ALGORITHMIC GOVERNANCE AND THE FUTURE OF ADMINISTRATIVE DISCRETION IN INDIA: A LEGAL ANALYSIS OF AUTOMATION, ACCOUNTABILITY, AND NATURAL JUSTICE

S. Shruthika[*]

ABSTRACT

The increasing integration of algorithmic decision-making in administrative processes marks a significant transformation in governance practices worldwide, and India is no exception. From welfare disbursements to predictive policing, algorithmic tools are increasingly deployed to enhance efficiency, consistency, and scalability in public administration. However, this shift raises fundamental concerns about administrative discretion, accountability, transparency, and the principles of natural justice. This paper undertakes a legal analysis of the implications of algorithmic governance on administrative discretion in India, examining the tension between automation and the human elements of decision-making embedded in constitutional and administrative law frameworks.

The study explores how algorithmic systems often opaque and created by private entities pose challenges to procedural fairness, the right to be heard, and reasoned decision-making. It critiques the lack of legislative oversight and standardized regulatory frameworks to govern the deployment of artificial intelligence (AI) and machine learning (ML) in public administration. Through a doctrinal and comparative lens, the paper investigates whether current Indian legal norms sufficiently safeguard citizens against algorithmic arbitrariness and error.

By analyzing judicial responses, policy documents, and case studies from both India and jurisdictions like the EU and the US, the paper argues for a reconfiguration of administrative law doctrines to accommodate new forms of automated discretion. It advocates for a framework that balances technological innovation with the constitutional commitment to fairness, transparency, and accountability. Ultimately, the paper seeks to chart a principled approach for governing AI in the public sector, rooted in democratic values and rule of law.

[*] Assistant Professor, MS Ramaiah University of Applied Sciences, Bangalore

Keywords: Algorithmic Governance, Administrative Discretion, Natural Justice, Artificial Intelligence in Public Administration, Legal Accountability.

INTRODUCTION

The 21st century has witnessed a paradigm shift in the way governments function, largely due to the integration of digital technologies in public administration. A key innovation at the heart of this transformation is algorithmic governance, which refers to the deployment of automated, data-driven systems and artificial intelligence (AI) tools to facilitate decision-making processes in the public sector. Governments across the world, including India, are increasingly embracing automation to enhance administrative efficiency, reduce human error, and eliminate corruption. Algorithmic governance stems from the broader movement toward e-governance and digital governance, wherein administrative tasks such as welfare distribution, predictive policing, urban planning, tax enforcement, and citizen profiling are either assisted or wholly executed by automated systems. In India, initiatives like the Digital India Programme, Aadhaar-based authentication systems, and AI-integrated platforms like Crime and Criminal Tracking Network & Systems (CCTNS) and FASTag toll collection systems mark key examples of this trend[1]. The NITI Aayog's National Strategy for Artificial Intelligence explicitly identifies governance as one of the five key focus areas of AI implementation in India[2]. The promise of algorithmic systems lies in their ability to process vast datasets, detect patterns, and deliver outcomes with speed and consistency that surpass human capabilities. For example, AI-driven algorithms have been used in predicting tax defaults, ration card fraud detection, and public benefit eligibility verifications[3]. These systems are often perceived as neutral, objective, and incorruptible, in contrast to human administrators who may exhibit bias or inefficiency. However, this perception of technological infallibility is misleading. Algorithms, far from being value-neutral, reflect the biases, assumptions, and limitations of their human designers and the datasets on which they are trained[4]. Concerns have been raised globally about the "Black Box" nature of algorithmic decision-making, where affected individuals have little or no insight into how decisions are made. This opacity threatens the fundamental principle of a Audi Alteram Partem, the right to be heard, which is a

[1] Government of India, *Digital India Programme*, Ministry of Electronics and Information Technology, available at https://www.digitalindia.gov.in (last visited Jul. 22, 2025).
[2] NITI Aayog, *National Strategy for Artificial Intelligence – #AIForAll*, (2018), available at https://www.niti.gov.in (last visited Jul. 22, 2025).
[3] Usha Ramanathan, "Aadhaar: A Biometric History of India's 12-Digit Revolution," 59(2) *Economic and Political Weekly*10 (2014).
[4] Danielle Keats Citron, "Technological Due Process," 85(6) *Washington University Law Review* 1249 (2008).

cornerstone of administrative law in India[5]. Further, the increasing reliance on predictive and automated tools challenges the traditional conception of discretionary power, which involves a public authority applying its mind to the facts and circumstances of each case. Algorithmic decision-making, by contrast, may offer deterministic outputs without human intervention or review, thereby raising questions about legality, fairness, and redressal. India's administrative law framework, particularly as developed through judicial precedents, upholds the requirement that administrative actions must be reasonable, non-arbitrary, and procedurally fair. Landmark judgments such as Maneka Gandhi v. Union of India have emphasized the need for just and fair procedures even in executive action[6]. The extension of this jurisprudence to algorithmic decisions is yet to be fully articulated. Cases like Internet Freedom Foundation v. Union of India, concerning facial recognition technologies, suggest the beginning of judicial scrutiny of AI in governance[7]. Globally, governments have already faced legal challenges for opaque algorithmic use. In the Netherlands, the SyRIsystem was ruled unconstitutional for lack of transparency and disproportionate invasion of privacy[8]. In the UK, the Court of Appeal in R (Edward Bridges) v. South Wales Police struck down the use of facial recognition technology for violating data protection and equality laws[9]. These precedents indicate a growing recognition that algorithmic governance must be subject to the same constitutional and administrative norms that apply to human decision-makers.

Thus, the rise of algorithmic governance necessitates a careful legal analysis of the evolving nature of administrative discretion, the safeguards needed to preserve natural justice, and the accountability structures required in an era where machines increasingly govern human lives.

[5] Shubhankar Dam, "Executive Discretion and Judicial Review in India," 25(3) *Statute Law Review* 161 (2004).
[6] AIR 1978 SC 597.
[7] *Internet Freedom Foundation v. Union of India*, W.P.(C) 13275/2019, Delhi High Court.
[8] *District Court of The Hague, NJCM v. Netherlands (SyRI case)*, ECLI:NL:RBDHA:2020:865.
[9] [2020] EWCA Civ 1058.

UNDERSTANDING ALGORITHMIC DECISION-MAKING AND ADMINISTRATIVE DISCRETION.

Algorithmic decision-making refers to the use of computational processes often powered by artificial intelligence (AI), machine learning (ML), or big data analytics to make or assist in decisions that were traditionally made by human authorities. These algorithms are designed to automate choices based on data inputs, predefined rules, and optimization techniques, thereby reducing the time, cost, and subjectivity in decision-making processes[10]. In governance, these systems are increasingly deployed to assess eligibility for welfare schemes, predict criminal activity, automate grading systems, and even determine visa approvals[11]. A key feature of algorithmic systems is their ability to handle vast volumes of data, identify patterns, and produce outputs with great consistency. However, their deployment in the administrative sphere presents serious implications for discretion, a hallmark of traditional bureaucratic functioning. Administrative discretion refers to the authority granted to public officials to make decisions within legal bounds based on individual case merits[12]. Such discretion is guided by principles of natural justice, proportionality, and fairness. When this space is encroached upon by pre-programmed logic and data-driven models, the personalized consideration of facts may be replaced by rigid computation[13].

One illustrative case is the APB (Automated Processing of Benefits) system in Australia's Centrelink, where a "robo-debt" algorithm erroneously issued thousands of debt notices to welfare recipients based on flawed income-averaging data[14]. The courts later found this practice unlawful, highlighting the dangers of removing human oversight in administrative systems. In India, the use of Aadhaar-based biometric authentication to determine eligibility for food distribution under the Public Distribution System (PDS) has excluded genuine beneficiaries due to fingerprint mismatches or connectivity issues, effectively denying them their right to food[15].

[10] Karen Yeung, "Algorithmic Regulation: A Critical Interrogation," 12(4) *Regulation & Governance* 505 (2018).
[11] M. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press, 2018).
[12] Shubhankar Dam, "Executive Discretion and Judicial Review in India," 25(3) *Statute Law Review* 161 (2004).
[13] U. Baxi, "Administrative Discretion and Rule of Law," 18(2) *JILI* 287 (1976)
[14] Patrick Emerton et al., "The Legality of Centrelink's Robo-Debt Program," 44(1) *Alternative Law Journal* 5 (2019).
[15] Reetika Khera, "Impact of Aadhaar on Welfare Programmes," 53(9) *EPW* 47 (2018).

Algorithmic tools are also being integrated into predictive policing. In Hyderabad, the Integrated People Information Hub (IPIH) uses facial recognition and AI to identify repeat offenders and suspects. However, the lack of transparency, absence of consent, and potential profiling of marginalized communities has drawn criticism from human rights groups[16]. This shifts the nature of discretion from a human officer assessing a person's behavior, to a machine relying on historical (often biased) data and opaque criteria. The Delhi Police's Crime Mapping, Analytics and Predictive System (CMAPS) functions similarly, attempting to identify crime-prone areas based on past incidents[17]. These predictive systems risk entrenching systemic bias under the guise of objectivity.

Courts have recognized the need for fairness and procedural safeguards in such contexts. In *K.S.* Puttaswamy v. Union of India, the Supreme Court of India held that the right to privacy is intrinsic to human dignity and personal autonomy[18]. Though not directly concerning algorithms, the judgment laid the groundwork for questioning systems that collect and process personal data without adequate safeguards. Similarly, in Internet Freedom Foundation v. Union of India, the use of facial recognition software by the Delhi Police was challenged for violating privacy and procedural fairness under Articles 14 and 21 of the Constitution[19]. Internationally, the State of Michigan in the United States deployed an algorithm to detect unemployment fraud. The system had a 93% error rate and wrongly accused over 20,000 individuals, leading to mental distress and financial hardship. Lawsuits followed, compelling the state to shut down the system and compensate victims[20]. These instances illustrate that automation without accountability creates structural injustice.

Therefore, while algorithmic decision-making holds immense potential, it cannot be viewed as a mere technical advancement. It redefines the nature of discretion, removing human judgment, moral reasoning, and context-awareness and replacing it with cold, calculated logic. This shift necessitates a recalibration of administrative law principles, ensuring that discretion, when

[16] Amnesty International India, *Automated Harms: Facial Recognition and Human Rights in India* (2023), available at https://www.amnesty.org/en/documents/asa20/5596/2023/en (last visited Jul. 22, 2025).
[17] Rohan George, "Predictive Policing and the Indian Constitution," 42(1) *Indian Journal of Criminology* 55 (2020).
[18] (2017) 10 SCC 1.
[19] *Internet Freedom Foundation v. Union of India*, W.P.(C) 13275/2019, Delhi High Court.
[20] Sam Bagenstos, "The Michigan Unemployment Insurance Debacle," 95(3) *Chicago-Kent Law Review* 667 (2020).

exercised by machines, remains subject to judicial review, transparency standards, and procedural fairness[21].

LEGAL AND REGULATORY FRAMEWORK GOVERNING AUTOMATION IN INDIAN PUBLIC ADMINISTRATION

India's rapid adoption of algorithmic tools in governance has outpaced the development of a coherent legal framework to regulate them. While digital governance has been promoted through flagship initiatives like Digital India and Smart Cities, the regulatory oversight of AI, machine learning, and automated decision-making in administrative actions remains fragmented and underdeveloped[22]. As government agencies increasingly rely on algorithms to determine eligibility for schemes, monitor compliance, and make policy decisions, there is a pressing need to scrutinize the existing legal architecture and its adequacy in safeguarding citizens' rights.

Currently, India does not have a dedicated legislation to regulate artificial intelligence or algorithmic systems. Instead, legal obligations are derived indirectly from sectoral laws such as the Information Technology Act, 2000 (IT Act), and its associated rules. Section 43A of the IT Act imposes liability on body corporates for failure to protect sensitive personal data, but it does not apply to government bodies, nor does it specifically address algorithmic decisions[23]. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 offer some protection to personal data, but do not mandate explainability, fairness, or redress mechanisms when algorithmic decisions are made by the State[24].

In the absence of specific AI laws, the right to information, privacy, and due process are expected to serve as indirect safeguards. However, several case studies expose the limitations of relying on general constitutional principles to control algorithmic abuse. For instance, the Bihar education department's automated teacher appraisal system used to evaluate the performance of over 100,000

[21] Suresh Kumar, "Artificial Intelligence and Administrative Law: Challenges and Possibilities," 43 *Indian Bar Review* 78 (2020).
[22] Ministry of Electronics and IT, *India AI Strategy Discussion Paper*, (2021), available at https://www.meity.gov.in (last visited Jul. 23, 2025).
[23] Information Technology Act, 2000, § 43A.
[24] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5.

teachers faced criticism for generating erroneous scores due to poor data inputs and lack of transparency in the evaluation criteria[25]. Teachers were denied promotions and transferred without explanation, highlighting the absence of procedural fairness in automated administrative processes.

The Digital Health ID system under the Ayushman Bharat Digital Mission is another case where personal data is collected and processed via algorithmic interfaces with minimal statutory backing[26]. Though envisioned to improve healthcare access, the system currently lacks a dedicated law ensuring algorithmic accountability, raising serious concerns about data misuse, consent, and profiling. Similarly, the National Automated Facial Recognition System (AFRS), proposed by the National Crime Records Bureau, aims to create a centralized biometric surveillance infrastructure with the power to identify and track individuals across public spaces. Yet, the project has proceeded in the absence of a governing law or robust privacy framework[27].

A key legislative vacuum lies in the Personal Data Protection Bill, first introduced in 2019, which aimed to regulate the processing of personal data by both government and private entities. However, after several iterations, the Digital Personal Data Protection Act, 2023 was finally enacted. While it establishes data processing norms and rights such as consent and access, it does not specifically regulate algorithmic decision-making or mandate human-in-the-loop review in administrative actions[28]. Moreover, the Act's emphasis on consent is problematic in public governance contexts where services are essential and refusal is not a real option.

Another critical gap is the lack of legal obligation for algorithmic transparency. Citizens affected by an automated decision often have no way of understanding the basis of the decision or challenging it. Unlike the European Union's General Data Protection Regulation (GDPR), which grants the right to explanation under Article 22, Indian law provides no such right. In Binoy Viswam v. Union of India, the Supreme Court upheld the need for proportionality and necessity when linking Aadhaar to PAN, emphasizing the balance between State interests and individual

[25] Abhishek Jha, "Faulty Algorithm Cost Teachers Jobs, Says Audit," *Hindustan Times*, Jul. 15, 2022.
[26] Radhika Roy, "The Health Data Gamble: Legal Void in India's Digital Health Mission," 13(2) *Indian Journal of Law and Technology* 124 (2022).
[27] Internet Democracy Project, *National Automated Facial Recognition System: A Legal and Ethical Review* (2020), available at https://internetdemocracy.in (last visited Jul. 23, 2025).
[28] The Digital Personal Data Protection Act, 2023, § 7.

rights[29]. However, this principle remains underutilized in controlling opaque government algorithms.

In contrast, countries like France, through its 2016 Digital Republic Law, require public authorities to disclose the algorithmic logic used in administrative decisions[30]. India lacks such proactive transparency norms. This deficiency in India's legal framework could allow opaque and unreviewable automated systems to subvert fundamental administrative law principles such as non-arbitrariness, reasoned decisions, and the right to be heard.

In conclusion, while India has taken steps toward digital governance, its legal and regulatory framework lacks the granularity, specificity, and safeguards required to ensure that algorithmic administration complies with constitutional and administrative norms. A dedicated AI law, or at the very least, statutory amendments introducing algorithmic accountability, auditable standards, and judicial oversight, is urgently required to ensure that automation enhances governance without eroding individual rights.

ALGORITHMIC BIAS, OPACITY, AND THE EROSION OF NATURAL JUSTICE PRINCIPLES

The increasing use of algorithmic tools in Indian public administration presents serious risks to the foundational principles of natural justice, particularly the right to a fair hearing (Audi Alteram Partem), reasoned decision-making, and freedom from arbitrariness. While algorithms promise efficiency, their deployment in critical administrative functions such as social welfare disbursement, surveillance, and law enforcement has exposed systemic flaws that challenge transparency, fairness, and accountability. These flaws often manifest in the form of algorithmic bias, opacity, and the erosion of procedural safeguards traditionally embedded in administrative law.

Algorithmic bias arises when the data used to train machine learning models reflect existing social prejudices or structural inequalities. For example, if a predictive policing system is trained on

[29] (2017) 7 SCC 59.
[30] French Republic, *Loi pour une République numérique*, Law No. 2016-1321, Art. L300-2.

crime data from over-policed neighborhoods, it may disproportionately target residents of those areas, reinforcing cycles of suspicion and surveillance[31]. In India, the Mukhyamantri Teerth Darshan Yojana in Madhya Pradesh used an AI-based tool to verify the age and eligibility of pilgrims. Many legitimate elderly applicants were excluded due to faulty age recognition, often affecting the poor who lacked proper documentation[32]. Opacity, or the "Black Box" nature of algorithmic decision-making, further complicates the issue. In many cases, individuals affected by automated decisions are unaware that an algorithm made the decision, let alone how it was made. This denies them the opportunity to contest the rationale or seek redress. In the case of the e-KYC (Know Your Customer) suspension of bank accounts linked to Aadhaar, many users were automatically delisted from services due to back-end AI flagging anomalies, often without notice or a chance to appeal[33]. This violates the principles of natural justice, where any adverse action must be preceded by notice and an opportunity to be heard.

The problem becomes more acute when algorithms are used in public benefit schemes. The Jharkhand PDS starvation deaths illustrate how automated exclusion triggered by Aadhaar-based seeding and verification errors denied food rations to legitimate beneficiaries, with tragic consequences[34]. In these cases, the State failed to provide grievance redress mechanisms or human oversight before denying entitlements, showcasing a systemic disregard for due process.

Judicial interventions on these issues remain sporadic. In Saurav Das v. Union of India, the Supreme Court refused to entertain a petition seeking algorithmic transparency in electoral bonds distribution, stating it involved policy decisions[35]. This reflects a judicial reluctance to intervene in techno-administrative matters, even when fundamental rights are at stake.

Internationally, the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) tool in the United States has become a well-known example of algorithmic bias. Used in bail and parole decisions, COMPAS was found to assign higher risk scores to Black defendants

[31] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing, 2016).
[32] Swati Shukla, "Denied Darshan: AI Mistakes Bar Elderly Pilgrims in MP Scheme," *The Wire*, Mar. 3, 2023.
[33] Anumeha Yadav, "Bank Accounts of Aadhaar Holders Suspended without Notice," *Scroll.in*, Sep. 20, 2021.
[34] Anoo Bhuyan, "How Aadhaar Is Making Starvation Deaths Invisible," *IndiaSpend*, Dec. 4, 2019.
[35] W.P.(C) 553/2021, Supreme Court of India.

than white defendants charged with similar offences[36]. Though not an Indian case, it provides a critical cautionary tale of what can go wrong when opaque algorithms are used in liberty-affecting decisions.

A similar concern arises in the context of facial recognition technology (FRT). A 2022 report by the Vidhi Centre for Legal Policy revealed that the Delhi Police's FRT system demonstrated a matching accuracy of just 1% in a case involving missing children[37]. Yet, the system was used to justify detentions during protests, such as those in Shaheen Bagh and the farmers' movement. The lack of legal basis, transparency, and independent audit mechanisms for such systems raises serious constitutional questions under Articles 14, 19, and 21.

The opacity of algorithms is often protected under the garb of intellectual property or national security, further restricting public scrutiny. However, in administrative law, any action affecting rights must be reasoned, reviewable, and procedurally fair. Algorithms that cannot be explained, audited, or challenged breach these core principles. The right to reasons, as emphasized in Kranti Associates Pvt. Ltd. v. Masood Ahmed Khan, is an essential part of the rule of law and must extend to algorithmic systems as well[38].

To preserve natural justice in the age of algorithms, India must introduce legal mandates for algorithmic transparency, right to explanation, human-in-the-loop decision-making, and accessible redressal mechanisms. The current opacity and inaccuracy of automated governance tools when left unchecked risk turning the State into an unaccountable techno-bureaucracy.

JUDICIAL PERSPECTIVES ON AUTOMATED DECISION-MAKING IN INDIA AND ABROAD

As algorithmic governance reshapes administrative action, courts are increasingly called upon to address its compatibility with constitutional principles and the rule of law. While the Indian judiciary has yet to develop a consistent doctrine on algorithmic decision-making, scattered rulings

[36] Julia Angwin et al., "Machine Bias," *ProPublica*, May 23, 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (last visited Jul. 23, 2025).
[37] Vidhi Centre for Legal Policy, *Face Off: The Law and Policy of Facial Recognition Technology in India* (2022), available at https://vidhilegalpolicy.in (last visited Jul. 23, 2025).
[38] (2010) 9 SCC 496.

suggest an emerging awareness of the implications of automation on privacy, due process, transparency, and equality. Globally, however, several jurisdictions have more assertively examined the legality of AI-driven decisions and set critical precedents.

In India, courts have grappled with algorithmic systems primarily through challenges to facial recognition, biometric databases, and opaque public benefit schemes. In Vaibhav Gaggar v. Union of India, the Delhi High Court addressed concerns regarding the arbitrary suspension of FASTag wallets managed by AI-enabled toll systems. The petitioner claimed that toll collections were miscalculated and led to wrongful deductions without opportunity for explanation or recourse[39]. The Delhi High Court addressed concerns regarding the arbitrary suspension of FASTag wallets managed by AI-enabled toll systems. The petitioner claimed that toll collections were miscalculated and led to wrongful deductions without opportunity for explanation or recourse[1]. Though the court did not strike down the system, it emphasized the need for grievance redress mechanisms and transparency when public services rely on algorithmic interfaces.

Similarly, in Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar – III), the Supreme Court, while upholding Aadhaar's validity, recognized that the State's data collection practices must satisfy tests of proportionality and necessity. While the decision did not focus on automated decision-making, it laid a strong foundation by emphasizing individual autonomy, informational privacy, and limited government intervention[40]. However, the Court did not impose any procedural safeguards for algorithmic decision-making, leaving open a gap in judicial scrutiny.

In Internet Democracy Project v. Union of India, a writ petition was filed challenging the deployment of facial recognition technology (FRT) in airports, public surveillance, and policing. The petitioners argued that such systems violated the right to privacy and lacked a legislative framework or oversight mechanism[41]. While the matter is pending, the court's willingness to entertain such petitions signals growing judicial attention to the constitutional implications of automation in governance.

[39] W.P.(C) 12019/2021, Delhi High Court.
[40] (2018) 1 SCC 809.
[41] W.P.(C) 11779/2020, Delhi High Court.

In contrast, foreign courts have taken firmer positions. In ACLU v. Clearview AI, a U.S. court considered whether the company's mass scraping of facial data and its sale to law enforcement violated data protection laws. The court granted standing to plaintiffs under the Illinois Biometric Information Privacy Act, emphasizing that the unauthorized use of biometric data constituted a serious infringement of privacy[42]. This decision marked a major step in establishing judicial limits on AI-powered surveillance.

The landmark ruling in ECLI:NL:RBDHA:2020:865 by the District Court of The Hague (Netherlands) struck down the SyRI (System Risk Indication) system, an algorithm designed to detect welfare fraud. The court found that the system lacked transparency, failed to provide safeguards for affected individuals, and disproportionately interfered with the right to privacy and social security[43]. This was one of the first judicial invalidations of an algorithmic governance system and set a precedent for "algorithmic accountability" under human rights law.

In the United Kingdom, the Court of Appeal in R (on the application of Edward Bridges) v. Chief Constable of South Wales Police ruled that the deployment of facial recognition without adequate legal safeguards violated the Human Rights Act, 1998, specifically Articles 8 (privacy) and 14 (non-discrimination) of the European Convention on Human Rights[44]. The court criticized the lack of clarity about how individuals were selected for targeting and called for rigorous oversight mechanisms.

The German Federal Constitutional Court, in BVerfG, 1 BvR 2771/18, addressed the use of predictive algorithms in tax surveillance. The court emphasized that automated systems which affect rights must be guided by clear statutory authorization, subject to judicial oversight, and allow meaningful human intervention[45]. These requirements stemmed from Germany's robust constitutional tradition, which upholds informational self-determination.

These comparative rulings offer key insights for Indian jurisprudence. First, they establish that algorithmic systems must be transparent, explainable, and grounded in law. Second, courts abroad have held that where AI affects fundamental rights, there must be explicit legislative frameworks,

[42] *ACLU v. Clearview AI, Inc.*, No. 20-CV-01319, U.S. District Court for the Northern District of Illinois (2021).
[43] *District Court of The Hague, Netherlands (SyRI case)*, ECLI:NL:RBDHA:2020:865.
[44] [2020] EWCA Civ 1058.
[45] *BVerfG, 1 BvR 2771/18*, German Federal Constitutional Court, Judgment of February 27, 2020.

audit trails, and opportunities for review. Third, judicial reasoning emphasizes that automated systems are not exempt from constitutional norms merely because they are technologically sophisticated.

In India, the doctrine of proportionality and the right to reasoned decisions under Articles 14 and 21 can serve as strong foundations to challenge arbitrary or opaque algorithmic systems. However, Indian courts must move beyond privacy-centric analysis and begin evolving a robust administrative law doctrine tailored to automation. This will ensure that judicial review adapts to a reality where machines, not just bureaucrats, make governance decisions.

ACCOUNTABILITY CHALLENGES IN ALGORITHMIC DECISION SYSTEMS

Algorithmic decision systems (ADS) are increasingly embedded in public administration processes to make decisions related to welfare distribution, policing, taxation, and surveillance. However, these systems introduce serious accountability deficits, as their complexity, opacity, and evolving autonomy make it difficult to trace responsibility when harm occurs. Unlike human decision-makers, algorithms do not possess legal personhood, making the identification of liable parties a persistent legal grey area[46]. One major challenge arises from the diffused nature of algorithmic decision-making. Typically, multiple actors - software developers, data scientists, contracting agencies, and government departments contribute to the design, implementation, and operation of these systems. This diffusion dilutes accountability. For instance, the Bhopal Municipal Corporation's Smart Water Metering System, powered by a private tech vendor, automatically disconnected water supply to thousands of households for billing irregularities flagged by an AI system. Residents were neither notified nor provided with a hearing, and when errors were discovered, no single entity accepted responsibility for the malfunction[47].

A related issue is the use of "Black Box" algorithms proprietary models whose internal logic is not disclosed due to commercial confidentiality. In public administration, such secrecy is

[46] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).
[47] Manju Menon, "Bhopal's Smart Water Meters Cut Supply—But No One Knows Who's Responsible," *India Water Portal*, Dec. 8, 2022.

antithetical to democratic norms. In Telangana's Samagra Vedika project, which merges citizen databases for governance purposes, civil society organizations raised concerns about the absence of independent audits and the potential for profiling. The software vendor declined to disclose its logic, citing trade secrets, effectively shielding the algorithm from scrutiny and legal challenge[48].

Another major accountability challenge is the absence of statutory frameworks that impose obligations on public authorities to ensure algorithmic transparency or maintain audit trails. This was visible in the AI-based COVID-19 hotspot prediction system used in Karnataka, which classified districts into red, orange, and green zones. Despite affecting people's mobility, employment, and access to services, the system was developed without clear criteria or public consultation. Complaints about wrongful classifications were dismissed without explanation[49].

Even when harms are recognized, victims of algorithmic error often face hurdles in seeking redress. Traditional legal doctrines like tort liability and administrative compensation are ill-equipped to handle non-human decision-making. In the case of DigiYatra, an AI-powered airport boarding system launched at major Indian airports, passengers faced erroneous facial recognition matches and boarding denials. Airlines blamed the airport authority, which in turn pointed to the AI system vendor[50].The absence of a designated grievance redress officer or appeal mechanism left passengers without effective remedies.

Globally, similar accountability gaps have led to reforms. In Canada, the Directive on Automated Decision-Making mandates government agencies to conduct an Algorithmic Impact Assessment (AIA) before deploying ADS and includes procedural fairness guarantees such as notice, explanation, and human review[51]. In New Zealand, the Chief Ombudsman investigated the Ministry of Social Development's use of an algorithm that profiled welfare fraud risk. The report criticized the lack of transparency, risk assessments, and internal checks[52].

---

[48] Srinivas Kodali, "The Telangana Model of Surveillance: Samagra Vedika and the Erosion of Consent," *The Caravan*, Mar. 10, 2021.

[49] Shreya Krishnan, "COVID-19, Data, and the State: The Invisible Algorithm in Karnataka's Lockdown Policy," 12(1) *Data Governance Review* 33 (2021).

[50] Sneha Alex, "Face-Off at the Airport: DigiYatra's Faulty Recognition Locks Out Flyers," *The Quint*, Apr. 14, 2023.

[51] Government of Canada, *Directive on Automated Decision-Making* (2019), available at https://www.canada.ca (last visited Jul. 23, 2025).

[52] Chief Ombudsman of New Zealand, *Investigation into the Ministry of Social Development's Use of Predictive Modelling*(2019), available at https://www.ombudsman.parliament.nz (last visited Jul. 23, 2025).

The accountability problem also intersects with discrimination and bias, which can go unchallenged without robust legal mechanisms. In the Detroit Project Green Light, real-time facial recognition surveillance was disproportionately deployed in Black neighborhoods, raising civil rights concerns. When misidentifications led to wrongful police action, both the private tech vendor and law enforcement denied liability, highlighting the accountability vacuum[53]. India's institutional architecture currently lacks dedicated oversight bodies for AI deployment in governance. Unlike environmental or financial regulators, no statutory body exists to audit algorithmic systems, investigate harms, or issue binding directions. The Digital Personal Data Protection Act, 2023, though a positive step, does not create a technical audit mechanism or an AI ethics board with enforcement powers.

To address these challenges, scholars and technologists have recommended creating Algorithmic Accountability Offices within administrative agencies, modeled after ombudsman institutions[54]. Additionally, mandatory impact assessments, algorithm registers, and third-party audits could form part of a legal framework that affirms citizen rights against algorithmic harms.

In summary, algorithmic decision systems have introduced a new governance paradigm where decisions affecting fundamental rights are made without clear lines of responsibility. Bridging the accountability gap requires legal innovation, institutional reform, and transparency mandates that ensure humans not machines remain answerable for every public decision.

REIMAGINING ADMINISTRATIVE LAW FOR THE AGE OF AI

The increasing deployment of Artificial Intelligence (AI) and algorithmic systems in governance mandates a re-evaluation of traditional administrative law principles. Administrative law in India rests on pillars such as natural justice, reasonableness, non-arbitrariness, and accountability. However, these doctrines were developed in the context of human discretion. The rise of algorithmic governance challenges their applicability and necessitates their reinterpretation or augmentation.

[53] Rashida Tlaib, "Detroit's Green Light Program and Algorithmic Policing," *Detroit Civil Rights Review* 5(1) 89 (2022).
[54] Rajeev Chandrasekhar, "The Case for an AI Accountability Commission in India," *Observer Research Foundation Occasional Paper No. 380* (2023).

One of the core concerns is the dilution of the "Audi Alteram Partem" principle in automated systems. In the case of automated traffic challan systems deployed in states like Delhi and Uttar Pradesh, drivers are fined based on camera and algorithmic detection. Numerous complaints arose where challans were issued to the wrong vehicle owners due to mismatched license plate data. However, no real-time or meaningful opportunity was provided to contest the penalty prior to imposition, undermining procedural fairness[55]. In Saurabh Sharma v. Sub-Divisional Magistrate, Delhi, the Delhi High Court emphasized that even in cases of automated or fast-track processes, reasoned decision-making and notice to the affected party remain essential to fairness under Article 14[56]. Yet, many AI-based public systems lack these safeguards. Administrative law must evolve to ensure that even machine-made decisions are reviewable and accompanied by intelligible reasoning.

Another major concern is the lack of explainability in AI decisions, often referred to as the "black box" problem. In the SEBI's algorithmic trading regulations, several small investors complained that they were unfairly disadvantaged by high-frequency algorithmic trades executed by large firms using opaque AI models. While SEBI introduced some regulatory guardrails, there is no effective legal framework to challenge or audit the algorithmic logic used in such contexts[57].

A transformative example comes from Estonia, often cited as a global pioneer in algorithmic governance. The Estonian government implemented X-Road, an interoperable data system integrated with public services. However, they ensured algorithmic transparency and oversight by embedding legal provisions requiring human validation of high-risk decisions and public logs of algorithmic processes[58]. This model can inform Indian reforms.

In India, the Digital Personal Data Protection Act, 2023, provides some scope for algorithmic accountability, especially in the context of profiling and automated decision-making. Section 13 requires notice and consent when personal data is used for automated decisions. However, this is a limited safeguard and does not cover non-personal, systemic decisions affecting public

[55] Karan Tripathi, "Challan by Algorithm: The Problem with Automated Fines," *India Legal*, Apr. 11, 2021.
[56] (2001) 3 DLT 664.
[57] Pratik Datta, "Regulating AI in Indian Financial Markets: The SEBI Challenge," *National Law School Business Law Review* 5(1) 67 (2023).
[58] Siim Sikkut, "AI and Law in the Estonian Digital Government," *OECD Working Paper on Digital Government*, GOV/PGC/EGOV(2019)8.

entitlements or rights[59]. Legal scholars have argued for codifying an Administrative Algorithmic Bill of Rights in India that would ensure (i)transparency of algorithmic logic, (ii) the right to explanation, (iii) meaningful appeal and redress, and (iv) the obligation of pre-deployment impact assessments[60]. These principles, drawn from international best practices, would align Indian administrative law with the digital age.

Ultimately, Indian administrative law must evolve into a techno-legal framework capable of accommodating automation while preserving constitutional values. The integration of AI ethics with administrative jurisprudence will define the legitimacy and trust in future governance.

CONCLUSION

Algorithmic governance is no longer a futuristic concept but a present-day reality in India's administrative landscape. From automated benefit disbursal systems under the Direct Benefit Transfer (DBT) program to AI-powered surveillance and predictive policing, the state increasingly relies on digital technologies to augment decision-making. While these innovations offer promises of speed, efficiency, and impartiality, they also introduce novel challenges to accountability, transparency, and procedural fairness - cornerstones of administrative law.

This paper has shown that traditional administrative principles such as Audi Alteram Partem, reasonableness, and non-arbitrariness are being tested in new ways due to the increasing delegation of discretion to algorithms. Systems powered by opaque machine learning models often make decisions that are neither intelligible nor easily reviewable, thereby threatening the constitutional safeguards guaranteed under Articles 14 and 21 of the Indian Constitution. Moreover, the administrative machinery lacks the techno-legal capacity to audit or question such decisions effectively.

Judicial responses, as examined through cases like Internet Freedom Foundation v. Union of India, Saurabh Sharma v. SDM, and others, indicate a growing awareness of the risks posed by unregulated automation. However, Indian jurisprudence is still in the early stages of articulating

[59] The Digital Personal Data Protection Act, 2023, Ministry of Law and Justice, Government of India.
[60] Arghya Sengupta & Shruti Vidyasagar, "A Constitutional Framework for Algorithmic Decision-Making in India," *Vidhi Centre for Legal Policy* (2022).

doctrinal clarity on the standards that should govern algorithmic decision-making. Current legislation such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 offers only fragmented safeguards.

In moving forward, there is a pressing need to codify legal standards for algorithmic governance. These should include:

1. Algorithmic Transparency: All government-deployed algorithms should be subject to public disclosure obligations, at least in terms of basic functionality and intended outcomes.
2. Right to Explanation and Appeal: Citizens must have the right to understand how a decision was made and contest it before an impartial forum.
3. Human-in-the-Loop Protocols: High-impact decisions affecting rights, liberties, or entitlements must involve human oversight and discretion to ensure accountability.
4. Algorithmic Impact Assessments (AIAs): Inspired by models in Canada and the EU, India should institutionalize pre-deployment impact assessment frameworks to evaluate risks to fairness, bias, and legality.

Importantly, capacity-building is as crucial as regulation. Administrators, judges, and oversight bodies must be trained to understand the logic and limitations of AI systems. A collaborative ecosystem involving technologists, lawyers, ethicists, and civil society must be encouraged to co-create standards and monitor their implementation.

Furthermore, administrative law must embrace adaptive and anticipatory governance models. Instead of reacting to failures, laws must be forward-looking, resilient to rapid technological changes, and designed with constitutional values as their foundation.

In sum, algorithmic governance presents a paradigm shift in the exercise of administrative discretion. If India fails to equip its legal frameworks to regulate these tools, it risks automating injustice rather than enhancing justice. The challenge lies not in resisting technology but in shaping it through a robust rule-of-law architecture that secures fairness, transparency, and dignity for every citizen.