(JOINT JURIST)

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL]

| VOLUME 1 | ISSUE 1 | MAY 2026

ABOUT THE JOURNAL

The **Joint Jurist** is a strictly law-focused national publication designed to bridge the gap between academic research and litigation expertise. We operate on a **Double-Blind Peer-Review** model, ensuring that every published work meets the highest standards of original scholarship and academic integrity. Our platform is dedicated to providing an openaccess environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **Dr. Seema Gupta**
- **Dr. Mohd Rafiq**
- **Dr. Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**

NAME	DESIGNATION	INSTITUTION/AFFILIATION	SPECIALIZATION & IMPACT
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	**High Court of Himachal Pradesh**	IPR Specialist, Courtroom Strategy & Legal Research.
Prof. (Dr.) Seema Gupta	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**	Constitutional Law, IPR, & Supreme Court Certified Mediator/ Interdisciplinary Legal Studies.

| VOLUME 1 | ISSUE 1 | MAY 2026

"THE RULE OF LAW IN THE ALGORITHMIC STATE: CONSTITUTIONAL CHALLENGES OF AI-BASED ADMINISTRATIVE DECISION-MAKING IN INDIA"

AUTHOR: AYUSHI OJHA, LL.B. ICFAI UNIVERSITY DEHRADUN, LL.M. NLU KOCHI, PG DIPLOMA NLU LUCKNOW

Abstract

The integration of artificial intelligence (AI) into governance systems represents a profound transformation in the structure and functioning of modern administrative states. Algorithmic systems are increasingly being deployed in critical areas such as welfare delivery, taxation, policing, immigration control, and regulatory decision-making. While these technologies promise efficiency, speed, and data-driven precision, they simultaneously raise significant constitutional concerns relating to transparency, accountability, fairness, and due process.

This paper examines the rise of algorithmic governance through the normative framework of the Rule of Law, arguing that the opacity and complexity of AI-driven decision-making systems pose a direct challenge to foundational constitutional principles under Articles 14, 19, and 21 of the Constitution of India. It highlights how automated and data-driven processes may result in arbitrariness, exclusion errors, and a lack of intelligible reasoning, thereby weakening procedural safeguards that traditionally govern administrative action.

The paper further critically analyses the limitations of India's existing legal framework, particularly the Digital Personal Data Protection Act, 2023, in addressing issues of algorithmic accountability, explainability, and state responsibility. In doing so, it identifies a significant regulatory gap in the governance of automated public decision-making systems.

Drawing comparative insights from the European Union's Artificial Intelligence Act, United States administrative law jurisprudence, and OECD ethical principles on artificial intelligence, the paper argues for the development of a structured and rights-based regulatory framework. Such a framework must incorporate algorithmic transparency, independent audit mechanisms, enforceable accountability standards, and mandatory human oversight in high-impact decisionmaking processes.

The paper concludes that while AI has the potential to significantly enhance administrative efficiency and governance capacity, its deployment must remain firmly within constitutional limits. Without adequate safeguards, there is a risk of the emergence of an opaque and unaccountable "black box" governance system that undermines the core values of constitutional democracy and the Rule of Law.

Keywords: Algorithmic Governance, Rule of Law, Artificial Intelligence Regulation, Constitutional Law in India, Administrative Accountability, Digital Governance

1. Introduction

The increasing deployment of AI in governance marks a structural transformation in the nature of the modern administrative state. Traditionally, public administration in constitutional democracies has been premised on human agency, where officials exercise discretion within a framework of statutory authority, constitutional limitations, and principles of natural justice. This structure ensures accountability, reasoned decision-making, and effective judicial review.

However, with the rise of algorithmic governance, decision-making is increasingly mediated through computational systems, including machine learning models, predictive analytics tools, and automated classification systems. These systems are now deployed in welfare administration, taxation, policing, immigration control, surveillance mechanisms, and regulatory enforcement.

In India, the integration of digital governance systems such as Aadhaar-based authentication, DBT, GSTN, FASTag systems, and emerging facial recognition technologies demonstrates a significant shift towards data-driven governance. While these systems are often justified on grounds of efficiency, transparency, and reduction of corruption, they simultaneously raise critical constitutional concerns regarding accountability, arbitrariness, and procedural fairness.

The central constitutional issue is whether decisions that directly affect fundamental rights can be delegated to systems that are incapable of providing intelligible reasons for their outcomes. This question lies at the intersection of administrative law and constitutional theory, particularly under Articles 14, 19, and 21 of the Constitution of India.

This paper argues that algorithmic governance must be understood not merely as a technological development but as a constitutional phenomenon requiring doctrinal regulation under the Rule of Law.

2. Conceptual Foundations of Algorithmic Governance

Algorithmic governance refers to the use of computational systems to assist or replace human decision-making in administrative processes. These systems operate through statistical inference rather than normative legal reasoning, relying on datasets to identify patterns and generate predictions.

Unlike traditional governance systems based on legal interpretation and human discretion, algorithmic systems function through probabilistic modelling. This marks a shift from normative reasoning to data-driven computation, fundamentally altering the epistemology of administrative decision-making.

Frank Pasquale describes this transformation as the emergence of a black box society, where decisions affecting individuals are generated through opaque systems that resist meaningful scrutiny.[1] Lawrence Lessig's proposition that "code is law" further highlights how software architecture increasingly determines regulatory outcomes.[2] It means software and computer code regulate people's behaviour just like legal rules do in the real world.

Algorithmic governance therefore represents not simply administrative reform, but a redistribution of decision-making authority from human actors to computational systems.

3. Rule of Law in the Algorithmic State

The Rule of Law is a foundational principle of constitutional governance. A.V. Dicey's classical formulation emphasises the supremacy of law, equality before law, and the absence of arbitrary power.[3] However, modern constitutional thought, particularly Joseph Raz's theory, expands the concept to include requirements of clarity, accessibility, and predictability of law.[4] Algorithmic governance challenges each of these dimensions.

3.1 Legality and Delegation of Power

In administrative law, delegation of power must be accompanied by clear statutory guidance. In *Ajoy Kumar Banerjee v Union of India*, the Supreme Court held that essential legislative functions cannot be delegated without adequate safeguards.[5] Algorithmic systems, however, often exercise quasi-decisional authority without explicit statutory frameworks governing their operation.

3.2 Transparency and Reasoned Decision-Making

A key requirement of administrative law is that decisions must be reasoned. In *S.N. Mukherjee v Union of India*, the Supreme Court held that recording reasons is an essential component of fairness and judicial review.[6] Algorithmic systems challenge this requirement because their outputs are often not explainable in human terms, particularly in machine learning models.

3.3 Equality and Non-Arbitrariness

Article 14 has been interpreted to prohibit arbitrariness in state action. In *E.P. Royappa v State of Tamil Nadu*, the Court held that arbitrariness is antithetical to equality.[7] Algorithmic systems, however, may produce discriminatory outcomes due to biased datasets, even in the absence of intentional discrimination.

4. Article 21: Due Process, Privacy, and Algorithmic Governance

Article 21 of the Constitution of India guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. Over time, judicial interpretation has transformed this provision into the most expansive guarantee of substantive due process within Indian constitutional law.

In *Maneka Gandhi v Union of India*, the Supreme Court held that the procedure under Article 21 must be "just, fair and reasonable" and not arbitrary or oppressive.[8] This judgment fundamentally redefined procedural fairness in Indian constitutional jurisprudence and remains central to evaluating state action in modern administrative systems.

With the rise of algorithmic governance, the scope of Article 21 has expanded further into domains involving digital identity, automated decision-making, and surveillance systems. The constitutional requirement of fairness is increasingly tested in situations where decisions are generated through opaque computational systems rather than human reasoning.

5. **Privacy and the Constitutional Limits of Data-Driven Governance**

The recognition of privacy as a fundamental right in *Justice K S Puttaswamy v Union of India* marked a watershed moment in Indian constitutional law. The Supreme Court held that privacy is intrinsic to life and personal liberty under Article 21 and is grounded in dignity, autonomy, and informational self-determination.[9] The Court further emphasised that any intrusion into privacy must satisfy the tests of legality, necessity, and proportionality. This doctrine has significant implications for algorithmic governance, as such systems rely heavily on large-scale data collection, profiling, and behavioural analysis.

Algorithmic governance systems, by design, require continuous processing of personal data. This raises concerns regarding:

- mass surveillance
- behavioural profiling
- lack of informed consent
- secondary use of data beyond original purpose

These concerns are amplified when data is processed through automated systems that generate decisions affecting welfare eligibility, law enforcement profiling, or access to public services.

6. **Aadhaar and Algorithmic Identity Infrastructure**

The Aadhaar framework represents one of the most extensive biometric identification systems globally and forms the backbone of India's digital governance infrastructure. In *K S Puttaswamy v Union of India*, the Supreme Court upheld the constitutional validity of the Aadhaar scheme while imposing specific limitations on its use, particularly in relation to private-sector linking and proportionality concerns.[10]

The shift from documentary identity to biometric authentication alters the traditional relationship between citizen and state. Despite judicial safeguards, concerns persist regarding exclusion errors arising from biometric authentication failures. Individuals engaged in manual labour, elderly citizens, and persons with worn fingerprints often face authentication failures, resulting in denial of welfare entitlements.

Such exclusion is constitutionally significant because it directly impacts the right to life and dignity under Article 21. In *Olga Tellis v Bombay Municipal Corporation*, the Court recognised that the right to livelihood is an integral component of the right to life.[11] Therefore, technological exclusion that deprives individuals of essential welfare benefits raises serious constitutional concerns.

In addition, Aadhaar operates as an example of what may be described as **a**lgorithmic identity infrastructure, where identity is not only verified but also continuously processed through automated systems across multiple platforms. This transforms identity into a dynamic, systemdependent construct rather than a purely legal or documentary status. Thus, while Aadhaar has strengthened administrative efficiency and reduced certain forms of fraud, it has simultaneously introduced new constitutional challenges relating to exclusion, data protection, and algorithmic dependence in governance systems.

7. Algorithmic Exclusion and Structural Harm

A key feature of algorithmic governance is that the harm it causes is usually systemic rather than personal. Unlike traditional administrative decisions, which can be linked to a specific officer or authority, algorithmic harm often comes from how the system is designed, the data it uses, and the way it processes information automatically.

This results in what may be described as structural constitutional harm, where:

- there is no explicit decision-maker
- reasons for exclusion are not disclosed
- remedies are procedurally unclear
- accountability is diffused across institutions and systems

Such harm is particularly evident in welfare delivery systems relying on Direct Benefit Transfer mechanisms, where data mismatches and authentication failures may lead to denial of entitlements without formal rejection orders.

8. Surveillance, Predictive Systems, and Article 21 Concerns

Algorithmic governance extends well beyond welfare administration and is increasingly embedded in domains such as law enforcement, criminal justice, and state surveillance. Advanced technologies including facial recognition systems, predictive policing tools, and automated risk-assessment models are now being deployed to identify individuals, detect patterns of behaviour, assess potential threats, and assist investigative decision-making by law enforcement agencies.

While these technologies are often justified on the grounds of efficiency and enhanced security, they raise significant constitutional and legal concerns. One major issue is the risk of false positives and false negatives, where individuals may be wrongly identified as suspects or highrisk persons due to algorithmic error. In addition, these systems often reflect embedded demographic bias, as they are trained on historical data that may already contain structural inequalities.

In *Kharak Singh v State of Uttar Pradesh*, the Supreme Court recognised that surveillance activities can infringe upon personal liberty and dignity.[12] Modern algorithmic surveillance systems intensify these concerns due to their scale, automation, and continuous data processing capabilities.

The constitutional concern, therefore, is not confined merely to instances of direct rights violations but extends to the broader impact such systems have on civil liberties in practice. The pervasive presence of algorithmic surveillance can reshape the relationship between the individual and the State by normalising constant monitoring as a routine feature of governance. This may gradually alter behavioural patterns, as individuals begin to adjust their actions in anticipation of being observed or assessed by automated systems. In this sense, the impact of algorithmic surveillance lies not only in identifiable harm but also in its subtle influence on autonomy, privacy, and the overall exercise of constitutional freedoms within a democratic society.

9. Procedural Fairness and Automated Decision-Making

Procedural fairness under Indian administrative law requires notice, hearing, and reasoned decision-making. However, algorithmic systems challenge each of these requirements.

In automated systems:

- notice may not be provided in meaningful form
- hearings may not be effective without access to algorithmic logic
- reasons may be non-intelligible or statistically framed

This creates a gap between formal procedural compliance and substantive fairness.

The absence of explainability in algorithmic decision-making therefore raises serious concerns under both Article 14 and Article 21.

10. India's Legal and Regulatory Framework: A Fragmented Approach

Despite the rapid expansion of algorithmic governance in India, there is no dedicated, comprehensive statutory framework regulating the use of artificial intelligence in public administration. Instead, the regulatory landscape remains fragmented across general technology law, data protection legislation, and policy-level documents.

The Information Technology Act, 2000 primarily governs cyber activities, electronic records, and intermediary liability. However, it was enacted in a pre-AI era and does not address algorithmic decision-making, automated administrative action, or transparency obligations for computational systems used by the State.

Similarly, the Digital Personal Data Protection Act, 2023 regulates personal data processing but does not impose substantive obligations regarding explainability, algorithmic transparency, or accountability in automated decision-making systems. It focuses on consent and data processing principles but remains silent on how data-driven decisions affecting rights are generated and justified.

11. Policy-Based Governance and Its Limitations

India's approach to artificial intelligence governance is largely policy-driven rather than rooted in binding legislation, reflecting an early-stage regulatory framework that prioritises innovation over enforceable legal safeguards. The NITI Aayog's National Strategy for Artificial Intelligence serves as the primary guiding document in this area and promotes the adoption of AI across key sectors such as healthcare, agriculture, education, smart cities, infrastructure, and public governance. The strategy envisions AI as a tool for economic growth and social transformation, often describing it in terms of "inclusive growth" and "responsible innovation."

However, While the strategy emphasises innovation, inclusivity, and economic growth, it does not establish enforceable rights, statutory safeguards, or institutional accountability mechanisms for algorithmic systems deployed by the State.[13] It also fails to establish statutory safeguards addressing key concerns such as transparency in algorithmic decision-making, accountability for automated outcomes, or procedural protections for individuals affected by such systems. Furthermore, there is no dedicated institutional mechanism tasked with auditing, regulating, or independently reviewing algorithmic systems used by the State. The absence of

enforceable standards results in a regulatory gap between technological deployment and constitutional accountability.

As a result, AI governance in India currently operates primarily through soft law instruments, including policy reports, ethical guidelines, and advisory frameworks. These instruments, while useful in shaping discourse and encouraging best practices, lack binding force, enforceability, and direct judicial oversight. Consequently, individuals affected by algorithmic decisions often have limited legal recourse, as courts can only indirectly engage with such systems through existing constitutional or administrative law principles.

This reliance on non-binding frameworks creates a significant regulatory gap, particularly in high-impact domains where algorithmic decisions may affect fundamental rights such as access to welfare benefits, privacy, and equality before law. It also raises broader concerns regarding institutional accountability, as responsibility for algorithmic outcomes remains diffused across policymakers, implementing agencies, and private technology providers.

12. **Administrative Law and the Breakdown of Reasoned Decision-Making**

A foundational principle of Indian administrative law is that state decisions affecting rights must be reasoned. In *S N Mukherjee v Union of India*, the Supreme Court held that recording reasons is an essential component of natural justice and enables effective judicial review.[14]

Algorithmic systems, however, disrupt this principle because their outputs are often:

- probabilistic rather than reasoned
- generated through non-intelligible computational processes
- dependent on machine learning models that do not produce human-readable justification

This creates a situation where administrative decisions are functionally binding but epistemically opaque.

The absence of intelligible reasoning undermines the ability of affected individuals to challenge decisions, thereby weakening judicial review under Articles 32 and 226 of the Constitution.

13. **Accountability Vacuum and Responsibility Fragmentation**

Algorithmic governance introduces a structural challenge to traditional accountability frameworks. In conventional administrative systems, responsibility can be traced to identifiable officials or departments. However, in algorithmic systems, decision-making is distributed across multiple actors, including:

- government agencies deploying AI systems
- private vendors designing algorithms
- data scientists training machine learning models
- automated systems generating outputs

This diffusion creates what scholars describe as a responsibility gap, where no single actor can be held fully accountable for outcomes produced by algorithmic systems.

From a constitutional perspective, this undermines the principle of accountability, which is essential to the Rule of Law.

14. Judicial Review in the Algorithmic Context

Judicial review under Articles 32 and 226 is a cornerstone of Indian constitutionalism. However, algorithmic governance creates new challenges for courts.

First, opacity in algorithmic systems limits the ability of courts to assess the reasoning behind decisions. Second, proprietary algorithms used by private vendors may restrict disclosure of system logic. Third, technical complexity may hinder meaningful judicial scrutiny.

As a result, judicial review risks being reduced to procedural review rather than substantive examination of decision-making logic.

This raises a serious constitutional concern that whether traditional judicial mechanisms are sufficient to regulate algorithmic administrative action.

15. Comparative Context: Emerging Global Regulatory Responses

Globally, jurisdictions are beginning to address algorithmic governance through structured regulatory frameworks. The European Union Artificial Intelligence Act represents the most comprehensive attempt to regulate AI systems through a risk-based approach. The EU framework classifies AI systems into different risk categories and imposes stricter obligations on high-risk systems, including transparency requirements, human oversight, and conformity assessments.[15]

International organisations such as the OECD and UNESCO have also developed ethical frameworks emphasising transparency, accountability, fairness, and human-centred AI governance.[16] These frameworks, although non-binding, reflect an emerging global consensus that algorithmic systems must be governed by rights-based principles.

15.1 European Union: The Artificial Intelligence Act and Risk-Based Regulation

The European Union Artificial Intelligence Act (EU AI Act) represents the most developed and comprehensive attempt to regulate artificial intelligence through a binding legislative framework. It adopts a risk-based regulatory model, distinguishing AI systems according to the level of risk they pose to fundamental rights and public safety.

Under this framework, AI systems are classified into four categories: unacceptable risk, highrisk, limited risk, and minimal risk. High-risk systems include those used in areas such as employment, credit scoring, biometric identification, law enforcement, and public administration.

High-risk systems are subject to stringent regulatory obligations, including:

- mandatory risk assessments prior to deployment
- transparency and documentation requirements
- human oversight obligations
- conformity assessments and post-market monitoring

The significance of the EU approach lies in its preventive orientation. Instead of addressing harm after it occurs, the framework regulates AI systems ex ante, thereby embedding accountability into system design itself.[17]

This model is particularly relevant for India, where algorithmic systems are often deployed without prior impact assessment or statutory safeguards.

16. **United States: Algorithmic Decision-Making and Due Process Concerns**

In the United States, AI regulation is less centralised, but constitutional litigation has raised important concerns regarding algorithmic decision-making, particularly in criminal justice contexts.

One of the most discussed cases is *State v Loomis*, where the Wisconsin Supreme Court upheld the use of a proprietary risk assessment algorithm in sentencing decisions. The Court acknowledged concerns regarding transparency and due process, but ultimately allowed its use, noting that it was one factor among many in sentencing.[18] However, this case also highlighted a critical constitutional tension: the inability of defendants to meaningfully challenge algorithmic reasoning due to proprietary protection of the software.

In addition, the US Supreme Court in *Mathews v Eldridge* established a balancing test for procedural due process, weighing private interests, risk of erroneous deprivation, and governmental interest.[19] This framework is particularly relevant for algorithmic governance systems, where the risk of erroneous deprivation increases due to automated classification and predictive modelling.

Similarly, in *Carpenter v United States*, the Court recognised that digital surveillance and data aggregation raise serious Fourth Amendment concerns, reinforcing the idea that technological systems can significantly expand state power over individuals.[20]

This raises serious due process concerns under the Fourteenth Amendment, particularly where algorithmic tools influence liberty-depriving decisions without full disclosure of their functioning.

The broader US debate reflects a growing concern that algorithmic governance may create "due process opacity," where individuals are subject to decisions they cannot effectively contest.

17. **Algorithmic Bias and Discrimination in Computational Systems**

A central concern in algorithmic governance is the risk of embedded bias within computational systems. Unlike traditional forms of discrimination, which are often intentional, visible, or attributable to specific decision-makers, algorithmic bias tends to be structural in nature. It arises not from deliberate exclusion but from the way data is collected, the assumptions embedded in system design, and the modelling choices made during algorithm development.

Such bias may enter algorithmic systems in multiple ways. It can originate from historical datasets that already reflect existing social and economic inequalities, thereby reproducing past discrimination in present decision-making. It may also arise through the use of proxy variables that indirectly capture protected characteristics such as caste, gender, or race. In many cases, underrepresentation of certain groups in training data further skews outcomes, making the

system less accurate or fair for those populations. Additionally, optimisation goals that prioritise efficiency, speed, or cost reduction over fairness can unintentionally reinforce unequal treatment across different groups.

This leads to what scholars describe as "disparate impact," where algorithmic systems produce unequal or adverse outcomes for certain groups even in the absence of explicit discriminatory intent. From a constitutional perspective, this raises concerns under equality doctrines, particularly where state-deployed systems disproportionately affect marginalised or vulnerable communities.

Algorithmic discrimination becomes especially significant in high-impact domains such as predictive policing systems, welfare eligibility determination, employment screening, and credit scoring mechanisms. In these contexts, automated decisions can directly influence access to liberty, livelihood, and essential public services. As a result, such systems risk reinforcing and amplifying existing structural inequalities while simultaneously presenting themselves as neutral, objective, and data-driven.

18. **Theoretical Foundations: Code, Power, and Governance**

The rise of algorithmic governance has been extensively analysed in legal theory. Lawrence Lessig's proposition that "code is law" remains central to understanding how digital architecture regulates behaviour in modern societies.[21] In this framework, software design becomes a form of regulatory power, shaping outcomes in ways that resemble legal norms but operate outside traditional democratic oversight.

Similarly, Frank Pasquale's concept of non-transparent computational decision-making structures highlights how algorithmic systems concentrate informational and decisional power in opaque institutional structures, making meaningful accountability difficult.[22]

These theories collectively suggest that algorithmic governance represents a shift from law as text to law as system architecture.

19. **Towards a Doctrinal Synthesis: Rule of Law in the Algorithmic State**

The Rule of Law, in its classical formulation, requires that state power be exercised through transparent, predictable, and reviewable processes. However, algorithmic governance introduces a structural transformation where decision-making is:

- automated rather than discretionary
- opaque rather than reasoned
- distributed rather than centralised

This challenges traditional legal doctrines in three key ways: First, legality becomes difficult to assess when decision-making is embedded within computational systems rather than explicit administrative orders. Second, accountability becomes fragmented across institutions, reducing the ability to assign responsibility. Third, reviewability becomes constrained due to the technical opacity of algorithmic systems.

Despite these challenges, constitutional principles remain adaptable. The Rule of Law must evolve to include not only legal rules but also computational governance structures that determine how those rules are applied.

20. Constitutional Synthesis: Articles 14, 19 and 21 in the Algorithmic State

The constitutional impact of algorithmic governance in India must ultimately be assessed through the triad of Articles 14, 19, and 21, which collectively form the golden triangle of fundamental rights.

Article 14, through judicial interpretation, prohibits arbitrariness in state action. In *E.P. Royappa v State of Tamil Nadu*, the Supreme Court held that arbitrariness is antithetical to equality.[23] Algorithmic systems, however, introduce a form of structural arbitrariness, where unequal outcomes arise not from intentional discrimination but from data-driven design, proxy variables, and historical bias embedded within datasets.

Article 21, as interpreted in *Maneka Gandhi v Union of India*, requires that any deprivation of life or liberty must follow a procedure that is just, fair, and reasonable.[2] In algorithmic systems, procedural fairness is compromised where decisions are automated, non-transparent, and not accompanied by intelligible reasoning.

Further, the right to privacy recognised in *Justice K.S. Puttaswamy v Union of India* reinforces that dignity, autonomy, and informational control are central to constitutional governance.[24] Algorithmic systems that rely on large-scale data processing must therefore satisfy constitutional standards of legality, necessity, and proportionality.

Article 19, particularly freedoms of speech, movement, and association, is also implicated through algorithmic surveillance systems that create behavioural monitoring environments, resulting in a chilling effect on constitutional freedoms.

21. Structural Harm and the Transformation of Constitutional Injury

Traditional constitutional violations are typically identifiable, attributable, and reversible through judicial remedies. Algorithmic governance, however, produces structural harm, which is:

- distributed across systems rather than individuals
- embedded in data architecture rather than discrete decisions
- continuous rather than episodic
- difficult to attribute to a single decision-maker

This transformation challenges the remedial structure of constitutional law, particularly under Articles 32 and 226, which depend on identifiable state action.

In algorithmic governance, harm often manifests as exclusion, denial of services, or surveillance without formal administrative orders, thereby complicating judicial intervention.

22. Toward a Rights-Based Framework for Algorithmic Governance

A constitutionally compliant framework for algorithmic governance must be grounded in enforceable legal safeguards rather than relying solely on policy guidance or ethical principles. This is because digital systems increasingly perform regulatory functions that directly influence

rights and entitlements, effectively shaping behaviour in a manner similar to formal law. In this context, Lawrence Lessig's proposition that "code is law" becomes particularly relevant, as it highlights how software architecture and system design can regulate conduct without the visibility or procedural safeguards associated with traditional legal norms. Similarly, Frank Pasquale's concept of the black box society draws attention to closed algorithmic architectures, where decision-making processes are often inaccessible, unexplainable, and difficult to scrutinise, thereby weakening institutional accountability.

These theoretical perspectives collectively underscore the necessity of embedding robust safeguards within any regulatory framework governing algorithmic systems. Such safeguards should include a legally recognised right to explanation for individuals affected by automated decisions, ensuring that outcomes are intelligible and capable of being meaningfully challenged. In addition, algorithmic transparency is essential to ensure that the logic, scope, and impact of such systems are not entirely concealed from public and judicial scrutiny. This must be complemented by meaningful human oversight in high-impact decision-making processes to prevent complete delegation of authority to automated systems. Finally, independent audit mechanisms are required to periodically assess the fairness, reliability, and constitutional compliance of algorithmic tools deployed in governance.

Moreover, Comparative frameworks such as the European Union's Artificial Intelligence Act demonstrate the importance of structured regulatory oversight, particularly for high-risk systems.[25] International standards developed by organisations such as the OECD and UNESCO further emphasise transparency, fairness, and accountability in AI governance.[26]

India must adopt a similar institutional approach to ensure constitutional compliance.

23. **Balancing Innovation with Constitutionalism**

The regulation of algorithmic governance must strike a balance between innovation and accountability. While technological development is essential, it must operate within constitutional limits.

Unchecked algorithmic systems risk undermining fundamental rights, whereas well-regulated systems can enhance governance without compromising legality.

CONCLUSION

Algorithmic governance marks a major shift in the functioning of the modern administrative state by replacing human decision-making with automated, data-driven systems. While this improves efficiency and speed in governance, it also raises serious constitutional concerns relating to transparency, accountability, and fairness.

This paper has shown that the increasing use of artificial intelligence in governance challenges the Rule of Law, particularly under Articles 14, 19, and 21 of the Constitution of India. The opacity of algorithmic systems often makes it difficult to understand how decisions are made or to effectively challenge them, leading to risks of arbitrariness and exclusion.

Despite its potential benefits, India's current legal framework remains inadequate to address the complexities of AI-driven governance. Comparative developments in jurisdictions such as the European Union and the United States highlight the need for stronger safeguards, including transparency requirements, human oversight, and accountability mechanisms.

The paper therefore argues for a structured regulatory approach that includes algorithmic transparency, independent audits, and meaningful human intervention in high-impact decisions. These safeguards are essential to ensure that technological advancement does not undermine constitutional values.

Ultimately, while AI can enhance governance efficiency, it must remain firmly within constitutional limits to preserve fairness, accountability, and the Rule of Law in a digital state.

LIST OF ABBREVIATIONS

- AI - Artificial Intelligence
- AIA - Algorithmic Impact Assessment
- AIA Act - Artificial Intelligence Act (European Union)
- Aadhar Act- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
- - Article (of the Constitution of India)
- API - Application Programming Interface
- DBT - Direct Benefit Transfer
- EU - European Union
- GSTN - Goods and Services Tax Network
- HITL - Human-in-the-Loop
- IT Act - Information Technology Act, 2000
- OECD - Organisation for Economic Co-operation and Development
- SC - Supreme Court of India
- UNESCO - United Nations Educational, Scientific and Cultural Organization
- UK - United Kingdom
- US - United States

TABLE OF CASES India

- Ajoy Kumar Banerjee v Union of India (1984) 3 SCC 127
- E P Royappa v State of Tamil Nadu (1974) 4 SCC 3
- Justice K S Puttaswamy v Union of India (2017) 10 SCC 1
- K S Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1
- Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295
- Maneka Gandhi v Union of India (1978) 1 SCC 248
- Olga Tellis v Bombay Municipal Corporation (1985) 3 SCC 545
- S N Mukherjee v Union of India (1990) 4 SCC 594

United States

- State v Loomis 881 NW 2d 749 (Wis 2016)
- *Mathews v Eldridge* 424 US 319 (1976)
- *Carpenter v United States* 585 US (2018)

TABLE OF STATUTES / LEGISLATION

- Constitution of India 1950
- Information Technology Act 2000
- Digital Personal Data Protection Act 2023
- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016
- European Union Artificial Intelligence Act (Draft Proposal) COM/2021/206 final

INTERNATIONAL INSTRUMENTS / POLICIES

- OECD Principles on Artificial Intelligence (2019)

UNESCO Recommendation

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

[2] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

[3] AV Dicey, *Introduction to the Study of the Law of the Constitution* (10th edn, Macmillan 1959).

[4] Joseph Raz, 'The Rule of Law and Its Virtue' (1977) 93 *Law Quarterly Review* 195.

[5] *Ajoy Kumar Banerjee v Union of India* (1984) 3 SCC 127.

[6] *S N Mukherjee v Union of India* (1990) 4 SCC 594.

[7] *E P Royappa v State of Tamil Nadu* (1974) 4 SCC 3.

[8] *Maneka Gandhi v Union of India (1978) 1 SCC 248.*

[9] *Justice KS Puttaswamy v Union of India* (2017) 10 SCC 1.

[10] *K S Puttaswamy (Aadhaar) v Union of India* (2019) 1 SCC 1.

[11] *Olga Tellis v Bombay Municipal Corporation* (1985) 3 SCC 545.

[12] *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.

[13] NITI Aayog, *National Strategy for Artificial Intelligence* (Government of India 2018).

[14] *S N Mukherjee v Union of India* (1990) 4 SCC 594.

[15] European Commission, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* COM/2021/206 final.

[16] OECD, *OECD Principles on Artificial Intelligence* (OECD 2019); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

[17] European Commission, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* COM/2021/206 final.

[18] *State v Loomis* 881 NW 2d 749 (Wis 2016).

[19] *Mathews v Eldridge* 424 US 319 (1976).

[20] *Carpenter v United States* 585 US (2018).

[21] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

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

[23] *E P Royappa v State of Tamil Nadu* (1974) 4 SCC 3.

[24] *Justice KS Puttaswamy v Union of India* (2017) 10 SCC 1.

[25] European Commission, *Artificial Intelligence Act Proposal* COM/2021/206 final.

[26] OECD (2019); UNESCO (2021) AI ethics frameworks.