
ALGORITHMIC EXECUTIVE POWER AND CONSTITUTIONAL GOVERNANCE IN INDIA: DUE PROCESS, EQUALITY AND JUDICIAL REVIEW IN AUTOMATED WELFARE ADMINISTRATION

Shanjida Israt Jahan Efat, Assistant Professor,
Department of Law, Notre Dame University Bangladesh.¹

ABSTRACT

This essay examines what constitutional governance looks like when executive actions are performed, mediated or rationalised by algorithmic algorithms. It starts from the proposition that automated welfare administration should not be just a question of efficiency of claims, or data privacy considerations. The Constitution of India's Articles 14 and 21 would be at stake. An individual excluded on the basis of an arbitrary biometric failure, risk score or opaque eligibility rule suffers not just a service delivery error but a deprivation that is *prima facie* arbitrary, discriminatory and procedurally unfair. This article presents a model of algorithmic due process, drawing on Indian constitutional doctrine and on international developments in the European Union, Canada, the United Kingdom, Netherlands and the United States. It proposes additional statutory duties of disclosure, impact assessments, human review, reasoned decisions, auditable records, and calibrated judicial review. What this article concludes, in other words, is that the digital State requires constitutional governance with limits on technology, and that tech companies should not be treated merely as things over which administrative deference, wilful or not, applies when harm actually occurs (which it does), and impossibility of regulation becomes equally real.

Keywords: Accountability, Algorithmic governance, Due process; Digital welfare; Judicial review.

¹ Assistant Professor, Department of Law, Notre Dame University Bangladesh.

I. INTRODUCTION

Constitutional governance in the twenty-first century is increasingly tested not only by emergency powers, weak institutions or partisan constitutionalism, but also by ordinary administrative systems that determine access to food, pensions, housing, education, identity and mobility. The modern executive does not always act through a visible officer sitting behind a counter. It acts through databases, scoring systems, biometric authentication, fraud-detection rules, eligibility engines and automated notices. These systems may appear technical, yet they perform constitutional work. They decide who is recognised by the State, who is trusted, who must prove entitlement again, and who is silently pushed out of a scheme. For that reason, algorithmic administration must be brought within the vocabulary of rule of law, equality, dignity, natural justice and judicial review.²

The problem is not that public administration uses technology. A constitutional State may legitimately use digital tools to reduce leakage, improve targeting and coordinate large programmes. The constitutional difficulty begins when automation is used in a way that displaces accountable judgment, hides reasons, transfers the burden of system failure to citizens, or makes welfare conditional on a form of machine-readable identity that some persons cannot produce. A pensioner whose fingerprint fails, a ration-card holder removed from a database, or a worker classified as fraudulent by an automated system encounters the State at its most concrete level. If the law has no answer until a writ petition is filed, constitutional governance has already failed at the point where it mattered most.³

There are resources in Indian constitutional law to tackle this issue. Article 14 has shifted from classifying the state as a mere cause of action to condemning State arbitrariness. In this, Article 21 has evolved from a provision against physical restraint to one that requires fairness, reasonableness and dignity in any State action which encroaches upon life and liberty. Judicial review under Articles 32 and 226 is not a ceremonial remedy; it forms a systemic protection against excesses by the executive. Another lesson of the basic structure doctrine is that the Constitution goes beyond institutional labels. Limited government, rule of law, and judicial review are constitutional commitments that must travel with power wherever power operates.⁴

² The Constitution of India, arts. 14, 21, 32 & 226.

³ *Kesavananda Bharati v. State of Kerala*, (1973) 4 S.C.C. 225 (India).

⁴ *Minerva Mills Ltd. v. Union of India*, (1980) 3 S.C.C. 625 (India).

However, existing doctrine does not provide an automatic fix to algorithmic exclusion. Traditional administrative law presumes a human officer has weighed in facts, applied law and issued some form of order. Algorithmic systems complicate that assumption. They can be purchased from vendors, trained on bad data, modified without public notice or baked into software that local officials cannot even explain. And when that happens, those affected might be told only that the system has deemed them a winner or a loser. The distinction between a legal rule and a technical parameter becomes unclear. The official who signs the rejection may not know how the result was generated. In such a setting, the familiar demand for reasons is at risk of becoming ritualistic.⁵

This article therefore asks how Indian constitutional governance should discipline algorithmic executive power, especially in welfare administration. The article deliberately focuses on welfare because constitutional harm is most acute where digital exclusion intersects with poverty, disability, age, caste, gender and rural deprivation. It does not suggest that all automated systems are unconstitutional. It argues instead that systems affecting welfare entitlements must be designed, authorised and reviewed as exercises of public power. Efficiency is relevant, but it cannot become a constitutional alibi. A system that saves money by wrongly denying entitlements is not efficient in a constitutional sense; it merely externalises administrative error onto citizens least able to absorb it.⁶

Why is this topic also important; welfare automation is seldom a unique event. An identity number was linked, verified biometrically, correction of spelling problems were dealt with, proof of residence required and grievances pursued through yet another digital pathway. Everything is slightly defensible individually. What approaches number two route to the constitutional problem is by way of that cumulative burden. The abstraction of administrative data poses the challenge that a rights-based analysis will not look at this single database, this one authentication device or one rejection notice.

The article defines the expression 'algorithmic executive power' rather generously. It includes machine-learning models, rule-based systems, biometric matching, database deduplication, automated eligibility checks and the use of risk-scoring tools when they assist or decide public decisions. This broad usage is deliberate. The distinction between systems which are

⁵ E.P. Royappa v. State of Tamil Nadu, (1974) 4 S.C.C. 3 (India).

⁶ Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).

technically artificial intelligence and those that are not should be unimportant for constitutional law. If a citizen can feel both the denial of a public benefit and its rationalization being excised by an opaque computational process that she is unable to comprehend or counter, it matters little whether she sees that as a form of harm.

II. LITERATURE REVIEW

The literature on constitutionalism and technology may be grouped into four broad strands. The first concerns Indian constitutional doctrine on equality, due process and reasoned administration. Indian courts have repeatedly expanded Article 14 from a narrow classification test into a guarantee against arbitrariness. The cases from *E.P. Royappa* to *Shayara Bano* show that equality is offended not only by explicit discrimination but also by irrational and capricious State action. This is important for algorithmic governance because automated systems often harm through apparently neutral rules rather than openly discriminatory classifications.⁷

The second line of argumentation pertains to Article 21 and procedural fairness. Liberty was tied to a procedure that is fair, just and reasonable *Maneka Gandhi*. Subsequent decisions arising from the right to life and privacy, in *Inter-American Court of Human Rights v.* When it comes to privacy, in particular, secrecy is only a thing of the past. This encompasses informative self-determination, social dignity, autonomy and protection against arbitrary State profiling. Algorithmic welfare systems that sift, link and process personal data for eligibility directly implicate these values.⁸

The final component originates from administrative law. Natural justice, the requirement to give reasons and the rule prohibiting after-the-fact justification are not mere technical niceties. They create the citizen-State relationship structures. Fairness included administrative action as well; so broadening fairness was the impact of *A.K. Kraipak* and *Swadeshi Cotton Mills: Mohinder Singh Gill* and *Kranti Associates* demanding 'tell me why', (the old *I.A. Rao* para, because the reasons given must be reason for decision). These principles become less, not more, important when a decision is software generated. However, if the State cannot offer an explanation as to why a person was excluded then this decision is not capable of being

⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India) [hereinafter *Aadhaar Judgment*].

meaningfully challenged.⁹

The fourth strand is work on algorithmic accountability, an area of increasing literature. Citron's research on technological due process continues to be at the center of these debates because it reveals how automated public systems can consistently produce systemic errors while masquerading as neutral. Pasquale's black box story, Barocas and Selbst's disparate impact decision and Selbst's critique of abstraction provide analytic reasons why bias is not solved simply by stripping explicit identity markers. Data analytics can create and reproduce social inequality through proxies, missing data, and design choices as well as feedback loops. These insights are critical for Indian public law, with administrative databases usually reinforcing existing exclusions.¹⁰

Practical models have been created in the field of comparative law. Consider, for example, the EU's planned Artificial Intelligence Act, which classifies some AI systems used in the public sector as high-risk, such as those that grant access to key services and public benefits. For example, the General Data Protection Regulation includes explicit protections for individual automated decisions with legal or similarly substantial significance. The Canadian Directive on Automated Decision-Making requires algorithmic impact evaluations, notice, human intervention and quality assurance for federal automated systems. The Council of Europe Framework Convention is tied to AI governance with strong human rights, democracy and rule of law aspects. These are not mechanical transplant equipment, but they indicate that democratic systems go from abstract ethics to enforced institutional protections.¹¹

Judicial opinions in other jurisdictions are equally educational. Last week, the Dutch SyRI judgment annulled a welfare-fraud risk system for lack of adequate transparency and safeguards in violation of the right to privacy. Bridges had discovered a legal framework with serious flaws in the law surrounding live facial recognition, the Court of Appeal ruled. In *State v. An Illustration of the social cost incurred when errors in automated fraud detection scale, which such systematic errors would do through public authority; MiDAS: A Federal Policy on Automated Fraud Detection* abarousa ago - Lawfare Altogether then, these examples show that algorithmic governance is a real law and human jeopardy not a hypothetical future threat.¹²

⁹ *State of W. Bengal v. Anwar Ali Sarkar*, 1952 S.C.R. 284 (India).

¹⁰ *Ajay Hasia v. Khalid Mujib Sehravardi*, (1981) 1 S.C.C. 722 (India).

¹¹ *Shayara Bano v. Union of India*, (2017) 9 S.C.C. 1 (India).

¹² *A.K. Kraipak v. Union of India*, (1969) 2 S.C.C. 262 (India).

Indian writing on Aadhaar and welfare automation provides the closest domestic setting. Scholars have documented biometric authentication failures, portability concerns, exclusion from ration systems and the difficulties of fallback mechanisms. The Aadhaar judgment upheld use of Aadhaar for welfare in principle, but it also recognised the constitutional significance of exclusion and the need for safeguards. The unresolved question is how courts, legislatures and administrators should operationalise that recognition when the State deploys newer AI and data systems beyond Aadhaar.¹³

A further theme in the literature is the distinction between accuracy and legality. Engineers often evaluate a system by accuracy, precision, recall or error rates. Public law must ask additional questions. Who is included in the test population? What happens to the false negatives? How quickly can errors be corrected? Does the system create incentives for officials to deny claims mechanically? A system may be statistically acceptable for a commercial recommendation engine and still be constitutionally unacceptable for ration distribution or pension suspension.

The literature goes on to caution against the framing of transparency as one universal value. Source code disclosures, model cards, public notices, individual rationale and audit reports each target distinct audiences. Citizens want practical reasons and the solution. A court needs adequate records for review. A regulator requires technical documentation. Purpose and scale and safeguards are what the public needs. Thus, constitutional governance must therefore embrace transparency rather than the outright demand for full public openness or total secrecy.

A further thing that comes in handy is a reminder: algorithmic systems are socio-technical. They do not determine constitutional effects simply by virtue of the code they write but rather as that code interacts with field officials, local infrastructure, language logics, documentation practices, and social hierarchy. A good system will not work in areas with poor connectivity or where officials treat output from machines as gospel. On the other hand, if there is a strong human defense in place then even for crude systems the risk may decrease. Hence, beyond technical models of banking, the governance of institutions and populations referring to regulation regarding incentives and remedies must form another layer in your training.

¹³ *Swadeshi Cotton Mills v. Union of India*, (1981) 1 S.C.C. 664 (India).

III. RESEARCH GAP

The literature that currently exists has made some important contributions to privacy, data protection, digital identity and algorithmic bias. However, three gaps remain. To begin with, Indian constitutional analysis frequently discusses algorithmic governance only in terms of privacy. You need privacy, and yet privacy is not enough. A welfare-programme citizen denied of access to the programme may need data protection yes but so too needs equal treatment, notice, reasons, a hearing, urgent restoration and court-enforceable remedies. A privacy-only approach may miss the public-law character of the deprivation.¹⁴

Second, scholarship has not sufficiently connected algorithmic administration with separation of powers. When a technical system silently changes eligibility, prioritises cases, flags suspected fraud or determines verification thresholds, it may effectively modify legal entitlements without legislative debate or reasoned executive rule-making. The problem is not merely opacity. It is that law-making, fact-finding and enforcement may collapse into a software environment that neither the legislature nor the court can easily inspect.¹⁵

Third, Indian doctrine lacks a structured standard for judicial review of algorithmic decisions. Courts may either defer to technology because it appears expert, or strike down systems without a workable method for distinguishing permissible automation from unconstitutional automation. What is needed is an intermediate approach: courts should ask whether the system has legal authority, a rights-sensitive design, auditable records, reasoned outputs, human review and remedies proportionate to the harm. This article seeks to develop that approach.¹⁶

A related gap concerns constitutional remedies. Much writing identifies algorithmic bias or opacity, but fewer accounts explain what a court should order after finding a defect. In welfare administration, retrospective declaration is often inadequate. A beneficiary needs food, pension or medical access immediately. The remedial frame must therefore include interim continuation, local correction camps, time-bound appeals and monitoring of compliance. Without such remedies, constitutional review may arrive too late to protect the right in practice.

There is also a gap between elite digital-policy discourse and local administrative reality.

¹⁴ Mohinder Singh Gill v. Chief Election Comm'r, (1978) 1 S.C.C. 405 (India).

¹⁵ Kranti Assocs. (P) Ltd. v. Masood Ahmed Khan, (2010) 9 S.C.C. 496 (India).

¹⁶ Olga Tellis v. Bombay Mun. Corp., (1985) 3 S.C.C. 545 (India).

Policy documents often speak of trustworthy AI, innovation and responsible deployment. Local beneficiaries encounter queues, devices, network failures, spelling mismatches and officials who disclaim responsibility by saying that 'the system' has rejected the claim. A publishable constitutional account must connect these two levels. The question is not whether India should use technology. It is how constitutional responsibility should travel through the technological and administrative layers that deliver State power.

IV. RESEARCH QUESTIONS AND OBJECTIVES

This article addresses three research questions. First, how can Articles 14 and 21 of the Indian Constitution be applied to automated welfare decisions without reducing constitutional review to either technical audit or abstract privacy rhetoric? Secondly, what institutional safeguards are necessary to preserve accountability and separation of powers when the executive deploys algorithmic systems in public administration? Thirdly, how should courts review opaque or complex algorithmic systems while respecting legitimate administrative expertise and confidentiality?¹⁷

The objectives follow from these questions. The first objective is doctrinal: to identify the constitutional principles that apply to algorithmic welfare decisions. The second objective is institutional: to propose safeguards for public bodies before, during and after deployment of automated systems. The third objective is remedial: to offer a model of judicial review that is capable of examining algorithmic power without requiring judges to become engineers. The article's central claim is that algorithmic due process should become a constitutional minimum for automated welfare administration.¹⁸

V. METHODOLOGY

The article uses doctrinal and comparative legal methodology. The doctrinal component examines Indian constitutional provisions, Supreme Court decisions, statutes and policy documents concerning equality, due process, privacy, administrative fairness, public accountability and digital governance. It treats automated welfare administration as an exercise of State power, not merely as a question of technological design.¹⁹

¹⁷ People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).

¹⁸ Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

¹⁹ Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).

The comparative component is selective rather than exhaustive. The European Union, Canada, the Netherlands, the United Kingdom and the United States are used because each has confronted a different aspect of algorithmic public administration: risk classification, automated decision rights, impact assessment, welfare-fraud scoring, biometric surveillance and criminal risk assessment. These jurisdictions are not offered as models to be copied. They are used to identify institutional techniques that may help Indian law give practical effect to constitutional principles.²⁰

The article is normative as well as descriptive. It does not conduct empirical fieldwork, although it relies on published studies of welfare digitisation and biometric authentication. Its purpose is to develop a constitutional framework capable of guiding legislators, administrators and courts. The recommended framework is evaluated against three criteria: fidelity to Indian constitutional doctrine, feasibility within public administration, and capacity to protect vulnerable persons before harm becomes irreversible.²¹

The article does not attempt to measure the national scale of algorithmic exclusion. Such a task would require government datasets that are not consistently public and fieldwork beyond the scope of this study. Instead, the article proceeds on a constitutional assumption: even if exclusion affects a small percentage of beneficiaries, the absolute number may be large in national welfare schemes, and the seriousness of deprivation may justify strict safeguards. Constitutional review is not triggered only by statistical majorities; it is also concerned with vulnerable minorities exposed to avoidable harm.

The comparative material is used with caution. The EU AI Act, GDPR, Canadian Directive and foreign case law operate within different institutional cultures. Their value lies in showing that public algorithms can be subjected to documentation, impact assessment, human oversight and review without preventing digital administration. The Indian framework proposed here is therefore not a transplant. It is an attempt to translate comparative techniques into the grammar of Indian constitutional law.

VI. ARTICLES 14 AND 21 IN AUTOMATED WELFARE DECISIONS

Article 14 is the natural starting point because algorithmic administration often presents itself

²⁰ Vineet Narain v. Union of India, (1998) 1 S.C.C. 226 (India).

²¹ S.P. Gupta v. Union of India, 1981 Supp. S.C.C. 87 (India).

as neutral. The system does not say that it treats persons differently on caste, gender, disability or class. It says only that a fingerprint did not match, that a record is inconsistent, that a risk score is high, or that a data field is incomplete. Formal neutrality, however, is not constitutional innocence. Indian equality law condemns arbitrary State action. If a system excludes persons for reasons unrelated to the lawful purpose of the scheme, or if it imposes burdens that certain groups are predictably less able to meet, Article 14 is engaged.²²

The anti-arbitrariness doctrine is especially useful because many algorithmic harms arise from design choices that are not visible as traditional discrimination. A biometric authentication requirement may impose disproportionate burdens on manual workers, elderly persons or persons with disabilities. A database-matching rule may penalise migrants whose addresses and documents change frequently. A fraud-detection model may target areas associated with poverty. The constitutional question should not be whether the software had discriminatory intent. It should be whether the system creates unjustified and unreasonable burdens in the enjoyment of legal entitlements.²³

Article 21 adds a second layer. Welfare administration often concerns the material conditions of life. Where food, pension, healthcare or housing is at stake, denial of access may threaten dignity, bodily integrity and livelihood. Indian courts have already recognised that life under Article 21 means more than animal existence. A State cannot answer a livelihood deprivation by saying that the decision was produced by a database. The more essential the benefit, the stronger the procedural safeguards must be.²⁴

The privacy judgment in Puttaswamy provides a bridge between data governance and constitutional due process. It recognises privacy as intrinsic to liberty and dignity, while also accepting that State action may restrict privacy if it satisfies legality, legitimate aim, proportionality and procedural safeguards. Algorithmic welfare systems often involve large-scale data collection and processing. The legality requirement means that the system must have clear statutory or rule-based authority. The legitimate aim requirement prevents vague reliance on efficiency. The proportionality requirement asks whether less restrictive alternatives are

²² Supreme Court Advocates-on-Record Ass'n v. Union of India, (2016) 5 S.C.C. 1 (India).

²³ Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code (2016), sec. 7.

²⁴ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

available. Procedural safeguards require notice, reasons, correction, review and remedies.²⁵

The Aadhaar judgment illustrates both the promise and limits of this approach. The majority upheld Aadhaar for welfare-linked subsidies, but the judgment did not give the executive a blank cheque. It was concerned with exclusion, data protection, purpose limitation and the need for alternative mechanisms. Justice Chandrachud's dissent placed even greater emphasis on constitutional identity, surveillance risk and the danger of making rights conditional on technological infrastructure. For present purposes, both the majority and dissent support a modest proposition: welfare technology must be judged by its effects on constitutional access, not merely by its administrative design.²⁶

A meaningful Article 21 procedure in automated welfare decisions should include at least five elements. First, the person must be informed that an automated or algorithmically assisted system has been used. Secondly, the person must receive intelligible reasons, including the material data points or rule triggers that affected the result. Thirdly, there must be an accessible method to correct inaccurate data. Fourthly, a trained human officer must have authority to override the system where constitutional harm is likely. Fifthly, interim relief must be available where denial of the benefit threatens subsistence.²⁷

This does not require the State to disclose every line of source code in every case. The Constitution does not demand technological theatre. It demands contestability. A person must be able to understand the case against her in practical terms and must be able to correct it before the deprivation becomes final. Where the State relies on trade secrecy or security, courts may use sealed technical review, expert commissioners or public summaries. But a total refusal to explain cannot be reconciled with Articles 14 and 21.²⁸

The most important shift is to treat system design as part of procedure. Traditional natural justice focuses on the moment of decision. Algorithmic systems require attention to earlier stages: data collection, training data, variables, thresholds, error rates, exception handling and update governance. If these stages are defective, a later hearing may not cure the constitutional

²⁵ Digital Personal Data Protection Rules, 2025, G.S.R. 843(E), Gazette of India, Extraordinary, Part II, sec. 3(i) (Nov. 13, 2025).

²⁶ Information Technology Act, No. 21 of 2000, India Code (2000).

²⁷ NITI Aayog, National Strategy for Artificial Intelligence #AIForAll 85-89 (2018).

²⁸ NITI Aayog, Responsible AI for All: Approach Document for India, Part 1: Principles for Responsible AI 7-18 (2021).

wrong. A hearing before an officer who cannot change the algorithm is not meaningful. Therefore, algorithmic due process must include both individual remedies and system-level duties.²⁹

A difficulty arises because many automated systems do not issue a formal order. The citizen may be unable to obtain rations, may be told that her name is not visible, or may be asked to return after correction of a data mismatch. The absence of a formal written order should not defeat constitutional scrutiny. Public law must recognise functional decisions. If a technological step has the practical effect of denying an entitlement, it should be treated as a decision requiring reasons, review and remedy.

The equality inquiry should also account for informational inequality. Middle-class citizens may correct digital records, upload documents and pursue online grievances with relative ease. Poorer citizens may lack smartphones, stable internet, English literacy, free time, travel money or confidence before officials. A formally identical digital procedure may therefore impose unequal real burdens. Article 14 should permit courts to examine whether procedural design is realistically accessible to the class of persons who depend on the scheme.

VII. ACCOUNTABILITY, SEPARATION OF POWERS AND INSTITUTIONAL SAFEGUARDS

The second research question concerns institutional design. In a constitutional democracy, the executive may implement law but cannot silently rewrite it. Algorithmic systems can blur this boundary. A statutory scheme may say that all eligible persons are entitled to a benefit, while the software may require additional data matches, biometric success, location consistency or risk-score clearance. When such conditions are not publicly authorised, the system becomes a shadow rulebook. This is a separation-of-powers problem, not merely a transparency problem.³⁰

The first safeguard is legal authorisation. Any automated system that affects legal rights, public benefits, sanctions or surveillance should be introduced through a published legal instrument. The instrument need not contain technical minutiae, but it must identify the purpose, scope,

²⁹ Press Information Bureau, Cabinet Approves IndiaAI Mission with an Outlay of Rs. 10,371.92 Crore (Mar. 7, 2024).

³⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) [hereinafter EU AI Act].

data sources, decision role of the system, affected persons, review mechanism and responsible authority. Executive departments should not be allowed to impose digital conditions through circulars, vendor contracts or backend parameters that citizens cannot find.³¹

The second safeguard is an algorithmic impact assessment before deployment. Canada's Directive provides a useful template because it links the level of scrutiny to the potential impact of the system. For India, an assessment should examine legality, purpose, necessity, proportionality, affected groups, error rates, language access, disability access, data quality, cybersecurity, fallback arrangements and grievance capacity. The assessment should be published in a form understandable to the public, with sensitive details redacted only where strictly necessary.³²

The third safeguard is public procurement discipline. Many algorithmic systems are designed by private vendors, yet the constitutional duty remains with the State. Contracts should require audit access, documentation, testing data, bias evaluation, security standards, explanation support, termination rights and continuing public ownership of decision records. A government cannot contract out constitutional accountability. If a vendor's model cannot be reviewed, it should not be used for decisions that affect fundamental interests.³³

The fourth safeguard is an auditable decision record. Every automated or algorithmically assisted decision should preserve the data inputs, rules or model version, timestamp, officer responsible, reason code, exception path and subsequent review. Without such records, courts cannot review the decision and administrators cannot identify systemic defects. Record keeping is not bureaucratic excess; it is the infrastructure of accountability.³⁴

The fifth safeguard is mandatory human review. Human review should not mean a clerk pressing an approval button after the system has already determined the result. It should mean a legally empowered officer who can consider context, receive evidence, correct data and override the automated outcome. The officer must also be accountable for the final decision. Otherwise human review becomes a fiction used to legitimise automation without changing its

³¹ Regulation (EU) 2016/679, art. 22, 2016 O.J. (L 119) 1 [hereinafter GDPR].

³² Treasury Board of Canada Secretariat, Directive on Automated Decision-Making (as amended June 24, 2025).

³³ Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (opened for signature Sept. 5, 2024).

³⁴ Rechtbank Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865 (Neth.) [SyRI Judgment].

practical effect.³⁵

The sixth safeguard is an independent oversight mechanism. India need not create a separate regulator for every algorithmic system, but high-impact public systems should be subject to periodic audit by an independent body with legal and technical competence. The Data Protection Board under the DPDP Act may address some personal-data issues, but constitutional harms extend beyond data protection. Equality, welfare access, natural justice and administrative legality require broader public-law oversight.³⁶

Comparative instruments support these safeguards. The EU AI Act places high-risk obligations on providers and deployers, including risk management, data governance, technical documentation, record keeping, transparency and human oversight. GDPR Article 22 recognises special protection against solely automated decisions with significant effects. The Council of Europe Convention frames AI governance around human rights, democracy and the rule of law. India's constitutional framework can draw on these institutional ideas while grounding them in Articles 14, 21 and judicial review.³⁷

The IndiaAI Mission and NITI Aayog's responsible AI documents show that India has already recognised the need for inclusive and ethical AI. The difficulty is that principles remain vulnerable unless converted into enforceable duties. Responsible AI cannot depend on administrative goodwill. Where the State deploys automation in welfare, principles such as safety, reliability, equality, transparency and accountability must appear in statutes, rules, procurement conditions and judicial standards.³⁸

Federalism must also be considered. Welfare delivery in India often involves central databases, State-level implementation and local-level distribution. A system error may arise at any of these levels, while the citizen is forced to move between offices. Constitutional accountability should therefore be joint and functional. The authority that benefits from automation should remain responsible for ensuring that no person is denied a legal entitlement merely because the

³⁵ R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058 (Eng.).

³⁶ State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

³⁷ S. M. G. Rankin, The MiDAS Touch: Atuahene's 'Stategraft' and Unregulated Artificial Intelligence, 98 N.Y.U. L. Rev. Online 48, 53-60 (2023).

³⁸ Jean Dreze, Nazar Khalid, Reetika Khara & Anmol Somanchi, Aadhaar and Food Security in Jharkhand: Pain without Gain?, 52 Econ. & Pol. Wkly. 50 (2017).

responsible database belongs to another department.³⁹

The legislature also has a continuing role after authorisation. Committees should be able to call for audit reports, procurement documents and information about exclusion rates. Budgetary approval for digital welfare infrastructure should be linked to evidence that grievance and fallback mechanisms are funded. Otherwise, automation may be financed while remedy remains under-resourced. Constitutional governance requires that the costs of fairness be treated as part of the cost of the system, not as an optional supplement.

Local accountability is equally necessary. Central dashboards may show high transaction success while local failures remain hidden. Public authorities should publish district-wise and scheme-wise data on authentication failures, reversals, appeals and delays. Such publication would allow legislators, courts, journalists and civil society to detect whether particular regions or groups are bearing disproportionate error. Aggregate success figures should never be allowed to conceal concentrated constitutional injury.

VIII. JUDICIAL REVIEW OF OPAQUE ALGORITHMIC SYSTEMS

The third research question concerns courts. Judicial review of algorithmic administration should avoid two extremes. One extreme is technological deference: the court assumes that a system is objective because it is mathematical or computer-based. The other extreme is technological suspicion: the court treats complexity itself as illegality. Neither approach is satisfactory. Constitutional review should focus on authority, procedure, evidence, proportionality and remedies.⁴⁰

The first question for a court should be legality. What law authorises the system? Does the law permit automated decision-making, or only digital assistance? What is the system's role: advisory, screening, ranking, verification, sanctioning or final determination? If the legal basis is unclear, the decision should not survive. In *Anuradha Bhasin*, the Supreme Court insisted that restrictions affecting rights must be published to allow challenge. The same logic applies

³⁹ Karthik Muralidharan, Paul Niehaus & Sandip Sukhtankar, *Integrating Biometric Authentication in India's Welfare Programs: Lessons from a Decade of Reforms*, 14 *India Pol'y F.* 1 (2018).

⁴⁰ Silvia Masiero, *Biometric Infrastructures and the Indian Public Distribution System*, 26 *S. Asia Multidisciplinary Acad. J.* (2020).

to algorithmic conditions that affect welfare access.⁴¹

The second question should be reason-giving. Courts need not demand a full technical explanation in ordinary language, but they should demand a legally adequate explanation. A reason code such as 'system rejected' is not a reason. A lawful explanation should state the rule or factor that led to rejection, identify the disputed data, explain how the person may correct it, and identify the officer responsible for review. The duty to give reasons is a constitutional control on arbitrary power.⁴²

The third question should be proportionality. The State may have a legitimate interest in preventing fraud or improving targeting. The court should then ask whether the system is suitable for that aim, whether less rights-restrictive alternatives are available, whether safeguards reduce error, and whether the burden on affected persons is excessive compared with the public benefit. A system that reduces leakage but produces serious exclusion must be assessed against the constitutional value of the entitlement.⁴³

The fourth question should be equality impact. Courts should ask whether the system has been tested across affected groups, languages, regions, disabilities and socio-economic conditions. It is not enough to show average accuracy. In welfare schemes, small error rates can translate into large numbers of excluded persons. A constitutionally acceptable system must identify who bears the errors. If errors fall disproportionately on already vulnerable groups, Article 14 scrutiny should be heightened.⁴⁴

The fifth question should be remedy. Algorithmic cases require both individual and structural remedies. Individual relief may include restoration of benefit, correction of data, compensation, interim continuation and a fresh hearing. Structural relief may include publication of rules, independent audit, creation of fallback procedures, appointment of nodal officers, reporting to the court and suspension of a defective model. Courts should not hesitate to issue continuing

⁴¹ Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 11-36 (2018).

⁴² Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1254-66 (2008).

⁴³ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 1-17 (2015).

⁴⁴ Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671, 673-81 (2016), doi:10.15779/Z38BG31.

mandamus where the harm is systemic, but they should frame orders that administrators can implement.⁴⁵

Courts may use expert assistance without surrendering judgment. Algorithmic review often involves technical documents, error metrics and system architecture. Expert commissioners, amicus curiae with technical competence, sealed review and public summaries may help. However, the ultimate constitutional questions remain legal: whether the State has lawful authority, whether the decision is fair, whether rights are proportionately restricted, and whether remedies are effective.⁴⁶

The SyRI and Bridges decisions are useful because they show that courts can review technological systems through ordinary public-law principles. The Dutch court did not need to rebuild the algorithm; it examined transparency, safeguards and privacy impact. The Court of Appeal in Bridges focused on whether the legal framework gave excessive discretion and whether equality duties had been met. Indian courts can adopt a similar approach. The opacity of a system should not place it beyond law.⁴⁷

Loomis is a cautionary example. The Wisconsin Supreme Court allowed use of COMPAS with warnings, but the case illustrates the dangers of proprietary systems affecting legal outcomes. Warning labels may be insufficient when the affected person cannot test the methodology. In welfare administration, where decisions may affect subsistence, a weaker standard would be constitutionally troubling. Indian courts should require meaningful contestability rather than merely cautioning officials about limitations.⁴⁸

Courts should also distinguish between opacity that is technically unavoidable and opacity that is institutionally convenient. Some model behaviour may be difficult to explain fully. But many government systems are opaque because rules, datasets, contracts and logs are not published or preserved. The latter is not a feature of technology; it is a failure of administration. Judicial review should be strict when opacity results from avoidable secrecy or poor record keeping.

⁴⁵ Andrew D. Selbst et al., Fairness and Abstraction in Sociotechnical Systems, Proc. FAT* 2019, 59, 60-62, doi:10.1145/3287560.3287598.

⁴⁶ Margot E. Kaminski, The Right to Explanation, Explained, 34 Berkeley Tech. L.J. 189, 196-205 (2019).

⁴⁷ Mireille Hildebrandt, Smart Technologies and the End(s) of Law 165-91 (2015).

⁴⁸ Harini Suresh & John Guttag, A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle, arXiv:1901.10002 (2019).

In addition, courts should resist the argument that disclosure will always enable fraud. That concern may justify redaction of narrow operational details, but it cannot justify withholding the existence of a system, the legal basis for its use, the categories of data relied upon, the broad criteria for adverse action or the available remedies. A constitutional democracy cannot make welfare conditional on secret rules. The State may protect legitimate security interests while still giving citizens enough information to contest deprivation.

IX. DISCUSSION

The answer to the first research question is that Articles 14 and 21 can be adapted to algorithmic welfare decisions by treating automation as a form of State action. Article 14 examines whether the system is arbitrary, irrational or disproportionately burdens particular groups. Article 21 examines whether the deprivation of welfare-linked interests follows fair, just and reasonable procedure. The two provisions should be read together: equality prevents unjustified exclusion, while due process supplies the procedures through which exclusion may be contested.⁴⁹

The answer to the second research question is that accountability requires ex ante, contemporaneous and ex post safeguards. Ex ante safeguards include legal authorisation, impact assessment and procurement duties. Contemporaneous safeguards include notice, reasoned outputs, fallback channels and human review. Ex post safeguards include audit, appeal, judicial review, data correction and compensation. These safeguards preserve separation of powers because they prevent technical systems from becoming hidden sources of law.⁵⁰

The answer to the third research question is that courts should review algorithmic systems through a structured public-law test. The proposed test has six stages: legality, disclosure, procedural fairness, proportionality, equality impact and remedy. This test does not require courts to decide which model is technically best. It requires courts to ensure that public power remains lawful, intelligible, accountable and contestable. Judicial review can thus remain institutionally modest while still being constitutionally firm.⁵¹

⁴⁹ Nat'l Inst. of Standards & Tech., Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (2023).

⁵⁰ P. Jonathon Phillips et al., Four Principles of Explainable Artificial Intelligence, NISTIR 8312 (2021).

⁵¹ OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, amended 2024).

Taken together, the three answers support a broader thesis. Algorithmic due process is not a new fundamental right detached from the Constitution. It is the application of old constitutional commitments to new administrative forms. The language of natural justice, non-arbitrariness, dignity, proportionality and judicial review is sufficient, but it must be operationalised with new institutional tools. Otherwise constitutional doctrine will remain elegant while administrative harm becomes automated.⁵²

X. RECOMMENDATIONS

First, Parliament should enact a public-sector automated decision-making law or add a dedicated chapter to existing digital governance legislation. The law should apply to automated and algorithmically assisted systems used by public authorities for welfare, licensing, policing, migration, education, taxation, healthcare and other rights-affecting decisions. It should define levels of risk and prohibit final automated decisions in domains where life, liberty or subsistence is directly affected unless strict safeguards are satisfied.⁵³

Secondly, every high-impact system should be preceded by a mandatory algorithmic impact assessment. The assessment should be published before deployment, updated after material changes and subject to public comment where large populations are affected. It should identify purpose, legal authority, data sources, affected groups, likely errors, fallback arrangements, human review mechanisms and grievance capacity. Publication would also improve legislative and civil-society oversight.⁵⁴

Thirdly, welfare systems should adopt a constitutional fallback rule: no eligible person should be denied an essential benefit solely because biometric authentication, database matching or automated verification fails. The State may verify claims through alternative means, but the burden of system failure should not fall on the citizen. This rule is necessary because essential welfare is different from ordinary administrative convenience. Temporary continuation with later verification is often less harmful than immediate denial.⁵⁵

Fourthly, all automated decisions should be accompanied by intelligible reasons. The reasons should identify whether the decision was automated or algorithmically assisted, the legal rule

⁵² UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

⁵³ State of Kerala v. N.M. Thomas, (1976) 2 S.C.C. 310 (India).

⁵⁴ Modern Dental Coll. & Research Ctr. v. State of Madhya Pradesh, (2016) 7 S.C.C. 353 (India).

⁵⁵ Chintaman Rao v. State of Madhya Pradesh, 1950 S.C.R. 759 (India).

applied, the relevant data fields, the reason for rejection or flagging, and the steps for correction or appeal. Public authorities should develop standard reason templates that are short, local-language accessible and legally meaningful.⁵⁶

Fifthly, public procurement contracts should include constitutional clauses. Vendors should be required to provide technical documentation, audit logs, bias testing, security certification, explanation support and access for oversight bodies. Trade secrecy should not defeat constitutional review. If a system cannot be audited, it should not be procured for rights-affecting public administration.⁵⁷

Sixthly, an independent oversight body should be empowered to audit high-impact public algorithms. The body could be placed within an existing institution or created through legislation, but it must include legal, technical and social-policy expertise. Its reports should be public except for narrowly justified redactions. It should be able to recommend suspension of systems that create serious constitutional risk.⁵⁸

Seventhly, courts should develop procedural rules for algorithmic litigation. Petitioners should be allowed to seek disclosure of model documentation, impact assessments, error rates and decision logs. Courts should be able to appoint technical experts and order interim continuation of benefits where subsistence is at risk. Public-interest litigation should remain available where system design affects a class of persons unable to litigate individually.⁵⁹

Eighthly, administrators should receive training in constitutional technology governance. Local officers must understand that a digital rejection is not conclusive and that they retain a duty to prevent unconstitutional exclusion. Training should cover natural justice, disability access, language access, data correction, fallback procedures and record keeping. Algorithmic accountability will fail if it remains confined to central policy documents.⁶⁰

Finally, India should align responsible AI policy with constitutional remedies. Ethical principles are valuable, but they must be translated into enforceable duties and citizen-facing rights. The proposed approach does not reject innovation. It asks that innovation be disciplined

⁵⁶ Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).

⁵⁷ Joseph Shine v. Union of India, (2019) 3 S.C.C. 39 (India).

⁵⁸ State of U.P. v. Raj Narain, (1975) 4 S.C.C. 428 (India).

⁵⁹ Right to Information Act, No. 22 of 2005, India Code (2005).

⁶⁰ Bennett Coleman & Co. v. Union of India, (1972) 2 S.C.C. 788 (India).

by the Constitution. A digital State can be efficient and rights-respecting only when every person affected by a machine-assisted decision can know, contest and correct it.⁶¹

A further recommendation is to require periodic sunset review. High-impact automated systems should not continue indefinitely merely because they were once approved. Technology, data practices and social conditions change. A system that was proportionate at the pilot stage may become unconstitutional when scaled nationally without grievance capacity. Periodic renewal should depend on evidence of accuracy, fairness, accessibility, grievance performance and continued legal necessity.

Civil-society participation should be built into oversight. Organisations working with persons with disabilities, elderly persons, migrant workers, women, rural communities and ration-card holders often know where digital systems fail before official reports acknowledge the problem. Impact assessments and audits should therefore include consultation with affected groups. Constitutional morality in digital governance requires listening to those who experience the State at the point of exclusion.

XI. CONCLUSION

The twenty-first century State is not becoming less powerful because it is becoming digital. In many respects it is becoming more pervasive. Automated systems can act across scale, time and territory in ways that traditional bureaucracy could not. They can also make deprivation appear impersonal, inevitable and technically justified. Constitutional governance must therefore insist that the digital form of a decision does not weaken the legal standards that apply to it.⁶²

This article has argued that algorithmic welfare administration in India should be governed by algorithmic due process. The concept rests on familiar constitutional foundations: Article 14's rejection of arbitrariness, Article 21's demand for fair procedure, the duty to give reasons, the availability of judicial review and the rule of law. Its distinct contribution is institutional. It requires impact assessments, disclosure, reasoned outputs, human review, audit trails, fallback mechanisms and remedies designed for automated systems.⁶³

⁶¹ Internet Freedom Found., Project Panoptic: A Database on Facial Recognition Systems in India (2024).

⁶² Vidhi Centre for Legal Policy, Comments on the Draft Digital Personal Data Protection Rules, 2025 (2025).

⁶³ Upendra Baxi, *The Indian Supreme Court and Politics* 82-121 (1980).

The argument is also democratic. When software determines access to welfare, citizens should not be reduced to data subjects or error cases. They remain constitutional persons. They are entitled to be heard, to receive reasons, to correct records and to approach a court. A government that cannot explain its automated decisions cannot claim constitutional accountability merely because its objectives are benevolent.⁶⁴

India has an opportunity to build a model of digital constitutionalism suited to a large, unequal and welfare-oriented democracy. The path should not be copied wholesale from the European Union, Canada or any other jurisdiction. But comparative experience confirms a common lesson: algorithmic power must be visible, contestable and supervised. The Constitution can accommodate technological change, but it cannot allow technology to become a substitute for constitutional government.⁶⁵

The proposed framework is intentionally practical. It does not require an ideal administration or perfect technology. It requires public authorities to know what their systems do, to publish the rules that matter, to preserve records, to provide human correction and to accept judicial scrutiny. These are not radical demands. They are the minimum conditions under which automation can coexist with constitutional government.

The deeper lesson is that constitutionalism must be updated at the level of administration, not only at the level of grand doctrine. Courts may declare privacy, dignity and equality in powerful language, but citizens meet the Constitution through ration shops, pension offices, portals, databases and grievance counters. If those sites are governed by opaque technological authority, constitutional promises become fragile. Algorithmic due process is therefore a method for carrying constitutional law into the everyday machinery of the digital State.

The approach also keeps space for experimentation. Pilot projects, sandboxes and digital public infrastructure may be valuable where they are transparent and reversible. The constitutional objection is not to experimentation itself, but to experiments imposed on dependent populations without consent, explanation or remedy. A rights-respecting State should test systems with safeguards before relying on them to interrupt subsistence benefits. In that sense, algorithmic due process is not anti-innovation. It is the discipline that allows innovation to earn public trust.

⁶⁴ M.P. Jain, *Indian Constitutional Law* 924-1002 (8th ed. 2018).

⁶⁵ H.W.R. Wade & C.F. Forsyth, *Administrative Law* 339-80 (12th ed. 2023).

For a law journal issue on constitutional governance in the twenty-first century, this subject deserves close attention because it shows how constitutional power now travels through ordinary code, procurement and databases. The future of constitutionalism will not be decided only in constitutional amendments or landmark judgments. It will also be decided in the design of administrative systems that determine whether the poorest citizen can actually receive what the law promises.

The final claim is simple. A constitutional democracy may automate assistance, detection and verification, but it may not automate unaccountability. Whenever public power becomes computational, constitutional law must require a humanly intelligible path back to legality, reasons and repair.

That path is also necessary for legitimacy. Citizens will accept administrative technology more readily when they can see that errors are acknowledged, officials remain responsible and courts can still examine the exercise of power. Trust is not created by speed alone; it is created by accountable institutions.

REFERENCES

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

Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).

Barocas, Solon & Andrew D. Selbst. Big Data's Disparate Impact, 104 California Law Review 671 (2016). doi:10.15779/Z38BG31.

Citron, Danielle Keats. Technological Due Process, 85 Washington University Law Review 1249 (2008).

Coglianese, Cary & David Lehr. Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Georgetown Law Journal 1147 (2017).

Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (2024).

Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

Digital Personal Data Protection Rules, 2025, G.S.R. 843(E), Gazette of India, Extraordinary, Part II, sec. 3(i) (Nov. 13, 2025).

Dreze, Jean, Nazar Khalid, Reetika Khera & Anmol Somanchi. Aadhaar and Food Security in Jharkhand: Pain without Gain?, 52 Economic & Political Weekly 50 (2017).

EU Artificial Intelligence Act, Regulation (EU) 2024/1689, 2024 O.J. (L 1689).

Eubanks, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).

GDPR, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

Hildebrandt, Mireille. Smart Technologies and the End(s) of Law (2015).

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

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India).

Kaminski, Margot E. The Right to Explanation, Explained, 34 Berkeley Technology Law Journal 189 (2019).

Khera, Reetika. Dissent on Aadhaar: Big Data Meets Big Brother (2019).

Masiero, Silvia. Biometric Infrastructures and the Indian Public Distribution System, 26 South Asia Multidisciplinary Academic Journal (2020).

Muralidharan, Karthik, Paul Niehaus & Sandip Sukhtankar. Integrating Biometric Authentication in India's Welfare Programs: Lessons from a Decade of Reforms, 14 India Policy Forum 1 (2018).

NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (2023).

NITI Aayog. National Strategy for Artificial Intelligence #AIForAll (2018).

NITI Aayog. Responsible AI for All: Approach Document for India, Part 1: Principles for Responsible AI (2021).

OECD. Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, amended 2024).

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

Rankin, S. M. G. The MiDAS Touch: Atuahene's 'Stategraft' and Unregulated Artificial Intelligence, 98 N.Y.U. Law Review Online 48 (2023).

Rechtbank Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865 (Netherlands).

R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058 (England).

Selbst, Andrew D., Danah Boyd, Sorelle A. Friedler, Suresh Venkatasubramanian & Janet Vertesi. Fairness and Abstraction in Sociotechnical Systems, Proceedings of FAT* 2019, 59. doi:10.1145/3287560.3287598.

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

Treasury Board of Canada Secretariat. Directive on Automated Decision-Making (as amended June 24, 2025).

UNESCO. Recommendation on the Ethics of Artificial Intelligence (2021).

Wachter, Sandra, Brent Mittelstadt & Chris Russell. Counterfactual Explanations Without Opening the Black Box, 31 Harvard Journal of Law & Technology 841 (2018).