

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ALGORITHMIC BIAS IN GOVERNANCE: CONSTITUTIONAL IMPLICATIONS OF AUTOMATED DECISION-MAKING IN INDIA

AUTHORED BY - MAYANK GUPTA & PROF. NUZHAT PARVEEN KHAN

Abstract

The growing dependence of the State on the use of algorithmic systems to make decisions, including biometric identification, predictive policing, automated welfare targeting, and electoral roll revisions raises significant constitutional issues in India. It is an undeniable truth that in most cases, algorithmic governance is more efficient and scalable but very often it is opaque and biased in its data, with little to no accountability. This article examines the implication of automated decision-making on the fundamental rights of equality (Article 14), freedoms (Article 19), and life/liberty and privacy (Article 21) provided under the Indian Constitution. It constructs a doctrinal base for the evaluation of algorithmic intrusions based on Indian constitutional principles, viz; legality, proportionality, non-arbitrariness, and procedural fairness. Applying that fundamental understanding to high significant instances of algorithmic governance in India- including Aadhaar-based welfare authentication and the algorithmic flagging system used in the Special Intensive Revision (SIR) of electoral rolls-the article demonstrates how automated systems can produce systemic exclusion and disproportionate impacts on marginalised communities. The article concludes by suggesting a constitutional test for the admissibility of the use of algorithms by the State actors: statutory authorization, mandatory algorithmic impact evaluation, substantial human control, auditability, and effective remedies for enforcement.

Keywords: Artificial Intelligence, Algorithm, Fundamental Rights, Governance, Arbitrariness

1. INTRODUCTION

In the contemporary era, governance increasingly integrates algorithmic systems into the current and consequential functions of the State. From biometric identity verification and automated welfare eligibility checks, to algorithmic risk assessments used in policing and pre-trial detention, IT systems now decisively carry out or inform state actions that affect rights,

status, opportunity, and freedom.¹ The state's delegation of public power to automated systems – what this article calls “*Algorithmic governance*” – raises pressing constitutional questions in India.

The traditional constitutional law method of assessing the action of a State is considered to be based on the doctrinal mechanisms that are modified to fit human decision-makers: the rationality, procedural fairness, non-arbitrariness, proportionality and reasoned explanations.² Algorithms are problematic for these tools since they tend to work opaquely, use statistical correlations instead of legal standards, and exhibit social biases to the extent of their training data.³ The main normative challenge is to know whether, and under what circumstances the exercise of public power through algorithmic systems is compatible with the constitutional commitments in India towards equality, freedom and dignity. This article provides an answer to this question by constructing a constitutional test of acceptable algorithmic governance and providing an example of it, applied to real-world deployments in India.

The stakes are high. This is not an unreasonable fear: the consequences of errors and biases in the algorithmic systems include unjustified suspicion, deprivation of benefits and limited access to social and political life.⁴

Constitutionalism requires not only technical solutions, but also institutional guarantees: the express legal authorization, the proportionality, the human control, the transparency, the possibility to challenge automated outcomes and the permanence of judicial control.⁵

This article proceeds in seven parts. Part II establishes the conceptual foundations of algorithmic governance, distinguishing rule-based systems from machine-learning models and identifying the constitutional puzzles raised by the delegation of state power to non-human systems. Part III constructs the constitutional framework, examining algorithmic governance

¹ Ashwin Varghese, "The Dialectics of Discretion in Algorithmic Governance and Smart Policing," 12 Big Data & Society 1 (2025), available at: <https://journals.sagepub.com/doi/10.1177/20539517251403966> (last visited on 5 June 2026).

² *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3; *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

³ Christoph Molnar, *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable* (3rd edn, Lean Publishing 2021); Elena Beretta, Cristina Voto and others, "Decoding Faces: Misalignments of Gender Identification in Automated Systems" (2024) 19 *Journal of Responsible Technology* (2024).

⁴ *Justice K.S. Puttaswamy (Retd) v. Union of India*, (2017) 10 SCC 1 (*Puttaswamy I*).

⁵ *Pragya Prasun v. Union of India*, Writ Petition(s)(Civil) No. 289/2024, judgment dated 30 April 2025 (Supreme Court of India).

through the lenses of Articles 14 (equality), 19 (freedoms), and 21 (life and liberty) of the Indian Constitution. Part IV examines the application of administrative law principles—reasoned decisions, natural justice, and procedural fairness—to algorithmic decision-making. Part V presents case studies: Aadhaar-based welfare exclusion and the SIR electoral roll revision. Part VI offers a comparative analysis of algorithmic governance frameworks in the European Union, the United Kingdom, and the United States. Part VII concludes with a proposed regulatory framework and constitutional test for algorithmic governance in India.

2. CONCEPTUAL FOUNDATIONS OF ALGORITHMIC GOVERNANCE

The term algorithmic governance describes the application of computational techniques (algorithms, machine learning models, automated decision systems) by public authority to make, support or scale administrative decisions.⁶ These systems are not homogeneous: Rule-based (deterministic) algorithms are based on explicit rules (e.g., tax brackets), statistical/machine-learning models extrapolate patterns using data to generate results or classifications (e.g., credit rating, facial recognition); hybrid system combine features of both.⁷

Algorithmic governance can be differentiated by three features, as opposed to a traditional administrative action:

- a) Scale and speed: Automated systems have the ability to process large datasets and make decisions at scale and speed that is inaccessible to human operators, which allows continuous monitoring and real-time responses.⁸
- b) Opacity: A lot many machine-learning models (in particular, deep-learning) are black-boxes: their inner mechanics cannot be easily understood even by their designers.⁹
- c) Data-dependence: The outcomes will be based on the training data; the information-biases, gaps or historical injustices in data may cause systematic errors or discriminative outcomes.¹⁰

These functions have institutional consequences: administrative work is computerised, discretion is no longer exercised by individuals, but rather by designers and data editors and

⁶ Supra note 1, at 1.

⁷ Jaiveer Singh & Yagya Agarwal, “Invisible Hand of Code: Reimagining Constitutionalism in the Age of Algorithms”, NLIU Law Review (Jan. 27, 2025), at 1.

⁸ *Ibid.*

⁹ Molnar, *supra* note 3; Singh & Agarwal, *supra* note 7, at 2–3.

¹⁰ *Supra* note 7, at 2.

maps of responsibility are changed - at times obscuring constitutional responsibility for harm.¹¹

Machine-Learning: Bias, Data, and Predictive Logic

Machine learning algorithms are trained on statistical correlations from previous data. Models used for predictive policing, welfare eligibility assessment, and facial recognition operate according to this principle. There are two technical features that are significant from a constitutional point of view:

- a) Correlation vs. Causation: Algorithms identify correlations that can be predictive, but which are neither legally applicable, nor normatively warranted. A model might show that residents of a neighbourhood are statistically more likely to be arrested; Using such a correlation to direct policing reinforces historical biases in law enforcement instead of addressing causation.¹²
- b) Amplification of bias: When the training data is biased by policing, discriminatory lending practices, under- registration of certain communities, those trends are going to repeat and possibly amplify these injustices.¹³ Other jurisdictions, independently tested have revealed much higher error rates in facial recognition in darker-skinned women and people; Likewise results in India in the absence of dataset curation are likely to follow a similar pattern.¹⁴

Constitutionally, algorithmic bias is more than a mere technical flaw: It presents itself in discriminatory state action when the state relies on biased outputs in making decisions for the public.¹⁵

The “Algorithmic State” in the Indian Administrative Context

The Indian administrative structure is becoming increasingly digitised: Aadhaar-based services, e-governance platforms, crime databases, CCTV systems, and centralised biometric databases are the foundations of a data ecosystem that can be integrated with algorithms. Two institutional trends are particularly important:

- a) Automation of routine decisions: Eligibility checks, identity verification and preliminary risk scores are also automated to ease the administrative load.

¹¹ *Supra* note 1.

¹² *Supra* note 2, at 3

¹³ *Ibid.*

¹⁴ Rahul Shamota, Govind Yadav & Arpan Verma, “Artificial Intelligence and Criminal Justice: Challenges to Due Process and Legal Accountability in India,” in *Artificial Intelligence and the Law* 1 (2026), at 2.

¹⁵ *Supra* note 7, at 5-6.

- b) Outsourcing and procurement: Many algorithmic systems are developed by private vendors or integrated through public–private partnerships, raising questions about state accountability and transparency in procurement and design.¹⁶

The Indian context makes it all more complicated due to socio-economic heterogeneity and unequal access to digital services, the presence of linguistic diversity and deep structural inequalities, algorithmic systems developed on incomplete or asymmetric data sets are especially likely to lead to exclusionary results. Additionally, centralised databases (e.g., voting lists, passport, Aadhaar linkages) create single points where misclassification can ripple across all services.

In Kerala's experiment with algorithmic governance—including AI-powered automated traffic enforcement systems launched in 2023—the state's e-governance policy has sought to integrate ICT, big data, and AI technologies into essential state services.¹⁷ While such systems have been deemed successful in reducing road accidents and increasing state revenue through automatic processing of fines, they also raise important questions about data sovereignty, discretion, agency, and the potential harms of AI.¹⁸

Delegation of State Power to Non-Human Systems: A Constitutional Puzzle

The delegation of legislative power has long been a subject of constitutional debate. The Supreme Court, following the principles established in *In re: Delhi Laws Act*, has held that legislatures have plenary power within their respective fields and may delegate powers within certain limits, but cannot abdicate their essential legislative functions.¹⁹ Essential legislative function consists of laying down legislative policy with sufficient clearness and enunciating the standards to be enacted into a rule of law. What can be delegated is only the task of subordinate legislation ancillary to the statute which delegates the power to make it.²⁰

A similar analysis applies to algorithmic delegation: what are the constitutional constraints on delegating decision-making power to non-human, opaque, and adaptive systems?

Three interlinked puzzles arise:

- a) **Legality:** Does algorithmic decision-making meet the requirement of the “procedure established by law” when there is no law to authorise the specific automated processes?

¹⁶ Brennan M Kiel and Karen Levy, “Strange Loops: Apparent Versus Actual Human Involvement in Automated Decision Making” (2019) 34 *Berkeley Technology Law Journal* 745.

¹⁷ *Supra* note 1.

¹⁸ *Ibid.*

¹⁹ *In re: Delhi Laws Act*, 1951 SCR 747; *Ramesh Birch v. Union of India*, (1990) 3 SCC 318. See also *Devi Das Gopal Krishnan v. State of Punjab*, AIR 1967 SC 1895.

²⁰ *Municipal Corporation of Delhi v. Birla Cotton, Spinning and Weaving Mills*, AIR 1968 SC 1232.

Without explicit legislative authorisation, algorithmic encroachments on rights (e.g., privacy) are constitutionally questionable.²¹

- b) Non-arbitrariness: Human discretion is open to justification and judicial control; can algorithmic outcomes be considered administrative justifications subject to judicial oversight? In case the model is opaque, the courts will be unable to determine its intelligibility.²²
- c) Accountability: The definition of “State” in Article 12 encompasses bodies that perform public functions; however, application of the law is complicated by the contractual obscurity and claims of commercial secrecy.²³

These conundrums can be resolved through doctrinal adaptation. The courts must demand explicit statutory bases, require explainability where rights are a concern, and treat the application of outsourced algorithms as state action where algorithms exercise sovereign functions.

3. CONSTITUTIONAL FRAMEWORK

There is a cluster of rights that the Indian Constitution safeguards, which have been at the centre of the discussion on the subject of algorithmic governance. The doctrinal core is composed of three provisions, namely, Articles 14 (equality), 19 (freedoms) and 21 (life and personal liberty), by which algorithmic intrusions must be evaluated. Non-arbitrariness, legality, necessity and proportionality are tests of such non-arbitrariness, based on the interpretation of Supreme Court jurisprudence, especially interpretations of *The Maneka Gandhi* and *Puttaswamy decisions*, which are adaptable to the technological circumstances.²⁴ This section works out how each of these Constitutional provisions translates into certain legal limitations in algorithmic governance. It begins with Article 14, as equality and the exclusion of arbitrariness are the main limitations to the state decision-making; Articles 19 and 21 are discussed in the following subsections.

Article 14 — Equality, Non-Arbitrariness, and Algorithmic Decision-Making

Article 14 of the Indian Constitution guarantees “equality before the law” and “equal protection

²¹ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

²² Abhinav Viswanath & Krutha Janani, “Algorithmic Governance and AI-Driven Public Administration: Reimagining Accountability in Indian Civil Service”, 9 *International Journal of Law Management & Humanities* 1 (2026), at 2.

²³ *Ajay Hasia v Khalid Mujib Sehravardi* AIR 1981 SC 487.

²⁴ *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3; *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248; *Justice K.S. Puttaswamy (Retd) v. Union of India*, (2017) 10 SCC 1.

of the laws". The current doctrine of the Supreme Court identifies Article 14 as a prohibition on arbitrary state action and provides that any sort of categorization between individuals or classes must be based on an intelligible differentia and it must have a rational link with the object sought.²⁵

Algorithmic governance challenges this concept of equality on the following grounds:

- a) Intelligible differentia and algorithmic classification: There are numerous machine learning systems where people are determined to belong to a risk group or eligibility group based on high dimensional feature representations that are not legally intelligible. A social allocation model may cluster the candidates based on latent variables based on the transaction history, mobile usage or geolocation. These features are not legal categories; they fail to satisfy the intelligible differentia test since the affected individuals have no understanding on what a legally relevant criterion they are differentiated by.
- b) Opacity as arbitrariness: Cases in which the decision is supported by a proprietary model that generates an outcome-score which cannot be explained intelligibly, courts have no meaningful way to address the question of whether the classification bears a rational relationship to the purpose of the legislature. The black box issue thereby transforms the algorithmic obscurity into the possible arbitrariness. Supreme Court's emphasis on non-arbitrariness in *E. P. Royappa* suggests that courts should view automated and opaque decision-making with skepticism when rights are materially affected.²⁶
- c) Disparate impact and indirect discrimination: Indirect discrimination can occur even in the case of neutral algorithms which have disparate effects on vulnerable or protected groups. Indian equality jurisprudence acknowledges formal and substantive equality; a discriminatory effect, although not intentional, could be a breach of Article 14 by creating an unwarranted exclusion or concentration of burdens. Strategically misclassifying or misidentifying people of a specific caste, religion, gender or language group will thus have to be scrutinized closely.
- d) Addressing algorithmic arbitrariness: Article 14 demands remedies that are actually accessible. In the case of algorithmic governance, institutional solutions are algorithmic impact assessment prior to implementation, the requirement to disclose

²⁵ *State of West Bengal v Anwar Ali Sarkar* AIR 1952 SC 75; *EP Royappa v State of Tamil Nadu* (1974) 4 SCC 3.

²⁶ *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.

error rates by demographic characteristics, independent audits, and legislative restrictions on high-risk usages of the algorithms. Rules of evidence like the disclosure of algorithmic logic by the state is one of the judicial remedies in a constrained and confidential manner to be reviewed by adjudication.

Article 19 — Freedom of Expression, Movement, Trade, and Algorithmic Chilling Effects

The concept of algorithmic governance is becoming dominant in the manner in which people operate, communicate and engage in life within the society. Social media control mechanisms, automated surveillance systems and predictive policing technologies can produce unconstitutional chilling effects on freedom of speech, expression and movement.

In *Shreya Singhal* case²⁷, the Supreme Court accepted the doctrine of chilling effect and declared that restrictions on freedom of expression that were vague or over broad were against the Article 19(1)(a). Content moderation by the State, or State-led moderation by the private platforms, can generate the same unconstitutional effects.

Equally, algorithmic risk analysis to limit movement or provide travel warnings could play a role in an unreasonable restriction under the scope of Article 19(1)(d). Article 19(1)(g), which covers trade and profession rights, can be breached when it is the artificial and automated blacklists, risk-scoring of the employer, or automated background tests that prevent employment.

Under Article 19(6), restrictions must satisfy:

- a) Legality — based on statutory authority.
- b) Legitimate aim
- c) Proportionality, including the least restrictive alternative test.

The Supreme Court reaffirmed this in *Modern Dental College* and later in *Puttaswamy (Aadhaar)* case.²⁸ Algorithms that are implemented without the support of the legislation and without any guarantees fail the first part and are unconstitutional.

Article 21 — Automated Decision-Making, Due Process, and the Right to Explanation

Article 21 respects life and personal liberty and encompasses the rights to privacy, dignity, autonomy, and due process. Algorithms are often used in making decisions that touch on:

- access to welfare benefits

²⁷ *Shreya Singhal v Union of India* (2015) 5 SCC 1.

²⁸ *Modern Dental College v State of MP* (2016) 7 SCC 353; *KS Puttaswamy v Union of India (Aadhaar-5J)* (2019) 1 SCC 1.

- healthcare allocation
- policing and surveillance
- authentication of digital identity
- freezing of bank accounts or tax audits
- enrolment in learning institutions or scholarships.

The Court in the *Puttaswamy (Privacy)* judgment accepted informational privacy as a fundamental right, and asserted that any State data-processing system should meet the legality, necessity, proportionality and procedural requirements.²⁹

Given that algorithmic systems are used in processing huge volumes of personal information, the constitutional principles described in *Puttaswamy* could be applied directly.

In *Pragya Prasun v. Union of India*³⁰, the Supreme Court held that the right to digital access is a part of the right to life guaranteed by Article 21 of the Constitution. Justices J.B. Pardiwala and R. Mahadevan in the two-judge bench observed that the right to life guaranteed under Article 21 must be re-interpreted in the context of the present-day technological scenario, in which access to various essential services, governance, education, healthcare and economic opportunities is increasingly dependent on digital platforms.

Article 32 and 226 — Judicial Review of Algorithmic Decisions

Algorithmic decisions are subject to review through written jurisdiction. The courts have repeatedly stated that the State action, including the delegated activities, should be under the jurisdiction of the courts.³¹

This includes:

- computerized welfare determinations.
- classifications of predictive policing.
- scoring systems which are implemented by the authorities at large.
- authentication errors of digital identity.

The Court held in *Anuradha Bhasin v Union of India & Ors*³² that any limitation to fundamental rights should be subject to review and that the state should provide information on what material the decision is grounded upon. When applied to algorithmic governance, this means that the State needs to reveal: the model deployed, the variables factored, the training

²⁹ *Supra* note 4.

³⁰ *Supra* note 5.

³¹ *L Chandra Kumar v Union of India* (1997) 3 SCC 261.

³² AIR 2020 SC 1308.

data, the decision-making logic, and the protection against misuse. Opaque systems violate constitutional requirements of transparency.

Separation of Powers and Excessive Delegation to Algorithms

The other constitutional issue of great significance is whether the state can outsource critical decision-making to algorithms without contravening the separation of powers. Excessive delegation of the necessary legislative functions is barred by the Supreme Court.³³ Similarly, the executive has no power to design algorithmic systems that can successfully rewrite policy unless it has a legislative mandate.

Federalism Concerns in Centralised Databases

Algorithms based governance is based on large centralised data structures (e.g., Aadhaar, CCTNS, NDDb, welfare databases). Federalism is problematic when the Union gathers or processes the information of the states that lack any legislative authority. The Court in *State of Rajasthan v Union of India* believed that the federal balance is among the basic structure.³⁴ Centralized algorithmic systems used for policing, targeting welfare, or allocating resources can disrupt this balance.

4. ADMINISTRATIVE LAW AND ALGORITHMIC DECISION-MAKING

The postulates of administrative law are applicable to algorithmic governance to the fullest. The tools of State power are automated decision-making systems (hereinafter referred to as ADS) employed by the public authorities; thus, they must be aligned with the fundamental principles of the Indian administrative law: non-arbitrariness, reasoned decision-making, transparency, proportionality, observance of statutory boundaries, fairness, and natural justice.³⁵

The conceptual instruments to control the algorithmic decisions already exist in Indian administrative law.

Doctrine of Reasoned Decisions (Speaking Orders)

The Supreme Court has repeatedly held that administrative orders affecting rights must be

³³ *In re: Delhi Laws Act* 1951 SCR 747.

³⁴ (1977) 3 SCC 592.

³⁵ M.P. Jain & S.N. Jain, *Principles of Administrative Law* (Wadhwa Nagpur, 9th edn., 2021).

reasoned. Examples of algorithmic output that are not explained do not conform to this requirement. The Court in *Kranti Associates v Masood Ahmed Khan*³⁶ has said that reasons are the core of any finding; they are a key to judicial review. In case an ADS generates a welfare denial, or tax risk score, or predictive policing classification, and lacks an explanation, human-readable, the decision cannot be made.

Algorithms often produce statistical correlations rather than reasons, which Indian law does not recognise as sufficient justification. Thus, the right to reasons implicitly requires a right to explanation of algorithmic decisions.

4.2 Natural Justice — Notice, Hearing, and the Right to Contest

All the administrative procedures should meet:

1. Audi alteram partem — right to be heard;
2. Nemo iudex in causa sua — rule against prejudice.

Algorithmic systems contravene natural justice where:

- a) individuals are not informed of the use of an algorithm,
- b) the rationale or motivators are not revealed,
- c) there is no redress or picture of the automated result,
- d) the system is biased towards history (i.e., caste, religion proxies),
- e) non-government vendors come up with algorithms without responsibility.

The Supreme Court in *Mohinder Singh Gill v. Chief Election Commissioner*³⁷ held that fairness is the soul of natural justice. This is contrary to an ADS that refuses benefits without hearing.

4.3 Algorithmic Bias as Administrative Bias

Courts have held that the appearance of prejudice nullifies administrative action.³⁸ Discriminatory results of skewed-trained automated systems can be produced depending on caste or religion-driven discriminatory outputs. In *A. K. Kraipak v. Union of India*³⁹, the Court decided that administrative actions should not be biased and should observe fairness. On proxies, like area, language or consumption patterns, an indirect discrimination can be generated by use of algorithmic models that mimic administrative decisions of a biased kind.

³⁶ (2010) 9 SCC 496.

³⁷ (1978) 1 SCC 405.

³⁸ *Maneka Gandhi v Union of India*, 1978 SCR (2) 621; *AK Kraipak v Union of India* (1970) 1 SCR 457.

³⁹ (1970) 1 SCR 457.

4.4 Delegated Legislation and Excessive Delegation to Third-party Algorithms

The Supreme Court in a case known as *Delhi Laws Act*, held that the key legislative functions could not be delegated.⁴⁰ Algorithms used by the State are frequently developed by private companies. This raises concerns of horizontal opacity and privatisation of State functions. If private algorithmic designers decide entitlement to social protection schemes, police risk assessments, and tax audit categorisation etc., it will be unconstitutional privatization of State decision-making.

Likewise, the executive action should not cross limits of the statutes. Algorithms must not be able to add new criteria which are not allowed by the law. This amounts to unconstitutional outsourcing of State decision-making.

Obligations of Procedural Fairness and Transparency

The administrative law mandates that the decisions taken be clear, open to review and grounded on evidence before the party in question.

In *CERC v. Excide Industries Ltd*⁴¹, the court pointed out that administrative fairness required transparency. Algorithms that are based on proprietary code or unknown data sets do not comply with this requirement as citizens are unable to see on what grounds is the decision of the computer based.

Judicial Review of Algorithmic Decisions

Judicial review under Articles 32 and 226⁴² fully extends to decisions based on ADS. The legality of the deployment, compliance with the constitution, data used, rationality of the model, protecting and balancing can be reviewed by the courts.

In the *Ajay Hasia* case⁴³, the Supreme Court has decided that judicial review should be applied even where contractual means are used to conduct state functions. Equally, bodies that fulfilled public functions were also subjected to the jurisdiction of the Court in *Binny Ltd v V Sadasivan*.⁴⁴ Therefore, even private firms that make public algorithms are subject to the law.

5. CASE STUDY

5.1 ALGORITHMIC WELFARE EXCLUSION VIA AADHAAR AUTHENTICATION

The application of Aadhaar-based biometric authentications in systems of social assistance delivery is one of the most eloquent examples of algorithmic governance and its constitutional

⁴⁰ *In re: Delhi Laws Act*, 1951 SCR 747.

⁴¹ (2020) 12 SCC 524.

⁴² The Constitution of India, arts 32 and 226.

⁴³ *Ajay Hasia v. Khalid Mujib Sehravardi*, AIR 1981 SC 487.

⁴⁴ *Binny Ltd. v. V. Sadasivan*, (2005) 6 SCC 657.

perils in India. Authentication (fingerprint or iris scan) by Aadhaar is commonly used in institutions like the Public Distribution System (PDS) and the pension schemes and cash transfer programs to check recipients. However, years of research, government reports and audit findings are proving that persistent issue exists: biometric incompatibility, which causes the unjustified denial to actual beneficiaries.

Indicatively, a close examination of the Aadhaar-authentication process in Andhra Pradesh PDS program found that during the first half year of December 2017, of the 3.77 million authentication processes, nearly 94,030 were unsuccessful.⁴⁵ Among such failures, 92 per cent were explained by a biometric mismatch: fingerprints or an iris scan is not corresponding to the template registered. Such figures are not insignificant: millions of individuals are trying to authenticate every month, and even a slight percentage of denials will lead to significant deprivation of access to vital services to the population.

A broad report on Aadhaar also reported that in some of the states a very high percentage of the ePOS (electronic point of sale) failures at the PDS stores were due to biometric mismatch in the year 2016-17.⁴⁶ This is identical to the UIDAI own error code documentation: Common failure codes include "300 biometric data does not match" which means that the system has been known to reject scans that fail to match stored biometric templates.⁴⁷

Such failures have a grave human price. Survey of civil-society (e.g., by Khera and Amod Moharil) discover that elderly people, manual workers and low-income dwellers, whose fingerprints might be worn out or deformed, are repeatedly rejected, spend time and take cumbersome minerals to Aadhaar correction centres.⁴⁸ In other situations, there are people who make numerous visits within the course of a month in order to make attempts to update or modify their biometric information. attempt to update or modify their biometrics. The Comptroller and Auditor General (CAG) of India also has indicated weaknesses in this: out of over 30 million biometric updates annually, a significant amount of it is a consequence of authentication failures.⁴⁹

⁴⁵ Indicus Centre for Financial Inclusion, *White Paper: Improving Cash Benefit Transfers – The Role of Biometric Authentication Failures* (June 2022).

⁴⁶ IDinsight, "State of Aadhaar Report 2016–17," available at: <https://www.idinsight.org/project/state-of-aadhaar-initiative-2016-2018/> (last visited on 9 November 2025).

⁴⁷ Unique Identification Authority of India (UIDAI), "What Are Error Codes?" available at: <https://uidai.gov.in/en/305-faqs/aadhaar-online-services/aadhaar-authentication-history/10779-what-are-error-codes.html> (last visited on 17 November 2025).

⁴⁸ *The Wire*, "Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors," available at: <https://thewire.in/rights/digital-exclusion-poor-elderly-face-the-brunt-of-aadhaar-based-authentication-errors> (last visited on 4 November 2025).

⁴⁹ Government of India, Rajya Sabha, "Unstarred Question No. 882" (UIDAI response on exception-handling guidelines for benefit schemes), available at: [https://uidai.gov.in/images/rajyasabha/RSPQ882\(Unstarred\).pdf](https://uidai.gov.in/images/rajyasabha/RSPQ882(Unstarred).pdf) (last visited on 7 November 2025).

To make this issue even more complicated, the Unique Identification Authority of India (UIDAI) admitted in an affidavit submitted to the Supreme Court that authentication failure rates were 8.54 percent with iris scans and 6 percent with fingerprint scans. Even though the UIDAI says that failure does not imply rejection, and mechanisms have been implemented to handle exceptions (e.g. by using OTP-based backup authentication), in reality a significant portion of requesting agencies (such as welfare departments) do not actively deploy such fallbacks.⁵⁰

Aadhaar-linked accounts are automatically deactivated because of so-called duplicates being detected by algorithmic deduplication systems and there is no effective notification about this or any possibility of appeal. This means that citizens are deprived of food rations, pensions and cash transfers. These exclusions are not imaginary: they amount to deep structural injuries, especially to marginalized groups.

This case study shows that an algorithmic mechanism, as a mechanism of inclusion and efficiency, in fact causes extensive constitutional exclusion on a large scale - proxy of an administrative role, but mediated by biometric algorithms.

5.2 Algorithmic Tools in the Special Intensive Revision (SIR) of Electoral Rolls — Exclusion, Due Process, and Constitutional Rights

A. Introduction to the SIR Case Study

The Special Intensive Revision (SIR) of electoral rolls conducted by the Election Commission of India (ECI) in 2025-2026 is a compelling example of algorithmic governance in action. The SIR was a comprehensive revision exercise that, according to petitioners, prepared electoral rolls “de novo” using the 2002 or 2003 electoral rolls as a baseline, with the most significant exclusions occurring in Bihar and West Bengal (over 76 lakh names deleted in West Bengal alone).

The exercise was started in November, 2025 with the stated objective to resolve the issues with voter lists from the baseline electoral rolls of 2002. West Bengal alone accounted for about 1.36 crore entries flagged for discrepancy.⁵¹

⁵⁰ *Biometric Update*, “High Rates of Aadhaar Biometric Verification Failure Lead to UIDAI Scrutiny,” available at: <https://www.biometricupdate.com/202507/high-rates-of-aadhaar-biometric-verification-failure-leads-to-uidai-scrutiny> (last visited on 10 November 2025).

⁵¹ *National Herald*, “Why SIR in Bengal Stands Apart: Chaos Unlike Other States” (25 March 2026), available at: <https://www.nationalheraldindia.com/politics/why-sir-in-west-bengal-stands-apart-chaos-unlike-other-states-before-assembly-elections-2026> (last visited on 5 July 2026).

B. How the Algorithm Operated: The ERONET Software and Its Failures

The algorithmic aspect of the SIR appeared in the identification of "logical discrepancies" through the ERONET software system, which flagged large numbers of entries as 'logically inconsistent.' The software also had some difficulties with inconsistencies in transliteration from Bengali to English in the electoral lists, such as the difference between 'Mohammed' and 'Muhammad' or 'Mondal' and 'Mandal', officials said. In many instances, the quality of the scans of the older electoral lists made it difficult to match them electronically with family records.⁵² The ERONET system detected inconsistencies using automatic rules such as age difference between parents and children.

C. Algorithmic Bias and Disproportionate Targeting

The algorithmic process didn't just make mistakes; it made specific kind of mistakes – mistakes that had a certain demographic trait. The analysis of SIR data by district showed that the districts with Muslim majority had much higher rates of flagging. In Murshidabad district, where Muslims make about 66% of the electorate, the flagging rate stood at 30.20% of all electors, the highest rate in the dataset. Bankura (8% Muslim) and Purulia (7.8% Muslim) had the lowest Muslim population where only about 10-13% of Muslims were heard. Specifically, the rules of this algorithm were:

The "Progeny > 6" rule, which targeted those with more than six offspring, skewed the data towards Muslim majority areas.⁵³

The "Parent Age Difference < 15" rule flagged records where the parent was less than 15 years older than the child.⁵⁴

The Amartya Sen incident brought into light the arbitrary flagging of the software. The age difference of the person from his mother as entered in the database was less than 15 years, which leads to the automatic verification of the information according to SIR norms and hence a hearing notification was issued to the Nobel Laureate. The Chief Electoral Officer, West Bengal, clarified that the notice was generated "in parity with the other discrepancy cases" Family members of Sen said that his mother was born in 1914, a gap of 19 years, but that the records listed an incorrect birth date. The issue was resolved by officials visiting Sen's residence to complete the formalities.

⁵² *Ibid.*

⁵³ *Ibid.*

⁵⁴ *The Statesman*, "ECI Explains SIR Notice to Amartya Sen, Cites 'Age Difference with Mother' in Voter Records" (8 January 2026), available at: <https://www.thestatesman.com/india/eci-explains-sir-notice-to-amartya-sen-1503269123.html> (last visited on 3 July 2026).

D. Procedural Failures and Due Process Violations

The algorithmic governance model operated without adequate procedural safeguards. The total disenfranchisement was massive, with nearly 76 lakh names being deleted from the voter lists in West Bengal, of which about 63 lakh had been in previous rolls and about 13 lakh were in more recent adjudications.⁵⁵ There were also many instances of disenfranchisement in recent adjudications.⁵⁶ Of the 32 lakh cases that have been adjudicated, nearly 40 per cent (roughly 13 lakh names) have not appeared in the first supplementary list issued on 23 March 2026. There were concerns that a large proportion of the affected were from economically vulnerable communities, such as migrant workers, women in informal employment, and from the Matua community, among whom many did not have documentary records since 2002.⁵⁷

E. The Supreme Court's verdict and its Constitutional implications

A bench of Chief Justice Surya Kant and Justice Joymalya Bagchi of the Supreme Court, on May 27, 2026, said that the ECI could conduct special revisions under Article 324 of the Constitution and Section 21(3) of the Representation of the People Act. The Court went on to say that the ECI could make a limited enquiry into citizenship for the purpose of satisfying itself as to whether a person was eligible for inclusion in the electoral roll, but that it did not make a determination of citizenship in the strict sense, and that any action taken as a result of such an enquiry was limited to electoral consequences.⁵⁸ The Court clarified that deletion from electoral roll is not a legal declaration that the individual is not a citizen and that it is duty of the ECI to refer the individual to the Competent Authority under the Citizenship Act, 1955, for adjudication if it is satisfied that the individual is not deserving of being in the electoral roll. The Court directed the ECI to refer such cases within four weeks to the Competent authority under the Citizenship Act, 1955, for adjudication of their citizenship. The Competent Authority shall take the necessary decision in accordance with law, preferably before the next elections, after giving notice and an opportunity of hearing to deleted individuals.⁵⁹ The SIR process exemplifies the way in which algorithmic governance, when used in the absence of adequate safeguards, may prevent the governance of

⁵⁵ *Supra* note 51.

⁵⁶ *Supra* note 51.

⁵⁷ *ThePrint*, “SC Backs EC's Power to Conduct SIR, Says Exercise Breathes Life into Mandate for Fair Polls” (27 May 2026), available at: <https://theprint.in/india/sc-backs-ec-power-sir-bihar/> (last visited on 4 July 2026).

⁵⁸ *Ibid.*

⁵⁹ *Ibid.*

administration from being scrutinized and may result in systematic exclusion of minority communities, suggesting a profound violation of equality under Article 14. While the Supreme Court has found the SIR constitutional, its ruling has triggered a citizenship verification mechanism that critics fear can be used as a stealth National Register of Citizens.

6. COMPARATIVE ANALYSIS OF ALGORITHMIC GOVERNANCE FRAMEWORKS

The global debate on algorithmic governance has resulted in a broad variety of strategies: statutory, administrative and judicial. An overview of the chosen jurisdictions shows that India is aware of the constitutional implication of automated decision-making, but has no substantial regulation model. The European Union, the United States and the United Kingdom experiences are instructive in understanding how to develop relevant protection of innovation without having to infringe on the rights.

6.1 European Union: Rights-Centric, Regulation-First Model

The European Union (EU) has created one of the most complex mechanisms of regulating the algorithmic decision-making process, which is based mainly on the General Data Protection Regulation (GDPR). Normative structure against automated decision-making protects individuals against the cybernetic approach to decision-making through the cumulative establishment of Articles 13, 14, and 15 and 22 of the GDPR.⁶⁰ When the consequences of the decision are severe, the GDPR provides the right against a decision based on automated processing (including profiling) alone. It also involves substantial definitions, rules of access and manual intervention.

The next planned AI Act in the EU supplements the GDPR in that AI systems are classified into systems that are prohibited, high risk, and low risk. Systems with high risk (biometric identity systems or welfare-benefit eligibility systems) should be subject to compliance tests, must include human intervention, be accurate and have the ability to trace datasets and decision logic. The public bodies will be obliged to have algorithmic impact assessments (AIAs) and ensure that they have all the records that they can be audited.⁶¹

It is a rights-based regime that may be seen as a proactive ex-ante model of regulating algorithmic governance, and it is based on structural protection mechanisms instead of case-

⁶⁰ Regulation (EU) 2016/679 (General Data Protection Regulation), arts 13–15 and 22.

⁶¹ Information Commissioner's Office (UK), "Data Protection Impact Assessments" (ICO Guidance, 2023).

specific litigation, something which India is currently lacking.

6.2 United Kingdom: Emphasis on Accountability and Impact Assessments

The United Kingdom adheres to a hybrid approach based on GDPR principles, but formed by the local administrative law customs. The Data Protection Impact Assessments (DPIA) are required by the Information Commissioner Office (ICO) regarding algorithmic systems that are associated with risks to the rights of people.⁶² Departments in a government that use automated decision-making tools are required to post Algorithmic Transparency Records, which show the purpose of the model, characteristics of the dataset, risk classification, and fallback.⁶³

British case law also enhances administrative requirements. In *R (Bridges) v. The Court of Appeal, South Wales Police*⁶⁴, it was declared that the legality, necessity, and proportionality of using live facial recognition, including measures against discriminatory consequences, must be met. This adjudication states that algorithmic rulings are liable to the conventional public-law principles, like reasonableness, equity, and visibility.

6.3 United States: Sector-Specific Regulation and Anti-Discrimination Focus

The US lacks an omnibus data protection statute, but has created an effective sector-focused and rights-and-remedy ecosystem. Anti-discrimination provisions on automated decision-making regarding housing, employment, credit scoring, and insuring require civil-rights legislation, which includes the Civil Rights Act, the Fair Credit Reporting Act (FCRA), and the Equal Credit Opportunity Act (ECOA).

Much more recently, normative guidelines on discriminatory algorithms, human alternatives, and notice-and-explanation requirements were defined in the White House Blueprint on an AI Bill of Rights (2022).⁶⁵ Federal agencies have started to put these principles into practice although not in a binding way. To illustrate, the Federal Trade Commission (FTC) views the use of AI in manners perceived to be unfair or deceptive like opaque algorithmic scoring or discriminatory outcomes as a violation of the consumer protection law.⁶⁶

This model shows that the absence of widespread AI legislation can be partially mitigated by

⁶² *Ibid.*

⁶³ UK Central Digital and Data Office, *Algorithmic Transparency Recording Standard* (Cabinet Office, 2021).

⁶⁴ [2020] EWCA Civ 1058.

⁶⁵ White House Office of Science and Technology Policy, “*Blueprint for an AI Bill of Rights*” (2022).

⁶⁶ Federal Trade Commission, “*Aiming for Truth, Fairness, and Equity in Your Company’s Use of AI*” (FTC Business Guidance, 2021).

a well-established anti-discrimination doctrine, which would be sufficiently enforced by the regulation.

6.4 Lessons for India

Across all these jurisdictions, one could single out four thematic principles:

- (i) need of transparency and explanation;
- (ii) compulsory human control systems;
- (iii) fair and accurate independent audits; and
- (iv) ex-ante risk evaluation prior to implementation of critical systems.

7. CONCLUSION AND SUGGESTIONS

Algorithmic governance is not inherently unconstitutional, but it has potential dangers that must be carefully safeguarded by the constitution. The Indian constitutional law is already rich in a set of doctrinal tools, such as equality, due process, dignity, proportionality, transparency, judicial review, which now has to be transformed into automated decision-making. The Aadhaar authentication exclusions present an actual, modern-day example of how an algorithmic system, when designed or implemented in an inappropriate manner, may infringe on basic rights at a massive scale. An AI governance structure needs to be fair and explainable, non-discriminatory, procedurally guaranteed, human controlled and transparent. It is only then that automated governance will strengthen and not cripple the constitutional democracy in India.

7.1 Proposed Regulatory Framework for Algorithmic Governance in India

The increased use of algorithmic decision-making in welfare management, predictive policing, financial technology, and the identification systems in India require a regulatory regime in the form of a constitutional value.

7.1.1 Statutory Recognition of Automated Decision-Making

The Digital Personal Data Protection Act (DPDPA)⁶⁷ should be amended in India by introducing a specific law on algorithmic accountability or by including similar clauses in the current legislation. There should be clear legislation on automated decision making to include biometric identity systems, scoring models and algorithmic eligibility assessment tools applied

⁶⁷ The Digital Personal Data Protection Act 2023

by the authorities of the people.

7.1.2 Mandatory Algorithmic Impact Assessments (AIAs)

The deployment of an algorithmic system that impacts rights or entitlements should be legally mandated to undertake an algorithmic impact assessment by the public agencies before its implementation. The AIA should take into consideration such factors like purpose, sources of data, accuracy, risks of exclusion that can be predicted, demographic considerations, alternative approaches, and mitigation plans.

7.1.3 Transparency, Disclosure, and Public Notice

The public agencies should be required to release model summaries that will contain the following: the purpose of the system, the accuracy or failure rates, any known biases in the system, the data sets used, fallback mechanisms, and grievance procedures. These reports ought to comply with the pattern of the “Algorithmic Transparency Standard” of the United Kingdom.

7.1.4 Human-in-the-Loop Requirements

Whether it be a decision touching on one of the various fundamental rights, a right to welfare, an employment benefit or a criminal justice outcome, mandatory human review should be applied. Decisions made by the automated system must not lead to denial of the benefits unless a human agent verifies the files and outlines the same in written format.

7.1.5 Rights to Notice, Explanation, and Contestation

Under these conditions, individuals should be entitled to learn when automated system is in place, to receive a meaningful Explanation, to demand a human consideration, to object an unfavourable automated decision and to get records that concern the decision, which may include audit logs. These rights bring to operation the concepts of fairness and due-process in Articles 14 and 21 of the Indian Constitution.

7.1.6 Independent Audits and Bias Assessments

Any high-risk algorithmic systems should undergo periodic 3rd party audits. The audit needs to evaluate: accuracy; demographic equity; variation in error rates; data quality problems; structural biases.

7.1.7 Data Governance and Quality Standards

Many algorithmic damages are associated with poor-quality and incomplete or old data sets. The government agencies are to be able to implement strict standards of data quality, such as data minimization, regular checking, friendly correction process, and requirement of recording of all automated decisions.

7.1.8 Strong Remedies and Liability Framework

Citizens should be allowed to claim damages in case of exclusion or excess damage, individual responsibility against governmental organizations in case of an algorithm malfunction, as well as institutional solutions in case of harmful consequences by the courts or professional regulators. In cases where algorithmic systems result in repeat exclusions (like chronic biometric mismatch), official authorities should put the system on hold or adjust it until doing so returns compliance.

