines of legality, proportionality, equality, fairness and reasoned decision-making with AI-specific safeguards.

The proposal is therefore not a demand to prohibit governmental AI. It is a framework for ensuring that technological efficiency does not become a substitute for constitutional accountability.

11. CONCLUSION

AI is not constitutionally neutral merely because it is technologically sophisticated. An algorithm can reproduce historical inequalities, obscure the basis of decisions and distribute responsibility across institutions without eliminating the constitutional consequences of the resulting State action. The constitutional question is therefore not whether a decision was made by a person or a machine, but whether the exercise of public power remains consistent with fundamental rights.

Articles 14, 19 and 21 already provide substantial constitutional tools for addressing algorithmic discrimination, privacy violations, arbitrary decision-making and restrictions on liberty. Indian administrative law also supplies principles of natural justice, reasoned decision-making and judicial review. Yet traditional doctrines must be operationally adapted to algorithmic environments in which decisions can be opaque, responsibility can be distributed, discrimination can be indirect and decisions can occur at enormous scale.

India consequently requires a rights-based and risk-sensitive AI governance framework rather than regulation focused exclusively on innovation or data protection. Algorithmic impact assessment, risk classification, meaningful human oversight, notice, explanation, contestability, independent auditing, institutional transparency and effective remedies can translate constitutional

principles into operational safeguards. The objective should not be to prevent the State from using AI. It should be to ensure that technological delegation does not become a means of avoiding constitutional review or responsibility.

The central proposition of this paper is therefore simple: ****no individual should lose a constitutionally protected right merely because the decision affecting that right has been delegated to an algorithm.**** The Constitution regulates the exercise of State power irrespective of whether that power is exercised through a human official, an algorithm-assisted system or an automated technological process.

REFERENCES:

1. Constitution of India 1950, arts 14, 15, 19, 21, 32 and 226.
2. E P Royappa v State of Tamil Nadu, (1974) 4 SCC 3.
3. Maneka Gandhi v Union of India, (1978) 1 SCC 248.
4. Mohinder Singh Gill v Chief Election Commissioner, (1978) 1 SCC 405.
5. Swadeshi Cotton Mills Co Ltd v Union of India, (1981) 1 SCC 664.
6. Ajay Hasia v Khalid Mujib Sehravardi, (1981) 1 SCC 722.
7. Tata Cellular v Union of India, (1994) 6 SCC 651.
8. Kranti Associates (P) Ltd v Masood Ahmed Khan, (2010) 9 SCC 496.
9. Modern Dental College & Research Centre v State of Madhya Pradesh, (2016) 7 SCC 353.
10. Shayara Bano v Union of India, (2017) 9 SCC 1.
11. Justice K S Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1.
12. K S Puttaswamy (Aadhaar) v Union of India, (2019) 1 SCC 1.
13. Lt Col Nitisha v Union of India, (2021) 4 SCC 511.
14. Digital Personal Data Protection Act 2023, Act No 22 of 2023.
15. Digital Personal Data Protection Rules 2025, Ministry of Electronics and Information Technology.
16. Information Technology Act 2000, Act No 21 of 2000.
17. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, as amended.
18. NITI Aayog, National Strategy for Artificial Intelligence #AIforAll (2018).

19. NITI Aayog, Responsible AI for All: Approach Document for India, Part 1 — Principles for Responsible AI (2021).
20. NITI Aayog, Responsible AI for All: Approach Document for India, Part 2 — Operationalizing Principles for Responsible AI (2021).
21. NITI Aayog, Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology (2022).
22. Government of India, IndiaAI Mission (2024).
23. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689.
24. US Constitution, amends IV and XIV.
25. Civil Rights Act of 1964, Title VII, 42 USC §§ 2000e–2000e-17.
26. Equal Credit Opportunity Act, 15 USC §§ 1691–1691f.
27. Fair Housing Act, 42 USC §§ 3601–3619.
28. Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (National Institute of Standards and Technology, 2023).
29. NIST, AI Risk Management Framework Playbook (2023).
30. OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, amended 2024).
31. Solon Barocas and Andrew D Selbst, ‘Big Data's Disparate Impact’ (2016) 104 California Law Review 671.