ALGORITHMIC GOVERNANCE AND FUNDAMENTAL RIGHTS: RECONSTITUTING CONSTITUTIONAL PROTECTIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE IN INDIA

[1]Dr Saurabh Dudi

ABSTRACT

The rapid proliferation of artificial intelligence technologies in governmental administration, judicial adjudication, law enforcement, and public service delivery has generated profound constitutional questions that existing jurisprudence in India is ill-equipped to resolve. This paper examines the constitutional ramifications of algorithmic governance, focusing on the potential conflict between state-deployed AI systems and the fundamental rights guaranteed under Part III of the Constitution of India, 1950. Drawing upon landmark decisions of the Supreme Court of India, including Justice K.S. Puttaswamy (Retd.) v. Union of India, the Aadhaar judgment, and Shreya Singhal v. Union of India, the paper argues that algorithmic decision-making constitutes a novel form of state action that demands heightened constitutional scrutiny. The paper identifies three principal zones of constitutional tension: the right to privacy and autonomy under Article 21, the right to equality and non-discrimination under Articles 14 and 15, and the right to freedom of expression under Article 19(1)(a). It further explores the doctrine of due process and natural justice as a check on automated state action, contending that procedural fairness cannot be bypassed through technological delegation. The paper concludes by proposing a framework of constitutional AI governance premised on transparency, explainability, algorithmic accountability, and judicial reviewability, and calls for the enactment of a dedicated AI Regulation Act anchored in fundamental rights principles.

[1] **Dr Saurabh Dudi**, *Assistant Professor, School of Law, JECRC University, Jaipur*

Keywords: *Algorithmic Governance, Artificial Intelligence, Fundamental Rights, Constitutional Law, Right to Privacy, Article 14, Article 21, Due Process, AI Regulation, India*

I. INTRODUCTION

The emergence of artificial intelligence as an instrument of governmental power marks a pivotal and potentially transformative moment in the history of constitutional democracy. States across the world, including India, are increasingly deploying AI-driven systems to perform functions that were once exclusively within the domain of human deliberation: welfare eligibility assessments, judicial risk profiling, predictive policing, content moderation, tax surveillance, and biometric identification. While proponents argue that algorithmic governance enhances efficiency, reduces human bias, and scales public administration, critics warn of opacity, discriminatory outcomes, erosion of individual agency, and the wholesale displacement of constitutional safeguards.

India stands at a particularly consequential crossroads in this regard. The country has undertaken one of the world's most ambitious digital governance projects through the Aadhaar biometric identity system, the Digital India initiative, and the proposed National AI Strategy.[2]

At the same time, India's constitutional architecture, grounded in the transformative vision of the framers and interpreted expansively by the Supreme Court over seven decades, provides a rich normative framework for evaluating the legitimacy of state action. The central question this paper seeks to address is deceptively simple yet constitutionally profound: when the state acts through an algorithm, does it remain bound by the Constitution in the same manner and to the same degree as when it acts through a human official?

The answer, this paper argues, must be an unequivocal yes. The Constitution of India does not permit the state to escape its constitutional obligations by interposing a layer of automated decision-making between itself and the citizen. Algorithmic systems deployed by the state or by

[2]NITI Aayog, National Strategy for Artificial Intelligence (Government of India, 2018); Digital India Programme, Ministry of Electronics and Information Technology, Government of India.

private entities exercising public functions are subject to the full rigour of fundamental rights review. Yet the existing doctrinal apparatus, developed in the context of human administrative action, requires significant re-conceptualisation to meet the challenge of algorithmic governance. The "black box" character of many AI systems, the statistical nature of algorithmic determinations, the potential for encoded and amplified discrimination, and the structural inability of affected individuals to meaningfully contest automated decisions all call for new constitutional thinking.

This paper proceeds in six parts. Part II surveys the landscape of AI deployment in Indian governance. Part III examines the constitutional framework applicable to algorithmic state action. Part IV analyses the specific fundamental rights implicated by algorithmic governance. Part V develops a critique of current constitutional doctrine and identifies its limitations. Part VI proposes a framework for constitutional AI governance. Part VII concludes.

II. THE LANDSCAPE OF ARTIFICIAL INTELLIGENCE IN INDIAN GOVERNANCE

A. Digital Infrastructure and AI Adoption

India's experiment with AI-driven governance has evolved along several intersecting axes. The Aadhaar system, administered by the Unique Identification Authority of India (UIDAI), represents perhaps the most extensive state deployment of biometric AI in the world, with over 1.3 billion enrolled individuals as of 2024.[3]

The system relies on algorithmic matching of fingerprint and iris biometric data to authenticate identity and thereby gate access to an expanding array of government services and welfare entitlements. The constitutional validity of Aadhaar was upheld, with significant limitations, by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, decided in 2018, though the dissenting opinion of Justice D.Y. Chandrachud raised foundational concerns

[3]Unique Identification Authority of India, Annual Report 2023-24 (UIDAI, 2024). The figure of over 1.3 billion enrolled individuals reflects UIDAI official statistics.

about surveillance, exclusion, and the algorithmic denial of rights that remain highly relevant to the present analysis.[4]

Beyond Aadhaar, AI systems are being piloted and deployed across diverse governmental functions. The Crime and Criminal Tracking Networks and Systems (CCTNS) project integrates facial recognition technology across police stations. The National Automated Facial Recognition System (AFRS), proposed by the National Crime Records Bureau, contemplates a nationwide database capable of real-time identification of individuals from CCTV footage.[5]

Various state governments have introduced AI-based predictive policing tools. The Integrated Disease Surveillance Programme has piloted algorithmic epidemic forecasting. The Income Tax Department employs machine learning models for risk-based scrutiny of tax filings. Increasingly, social welfare schemes administered through direct benefit transfer mechanisms use algorithmic eligibility filtering.

B. The Governance Deficit

Despite this accelerating deployment, India lacks a comprehensive regulatory framework specifically governing AI in the public sector. The Information Technology Act, 2000, and the rules framed thereunder are ill-suited to address the constitutional and governance challenges of AI. The Personal Data Protection Bill, which has undergone repeated revisions, and the Digital Personal Data Protection Act, 2023 (DPDPA), address data privacy but do not directly regulate algorithmic decision-making or mandate explainability and fairness in AI systems.[6]

[4]Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1 (Chandrachud J., dissenting). Justice Chandrachud described Aadhaar as enabling a \u201csurveillance state\u201d and identified exclusion harms arising from authentication failures as constitutionally significant.

[5]National Crime Records Bureau, Request for Proposal: Automated Facial Recognition System (Ministry of Home Affairs, Government of India, 2019). See also Vrinda Bhandari & Faiza Rahman, \u2018Understanding Automated Decision Making in India: A Primer\u2019 (2020) 15 Indian Journal of Law and Technology 1, 8-11.

[6]Information Technology Act, 2000, No. 21 of 2000; Digital Personal Data Protection Act, 2023, No. 22 of 2023.

The NITI Aayog's National AI Strategy and its Responsible AI for All framework articulate principles of responsibility, transparency, and accountability but remain non-binding policy instruments.[7]

This regulatory vacuum stands in sharp contrast with developments in comparative jurisdictions. The European Union's Artificial Intelligence Act, 2024, establishes a comprehensive risk-based regulatory regime applicable to both public and private AI systems, with specific requirements for high-risk AI in critical sectors including law enforcement, social benefits, and border management.[8]

The United States has issued Executive Orders on AI safety and has developed sector-specific AI governance frameworks. Canada has enacted the Artificial Intelligence and Data Act as part of Bill C-27.[9]

The absence of comparable legislation in India makes the constitutional framework the primary, and currently the only, binding legal constraint on governmental use of AI.

III. THE CONSTITUTIONAL FRAMEWORK: STATE ACTION AND AI SYSTEMS

A. Algorithmic Decision-Making as State Action

The threshold constitutional question is whether the deployment of an AI system by the state constitutes "state action" amenable to fundamental rights review under Part III of the Constitution. The answer turns on the definition of "State" in Article 12, which includes "the Government and Parliament of India and the Government and Legislature of each of the States and

[7]NITI Aayog, Responsible AI for All: Adopting the Framework \u2014 A Use Case Approach on Facial Recognition Technology (Government of India, 2021).

[8]European Parliament and Council, 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), [2024] OJ L 1689.

[9]Government of Canada, Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act (44th Parliament, 1st Session, 2022).

all local or other authorities within the territory of India or under the control of the Government of India."[10]

The Supreme Court has progressively expanded the concept of "State" under Article 12 to encompass bodies exercising public functions or enjoying governmental control, even where they are nominally private in character. In Ramana Dayaram Shetty v. International Airport Authority of India, the Court held that an entity substantially financed by the government and performing public duties would be an instrumentality of the State.[11]

In Ajay Hasia v. Khalid Mujib Sehravardi, the Court articulated a multi-factor test focusing on governmental control, public function, and financial dependency.[12]

In Pradeep Kumar Biswas v. Indian Institute of Chemical Biology, the Constitutional Bench further refined this doctrine.[13]

Applying this framework, an AI system deployed by a government department or a statutory authority to make or materially influence decisions affecting citizens' rights clearly constitutes state action. The algorithm does not possess independent legal personality; it acts as an instrument of the state entity that programmes, deploys, and relies upon it. The constitutional obligations of the state cannot be divested through technological intermediation any more than they can be divested through contractual delegation to private parties performing public functions. The state remains the constitutional actor; the algorithm is merely its mechanism of action.

More complex questions arise when private entities are involved. If a private corporation operates an AI system under contract with the government to perform a public function, such as welfare eligibility determination or digital identity verification, the question of whether that

[10]Constitution of India, 1950, Art. 12. The definition has been expansively interpreted: see Ramana Dayaram Shetty v. International Airport Authority of India, (1979) 3 SCC 489; Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722.

[11]Ramana Dayaram Shetty v. International Airport Authority of India, (1979) 3 SCC 489, para 14 (Bhagwati J.).

[12] Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722. The Court identified seven indicia of an \u2018instrumentality or agency\u2019 of the State, including deep and pervasive government control.

[13]Pradeep Kumar Biswas v. Indian Institute of Chemical Biology, (2002) 5 SCC 111 (Constitutional Bench). The Court held that the test is whether the body is \u2018financially, functionally and administratively\u2019 dominated by or under the control of the Government.

entity's AI-driven decisions constitute state action requires careful analysis under the Ajay Hasia criteria. The better view is that where the governmental character of the function is sufficiently strong, and where the private entity is operating within the framework of a governmental scheme with governmental authorisation and for governmental purposes, its AI-driven decisions should be treated as state action for the purposes of fundamental rights review.

B. Constitutional Review of Algorithmic Decisions

Once the character of an algorithmic decision as state action is established, the decision becomes amenable to judicial review on all available constitutional grounds. The Supreme Court, in Minerva Mills Ltd. v. Union of India and numerous subsequent decisions, has affirmed that fundamental rights are the core of the constitutional scheme and cannot be abridged by legislative or executive action that fails to satisfy the applicable constitutional standard. This principle applies with equal force to algorithmic action.[14]

The standard of review applicable to algorithmic state action raises its own complexities. Administrative law review under Article 226 and Article 32 traditionally examines whether an action is in accordance with law, whether it is reasonable, and whether it violates fundamental rights. Applying these standards to algorithmic decisions requires courts to grapple with technical questions of model design, training data composition, feature selection, and output interpretation that lie outside conventional judicial expertise. This has led some scholars to argue for specialised institutional mechanisms for algorithmic accountability, a proposal considered further in Part VI of this paper.

IV. FUNDAMENTAL RIGHTS AND ALGORITHMIC GOVERNANCE

A. The Right to Privacy and Personal Autonomy under Article 21

The most immediate fundamental rights implication of algorithmic governance concerns the right to privacy, now firmly established as a fundamental right under Article 21 of the Constitution following the landmark nine-judge constitutional bench decision in Justice K.S.

[14]Minerva Mills Ltd. v. Union of India, (1980) 3 SCC 625, para 77 (Chandrachud CJ.). The Court reaffirmed the supremacy of fundamental rights as the grundnorm of the constitutional order.

Puttaswamy (Retd.) v. Union of India. The Court, unanimously affirming the existence of a constitutional right to privacy, recognised that privacy protects individual autonomy, dignity, and the freedom to develop one's own personality and identity. The right to informational privacy — the right to control information about oneself — was identified as a core component of this constitutional guarantee.[15]

Algorithmic governance, by its very nature, involves the collection, aggregation, processing, and use of vast quantities of personal data. AI systems trained on historical data about individuals make predictions and determinations about those individuals' futures — their creditworthiness, their likelihood of recidivism, their risk of disease, their eligibility for welfare. The process of datafication through which individuals are reduced to statistical profiles for algorithmic processing implicates privacy not merely as an informational concern but as a matter of personal dignity and autonomy.[16]

The Puttaswamy Court established a three-part test for justifiable limitations on the right to privacy: the limitation must have a legal basis, must be proportionate to the objective sought, and must have procedural guarantees against abuse.[17]

Applying this test to algorithmic governance reveals significant constitutional tensions. Many algorithmic systems operate without explicit statutory authorisation, relying instead on broad executive discretion or existing administrative frameworks. The proportionality requirement demands that the privacy intrusion entailed by an AI system be no greater than necessary to achieve the governmental objective — a requirement that is difficult to satisfy in the absence of robust data minimisation, purpose limitation, and access control frameworks. The requirement of procedural guarantees is perhaps most challenging: algorithmic systems are typically not designed to generate

[15]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. All nine judges unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution.

[16]Ibid., para 645 (Chandrachud J., concurring). The right to informational self-determination was discussed at length in the context of Aadhaar\u2019s data collection regime.

[17]Ibid., para 179 (Chandrachud J.). The three-part test draws upon proportionality principles developed in German constitutional law and adopted in Indian jurisprudence through the privacy judgment.

intelligible explanations of their outputs, making meaningful individual challenge essentially impossible.

The concept of informational self-determination, developed most influentially in the German Constitutional Court's Census judgment of 1983 and incorporated into Indian constitutional doctrine through Puttaswamy, affirms that individuals must retain control over their personal data and must be able to participate meaningfully in decisions about how that data is used.[18]

Algorithmic governance, which processes personal data through opaque and often proprietary models to generate consequential determinations without individual knowledge or consent, represents a systematic challenge to informational self-determination at scale.[19]

B. Equality, Non-Discrimination, and Algorithmic Bias under Articles 14 and 15

Articles 14 and 15 of the Constitution guarantee equality before the law and non-discrimination on grounds of religion, race, caste, sex, or place of birth. These provisions impose both negative obligations (not to discriminate) and positive obligations (to treat equals equally) on the state. Algorithmic systems, particularly those trained on historical data reflecting patterns of human discrimination, pose serious threats to both dimensions of the constitutional equality guarantee.[20]

The problem of algorithmic bias is well-documented in international literature and increasingly evident in the Indian context. When an AI system is trained on historical data reflecting social patterns in which, for instance, individuals from lower-caste backgrounds, religious minorities, or women have faced systematic disadvantage in access to credit, employment, or government services, the algorithm may learn and perpetuate those discriminatory patterns. This phenomenon — sometimes described as "laundering" historical discrimination

---

[18]Bundesverfassungsgericht [BVerfG], Judgment of 15 December 1983, 65 BVerfGE 1 (Census Case). The German Constitutional Court recognised \u2018informational self-determination\u2019 (informationelle Selbstbestimmung) as a constitutionally protected right.

[19]Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, 2015) 3-8; Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019) 63-97.

[20] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St. Martin\u2019s Press, 2018); Cathy O\u2019Neil, Weapons of Math Destruction (Crown Publishers, 2016) 20-45.

through the veil of mathematical objectivity — represents a novel form of indirect discrimination that existing Article 15 doctrine is not well-equipped to address.

The Supreme Court's equality jurisprudence under Article 14 has developed the concept of "intelligible differentia" — the requirement that any classification by the state must be founded on an intelligible differentia that has a rational nexus with the object of the legislation or action.[21]

Algorithmic systems routinely create classifications based on correlations in training data that may be statistically robust but normatively arbitrary or constitutionally impermissible. A model that denies welfare benefits to individuals in certain geographic clusters may reflect correlation between geographic location and poverty without reflecting the actual need of individual applicants — a classification that may lack rational nexus with the welfare objective and may disproportionately affect constitutionally protected groups.

The doctrine of indirect discrimination, while not yet fully developed in Indian constitutional jurisprudence in the manner it has been in European Union law, is gaining traction in the Court's equality reasoning. In Anuj Garg v. Hotel Association of India, the Court recognised that ostensibly neutral classifications may produce discriminatory effects that attract constitutional scrutiny.[22]

This doctrine is highly relevant to algorithmic discrimination, which typically operates through facially neutral variables — geography, transaction history, social network characteristics — that serve as proxies for constitutionally protected characteristics.[23]

C. Freedom of Expression and Algorithmic Content Governance under Article 19(1)(a)

The right to freedom of expression under Article 19(1)(a) is implicated by algorithmic governance in two significant ways: first, through the use of algorithmic content moderation and

[21]Constitution of India, 1950, Art. 14. The \u2018intelligible differentia\u2019 test was classically stated in State of West Bengal v. Anwar Ali Sarkar, AIR 1952 SC 75.

[22]Anuj Garg v. Hotel Association of India, (2008) 3 SCC 1, para 37. The Court observed that laws perpetuating stereotypes or producing adverse effects on protected groups warrant heightened scrutiny.

[23]Tarunabh Khaitan, A Theory of Discrimination Law (Oxford University Press, 2015) 41-55, developing the concept of \u2018abductive\u2019 and \u2018adductive\u2019 grounds of discrimination.

takedown mechanisms by intermediaries operating under governmental direction; and second, through the chilling effect produced by pervasive algorithmic surveillance on individuals' willingness to exercise their expressive freedom.

The Supreme Court's decision in Shreya Singhal v. Union of India, which struck down Section 66A of the Information Technology Act as an unconstitutional restriction on freedom of expression, established important principles regarding the constitutional limits on state regulation of online speech.[24]

The Court held that restrictions on free expression must be confined to the grounds specified in Article 19(2) — sovereignty, security, public order, decency, and the like — and must be narrowly tailored to those grounds. Vague and overbroad restrictions, the Court held, produce a chilling effect on constitutionally protected speech that is itself a constitutional harm.[25]

Algorithmic content moderation, which is increasingly used by social media intermediaries pursuant to governmental directions and intermediary liability frameworks, poses a serious challenge to these principles.[26]

Content moderation algorithms are typically trained to identify and remove content falling within certain categories, but the accuracy of such categorisation is inevitably imperfect. The systematic over-removal of speech — particularly political speech, minority cultural expression, and criticism of governmental authority — constitutes a constitutionally significant suppression of expression that cannot be justified merely by reference to the efficiency of automated processing.

The chilling effect dimension is equally important. When individuals are aware that their digital communications, online behaviour, and public movements are subject to pervasive algorithmic surveillance by the state, the knowledge of that surveillance — even in the absence of actual enforcement action — operates to suppress constitutionally protected behaviour. The

---

[24]Shreya Singhal v. Union of India, (2015) 5 SCC 1, para 94. The Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutional.

[25] Ibid., para 16-19. The Court distinguished between \u2018discussion\u2019, \u2018advocacy\u2019, and \u2018incitement\u2019, confining permissible restrictions under Article 19(2) to the last category.

[26]Chinmayi Arun, \u2018On Weaponising Intermediaries\u2019 (2019) 32 Harvard Human Rights Journal 1. See also Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4.

Supreme Court recognised the significance of chilling effects in Shreya Singhal and in the privacy jurisprudence of Puttaswamy.[27]

A constitutional doctrine of algorithmic governance must take seriously the structural chilling effects produced by state AI surveillance systems.

D. Due Process, Natural Justice, and the Right to be Heard

Beyond the substantive fundamental rights, algorithmic governance implicates fundamental principles of procedural fairness that flow from Article 21 and from the constitutional principles of natural justice. The right to be heard — audi alteram partem — the right to a reasoned decision, and the right to know the case against oneself are foundational elements of due process that cannot be vacated by the automaticity of algorithmic determination.[28]

The Supreme Court has consistently held that any order adversely affecting a person's rights must be preceded by adequate notice and an opportunity to be heard, and must be accompanied by reasons. In Union of India v. Tulsiram Patel and A.K. Kraipak v. Union of India, the Court affirmed that the principles of natural justice are deeply embedded in the constitutional guarantee of procedural due process under Article 21. These requirements are not merely formal technicalities; they are expressions of the fundamental constitutional commitment to treating individuals as subjects with dignity rather than objects of administrative power.

Algorithmic decision-making structurally undermines these procedural guarantees. An AI system that denies a welfare application, flags a tax return for scrutiny, or assigns a high-risk score to an individual in a predictive policing system typically does not generate a reasoned decision in any meaningful sense. The output of the algorithm — a score, a binary classification, a recommendation — reflects a mathematical transformation of input variables according to model parameters learned from historical data. The individual affected by such a determination cannot

[27]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, para 301 (Chandrachud J.). The chilling effect on privacy was analysed as a constitutional harm independent of any concrete adverse action.

[28]Union of India v. Tulsiram Patel, (1985) 3 SCC 398; A.K. Kraipak v. Union of India, (1969) 2 SCC 262. The principles of natural justice \u2014 audi alteram partem and nemo judex in causa sua \u2014 are constitutionally mandated under Art. 21.

effectively challenge it without understanding which inputs drove the output, which model was applied, and how the system was trained and validated.

This "explainability gap" creates a profound due process problem. The right to effective contestation of adverse decisions — what some scholars have termed the right to an explanation — is not merely a matter of administrative convenience; it is a constitutional imperative flowing from the dignity and autonomy of the individual.[29]

The German Federal Administrative Court's recognition of a right to explanation for automated administrative decisions, and the analogous provision in Article 22 of the European Union's General Data Protection Regulation, reflect constitutional and quasi-constitutional values that are deeply consonant with the Indian constitutional tradition.[30]

V. LIMITATIONS OF CURRENT DOCTRINE AND THE NEED FOR RECONCEPTUALISATION

A. The Inadequacy of Existing Frameworks

The constitutional challenges of algorithmic governance cannot be adequately met through the uncritical application of existing doctrinal frameworks developed in the context of human administrative action. Three structural inadequacies deserve particular attention.[31]

First, the doctrine of proportionality, while theoretically capable of subjecting algorithmic action to rigorous scrutiny, presupposes a degree of transparency about the means employed by the state that algorithmic systems characteristically deny. A court cannot meaningfully evaluate

[29]Mireille Hildebrandt, Smart Technologies and the End(s) of Law (Edward Elgar Publishing, 2015) 169-175. See also Sandra Wachter, Brent Mittelstadt & Luciano Floridi, \u2018Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation\u2019 (2017) 7(2) International Data Privacy Law 76.

[30]General Data Protection Regulation (EU) 2016/679, [2016] OJ L 119/1, Art. 22. Article 22 provides a right not to be subject to solely automated decisions producing significant legal effects and a right to obtain human review.

[31]Antoinette Rouvroy & Thomas Berns, \u2018Algorithmic Governmentality and Prospects of Emancipation\u2019 (2013) 177 R\u00e9seaux 163. The authors argue that algorithmic governance replaces normative regulation with statistical prediction, rendering subjects ungovernable in the classical sense.

whether an AI-driven decision is the least restrictive means of achieving a governmental objective if the workings of the algorithm — its training data, its feature weights, its error rates across demographic groups — are not disclosed. Proportionality review without algorithmic transparency is an empty exercise.

Second, the existing framework for discrimination analysis under Articles 14 and 15 focuses primarily on the intent and explicit classification criteria of the state actor. The shift to algorithmic determination of state classification creates a situation in which discriminatory outcomes may be produced without discriminatory intent and without explicit reliance on protected characteristics. The constitutional doctrine of indirect discrimination, while nascent in Indian jurisprudence, must be developed with sufficient depth to capture the full range of algorithmic discrimination effects.[32]

Third, the judicial review framework, while formally applicable to algorithmic state action, faces serious practical constraints. Courts are not institutionally equipped to audit complex machine learning models, evaluate training data composition, or assess statistical fairness metrics. The risk of deferring excessively to executive and technical expertise — what might be called algorithmic deference — is real, and it threatens to hollow out constitutional review of state AI action.

B. Toward an Algorithmically Aware Constitutional Jurisprudence

Reconstituting constitutional protections for the age of AI requires both doctrinal innovation and institutional creativity. At the doctrinal level, the Court must develop an algorithmically aware jurisprudence that: (i) establishes that the state's constitutional obligations apply fully to algorithmic action; (ii) requires disclosure of algorithmic systems used in consequential governmental decisions as a prerequisite for effective judicial review; (iii) develops the doctrine of indirect discrimination to encompass algorithmic bias; (iv) recognises a constitutional right to explanation for AI-driven adverse decisions; and (v) applies the chilling effect doctrine robustly to algorithmic surveillance.

[32]Kate Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence (Yale University Press, 2021) 211-224.

At the institutional level, consideration should be given to the establishment of specialised algorithmic accountability mechanisms — an independent AI Audit Commission with technical expertise to review high-risk government AI systems, powers to compel disclosure, and authority to recommend remediation. Such a body, operating under legislative mandate and subject to constitutional review, could bridge the technical and legal dimensions of algorithmic accountability that courts alone are not positioned to address.

VI. A FRAMEWORK FOR CONSTITUTIONAL AI GOVERNANCE IN INDIA

A. Core Principles

The paper proposes a framework for constitutional AI governance in India grounded in five core principles: constitutional conformity, transparency, explainability, accountability, and democratic oversight.

The principle of constitutional conformity requires that no AI system may be deployed in any governmental function that affects fundamental rights unless it has been subjected to prior constitutional impact assessment confirming that its design and operation are consistent with the requirements of Part III of the Constitution. This principle places the burden of demonstrating constitutional compliance on the state, not the individual.

The principle of transparency requires that the state disclose the existence, purpose, and general methodology of any AI system used in consequential governmental decisions. It demands, at minimum, a public register of AI systems in use, their intended purposes, the categories of data they process, and the accountability arrangements in place.

The principle of explainability requires that any AI-driven decision adversely affecting an individual's rights must be accompanied by an intelligible explanation of the primary factors contributing to the decision and the manner in which they were weighted. This principle directly addresses the due process concerns identified in Part IV(D).

The principle of accountability requires the designation of a responsible human official for every AI-driven governmental decision, who bears legal responsibility for the decision and can be

subjected to administrative and judicial scrutiny. Algorithmic systems cannot themselves be held accountable; accountability must be anchored in human actors within the constitutional system.

The principle of democratic oversight requires that high-risk AI systems in the public sector be subject to parliamentary oversight through mandatory reporting requirements and periodic review by an appropriately constituted committee with technical advisory support.

B. Legislative Recommendations

This framework calls for the enactment of a dedicated AI Governance and Regulation Act, the principal features of which should include: a risk-based classification of AI systems by reference to the potential severity of their impact on fundamental rights; a prohibition on certain categories of AI use that are incompatible with constitutional values, including real-time mass biometric surveillance in public spaces and AI-driven social scoring systems; mandatory conformity assessments for high-risk AI in the public sector; a statutory right to explanation and contestation of AI-driven decisions affecting individual rights; establishment of an independent AI Regulatory Authority with powers of investigation, audit, and enforcement; and civil and administrative liability frameworks for constitutional violations occasioned by AI systems.

The DPDPA 2023, while representing a significant step in the regulation of personal data, does not address these concerns comprehensively. Its provisions on automated decision-making are limited and do not establish a meaningful right to contestation or a framework for algorithmic accountability in the public sector. Supplementary legislation anchored explicitly in fundamental rights principles is essential.[33]

C. Judicial Remedies

In the absence of comprehensive legislation, the courts retain their constitutional responsibility to enforce fundamental rights against algorithmic state action. Several doctrinal tools are available. Mandatory disclosure orders under Articles 32 and 226 can require the state to reveal the AI systems it employs and the data it uses. Proportionality review can be deployed to strike down AI systems that intrude on fundamental rights without adequate justification. The writ of mandamus can compel the state to provide explanations for AI-driven decisions. Structural

[33]Constitution of India, 1950, Art. 142. This provision empowers the Supreme Court to make such order as is necessary for doing complete justice in any cause or matter pending before it.

injunctions can require the state to reform AI systems found to produce unconstitutionally discriminatory outcomes.

The Supreme Court's exercise of its broad curative jurisdiction under Article 142, read with its supervisory role over the constitutional system, may in appropriate cases extend to the issuance of directions establishing minimum standards for AI governance pending legislative action.[34]

The Court's practice of issuing guidelines pending legislation, illustrated in Vishakha v. State of Rajasthan, provides a relevant precedent.[35]

VII. CONCLUSION

Artificial intelligence is not a neutral technological force that the Constitution can afford to ignore. It is a system of power — a mechanism through which the state acts upon citizens, makes determinations about their lives, and allocates rights and resources. When the state acts through algorithms, it remains constitutionally responsible for those actions, and citizens retain their full complement of fundamental rights against algorithmic state power.

The constitutional framework of India, developed through decades of progressive judicial interpretation, contains the normative resources necessary to meet this challenge. The right to privacy under Article 21, the equality guarantee under Articles 14 and 15, the freedom of expression under Article 19(1)(a), and the procedural protections of natural justice and due process collectively provide a robust constitutional framework for the governance of AI. What is required is the intellectual willingness to apply these principles to the novel conditions of algorithmic governance, and the institutional creativity to develop enforcement mechanisms adequate to the technical complexity of AI systems.

---

[34]Vishakha v. State of Rajasthan, (1997) 6 SCC 241. The Supreme Court issued comprehensive guidelines on sexual harassment at the workplace pending legislation, invoking its jurisdiction under Art. 32 read with Art. 142.

[35]Digital Personal Data Protection Act, 2023, No. 22 of 2023. Section 16 provides a limited right to seek grievance redressal from data fiduciaries but does not establish a full right to explanation for automated decisions. See Rahul Matthan, \u2018The Exceptionalism of Data Privacy Law\u2019 (2022) National Law School of India Review 34.

The stakes of inaction are high. A constitutional democracy that permits the state to exercise arbitrary, opaque, and discriminatory power over citizens through algorithmic intermediation, while maintaining the formal apparatus of rights protection, risks becoming a constitutional democracy in name only. The challenge of algorithmic governance is, at its core, the challenge of ensuring that the transformative promise of the Constitution remains real and effective in a technologically transformed world.

This paper has argued that meeting this challenge requires doctrinal innovation in constitutional jurisprudence, legislative action to create a comprehensive AI governance framework, and institutional reform to create accountability mechanisms adequate to the technical character of AI systems. Each of these dimensions demands sustained scholarly, judicial, and legislative attention. The future of constitutional democracy in India may well depend on the quality of the legal response to the challenge of algorithmic governance.

REFERENCES

A. Cases

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

2. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1.

3. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

4. Minerva Mills Ltd. v. Union of India, (1980) 3 SCC 625.

5. Ramana Dayaram Shetty v. International Airport Authority of India, (1979) 3 SCC 489.

6. Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722.

7. Pradeep Kumar Biswas v. Indian Institute of Chemical Biology, (2002) 5 SCC 111.

8. Anuj Garg v. Hotel Association of India, (2008) 3 SCC 1.

9. Union of India v. Tulsiram Patel, (1985) 3 SCC 398.

10. A.K. Kraipak v. Union of India, (1969) 2 SCC 262.

11. Vishakha v. State of Rajasthan, (1997) 6 SCC 241.

B. Legislation

12. Constitution of India, 1950.

13. Information Technology Act, 2000, No. 21 of 2000.

14. Digital Personal Data Protection Act, 2023, No. 22 of 2023.

15. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18 of 2016.

16. European Parliament and Council, Artificial Intelligence Act (EU) 2024/1689, [2024] OJ L 1689.

17. General Data Protection Regulation (EU) 2016/679, [2016] OJ L 119/1.

C. Secondary Sources

18. Sudhir Krishnaswamy, Democracy and Constitutionalism in India: A Study of the Basic Structure Doctrine (Oxford University Press, 2009).

19. Tarunabh Khaitan, A Theory of Discrimination Law (Oxford University Press, 2015).

20. Nick Couldry & Ulises A. Mejias, The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism (Stanford University Press, 2019).

21. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, 2015).

22. Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St. Martin's Press, 2018).

23. Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (Crown Publishers, 2016).

24. Kate Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence (Yale University Press, 2021).

25. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs, 2019).

26. Justice B.N. Srikrishna (Chair), A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018).

27. NITI Aayog, Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology (Government of India, 2021).

28. Vrinda Bhandari & Faiza Rahman, 'Understanding Automated Decision Making in India: A Primer' (2020) 15 Indian Journal of Law and Technology 1.

29. Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(35) Economic and Political Weekly 10.

30. Chinmayi Arun, 'On Weaponising Intermediaries' (2019) 32 Harvard Human Rights Journal 1.

31. Rahul Matthan, 'The Exceptionalism of Data Privacy Law' (2022) National Law School of India Review 34.

32. Mireille Hildebrandt, Smart Technologies and the End(s) of Law (Edward Elgar Publishing, 2015).

33. Antoinette Rouvroy & Thomas Berns, 'Algorithmic Governmentality and Prospects of Emancipation' (2013) 177 Réseaux 163.

34. Sandra Wachter, Brent Mittelstadt & Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76.