MACHINE-MADE GOVERNANCE:

AI in Administrative Decision-Making

A Legal and Constitutional Analysis with Reference to India

[Author Hemasuruthi A S]
[The TamilNadu Dr Ambedkar law University]

ABSTRACT

Artificial Intelligence (AI) is becoming an important part of modern governance and administrative decision-making. Governments around the world are increasingly using AI technologies in areas such as public welfare schemes, taxation, policing, healthcare administration, digital surveillance, and policy implementation. In India, initiatives like Digital India have encouraged the use of digital technologies to improve governance and make public services faster and more efficient. AI helps authorities process large amounts of data quickly, reduce administrative delays, and improve the overall functioning of government institutions. At the same time, the growing use of AI in governance raises several legal and constitutional concerns. Decisions made through automated systems may sometimes lack transparency and human involvement, which can affect important principles of administrative law such as fairness, accountability, and natural justice. There is also a risk of algorithmic bias, misuse of personal data, and invasion of privacy. These concerns become more significant in light of Article 14 and Article 21 of the Constitution of India, which guarantee equality before law and protection of life and personal liberty. In addition, laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 play an important role in regulating digital governance and data protection. This paper examines the concept of machine-made governance and studies the role of AI in administrative decision-making from a legal perspective. It analyses the benefits and challenges of AI in governance and evaluates whether the existing legal framework in India is adequate to regulate AI-driven administration. The study concludes that while AI can improve efficiency and public service delivery, its use must be balanced with transparency, accountability, ethical regulation, and protection of fundamental rights.

Keywords: *Artificial Intelligence, Machine-Made Governance, Administrative DecisionMaking, Digital Governance, Constitutional Rights.*

I. Introduction

The emergence of Artificial Intelligence (AI) as a tool of governance represents one of the most profound transformations in the history of public administration. Across the world, governments are no longer merely using technology to record or store information — they are using it to *decide*. Automated systems now determine who receives welfare benefits, whose tax return is flagged for audit, which individual is identified as a security risk, and how scarce public resources are allocated. India is no exception to this global trend. The *Digital India* programme, launched in 2015, has accelerated the integration of digital and AI technologies into governmental functions at both the central and state levels.[1]

The promise of AI in governance is significant. Automated systems can process data at a scale and speed that no human administrator could match. They can reduce corruption by removing discretion from vulnerable decision points, ensure greater consistency in the application of rules, and make public services more accessible — particularly to citizens in remote areas who have historically been excluded from efficient administrative delivery. The Aadhaar biometric identification system, the Goods and Services Tax (GST) Network, and the FASTag highway toll system are examples of digital platforms that have meaningfully improved administrative efficiency in India.[2]

However, AI-driven governance raises fundamental legal and constitutional questions that have not yet received adequate attention in Indian administrative law scholarship. When a machine makes a decision that affects a citizen's rights, is that decision compatible with the requirements of natural justice? Does it satisfy the constitutional guarantees of equality under *Article 14* and personal liberty under *Article 21* of the Constitution of India? Who bears legal accountability when an automated system causes harm? These questions are urgent, and this paper attempts to answer them.[3]

This paper proceeds as follows. Section II provides an overview of AI in Indian governance. Section III analyses the constitutional and statutory framework applicable to algorithmic administrative decisions. Section IV examines the principal legal challenges. Section V evaluates the adequacy of existing law and proposes reforms. Section VI concludes.

II. AI in Indian Governance: An Overview

A. The Digital India Initiative and AI Policy

India's embrace of AI in public administration is driven primarily by the *Digital India* programme and, more recently, the *National Strategy for Artificial Intelligence* released by NITI Aayog in 2018.[4] The NITI Aayog strategy, titled *#AIforAll*, identified five sectors for priority AI application: healthcare, agriculture, education, smart cities and infrastructure, and smart mobility. In the domain of public administration, the strategy envisioned AI as a tool for transforming service delivery, improving tax compliance, and enhancing regulatory enforcement.

By 2024, multiple central government departments had deployed AI and algorithmic tools. The Income Tax Department uses data analytics and machine learning for *Project Insight*, which identifies tax evasion by correlating financial transactions across databases.[5] The Ministry of Home Affairs has explored AI-based facial recognition tools for law enforcement. State governments, including Telangana, Karnataka, and Maharashtra, have piloted AI in land records management, grievance redressal, and agricultural advisory services.

B. Aadhaar and Automated Welfare Administration

The *Aadhaar* system — the world's largest biometric identification system, covering over 1.3 billion individuals — is the most consequential example of algorithmic governance in India. Aadhaar is used as the basis for authentication in the delivery of welfare benefits under schemes such as the Public Distribution System (PDS), the Pradhan Mantri Jan Dhan Yojana, and the National Rural Employment Guarantee Scheme (MGNREGS). Automated authentication failures — caused by biometric mismatches, network errors, or database inconsistencies — have resulted in eligible beneficiaries being denied food, wages, and pensions.[6]

The Supreme Court of India addressed the Aadhaar system in the landmark decision of *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2018) 1 SCC 809, upholding the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, while striking down certain provisions as unconstitutional. The Court's majority held that Aadhaar was a proportionate measure for welfare delivery but imposed significant restrictions on its mandatory use, particularly in the private sector.[7] However, the operational reality of automated exclusion from welfare — what scholars have called 'technological exclusion' — has continued to generate harm for millions of citizens.

III. Constitutional and Statutory Framework

A. Article 14: Equality Before Law and the Prohibition of Arbitrariness

Article 14 of the Constitution of India provides that the State shall not deny to any person equality before the law or equal protection of the laws within the territory of India. The Supreme Court has consistently interpreted Article 14 as embedding not only a prohibition on class discrimination but also a prohibition on *arbitrariness* in State action. In *E.P. Royappa v State of Tamil Nadu*, (1974) 4 SCC 3, the Court held that equality is antithetical to arbitrariness. In *Maneka Gandhi v Union of India*, AIR 1978 SC 597, the Court further held that any law or executive action that is arbitrary is inconsistent with Article 14.[8]

> **Constitution of India, Article 14 — Right to Equality**
> *The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India.*

Algorithmic administrative decisions are susceptible to challenge under Article 14 on two grounds. First, if an automated system produces outcomes that are arbitrary — in the sense of being untethered from the relevant statutory criteria — those decisions will violate Article 14. Second, if the algorithm produces differential outcomes across groups defined by religion, caste, sex, or place of birth without rational justification, it may constitute discriminatory State action. The opacity of many algorithmic systems makes it difficult to assess

either ground, but the constitutional obligation is clear: State action that is arbitrary or discriminatory violates Article 14 regardless of whether it is carried out by a human or a machine.

B. Article 21: Right to Life, Personal Liberty, and the Right to Privacy

Article 21 of the Constitution provides that no person shall be deprived of his life or personal liberty except according to procedure established by law. The Supreme Court has, through a long line of decisions, interpreted Article 21 expansively to encompass the right to livelihood, the right to a fair hearing, and — most significantly for present purposes — the fundamental *right to privacy*.

> **Constitution of India, Article 21 — Protection of Life and Personal Liberty**
> *No person shall be deprived of his life or personal liberty except according to procedure established by law.*

In *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1, a nine-judge bench of the Supreme Court unanimously held that privacy is a fundamental right under Article 21 of the Constitution.[9] The Court identified informational privacy as a core component of the right to privacy, holding that individuals have a constitutionally protected interest in controlling personal data about themselves. AI systems used in governance necessarily involve the collection, processing, and analysis of vast quantities of personal data. Any such processing that is disproportionate to its legitimate aim, or that fails to meet adequate standards of data protection, will violate Article 21.

C. Principles of Natural Justice in Automated Decisions

Indian administrative law recognises two cardinal principles of natural justice: *audi alteram partem* (the right to be heard) and *nemo judex in causa sua* (no one shall be a judge in their own cause). These principles are applied by the courts as implied conditions in the exercise of statutory powers affecting individual rights. In *A.K. Kraipak v Union of India*, AIR 1970 SC 150, the Supreme Court held that natural justice requirements apply to all administrative action that affects the rights or legitimate expectations of individuals.[10]

Automated decisions present a structural challenge to *audi alteram partem*. If a welfare claim is denied by an algorithm without the applicant being informed of the specific adverse inputs or being given an opportunity to respond, the right to be heard has been violated. The challenge is that algorithmic systems typically apply generalised models to datasets — they do not generate individualised reasons that can be communicated to affected persons or contested before a human decision-maker.

D. Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is India's primary statute governing digital transactions and electronic records. Section 79 of the IT Act, as amended in 2008, provides exemptions from liability for intermediaries in respect of third-party content, subject to compliance conditions. More relevant for AI

governance is Section 43A, which imposes liability on corporate bodies holding sensitive personal data for failure to implement reasonable security practices.[11]

> **Information Technology Act, 2000, s 43A — Compensation for Failure to Protect Data**
> *Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.*

The scope of the IT Act is, however, limited when applied to AI governance. The Act was enacted before the era of machine learning and does not specifically address algorithmic decision-making, automated profiling, or the explainability of AI outputs. It imposes no obligation on government bodies to disclose the algorithmic basis of administrative decisions or to provide affected individuals with meaningful redress.

E. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) is India's most significant recent legislative development in the data governance space. The Act establishes a framework for the processing of digital personal data, grounded in principles of purpose limitation, data minimisation, and storage limitation. Section 4 of the DPDPA provides that personal data may be processed only for a lawful purpose for which the data principal has given consent or for certain specified legitimate uses.[12]

> **Digital Personal Data Protection Act, 2023, s 4(1) — Grounds for Processing Personal Data**
> *A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose — (a) for which the Data Principal has given her consent; or (b) for certain legitimate uses, as specified in section 7.*

Section 12 of the DPDPA confers on data principals the right to access information about their personal data and the right to correction. Section 13 provides a right to grievance redressal. Importantly, however, the DPDPA does not — as of its current form — confer an explicit right against solely automated decisions equivalent to Article 22 of the EU General Data Protection Regulation (GDPR). The absence of such a provision is a significant gap in India's data governance framework.[13]

IV. Principal Legal Challenges

A. Opacity, Explainability, and the Duty to Give Reasons

Indian administrative law imposes a duty on administrative authorities to give reasons for decisions that adversely affect individual rights. This duty has been recognised as a component of natural justice and as a

safeguard against arbitrariness. In *S.N. Mukherjee v Union of India*, (1990) 4 SCC 594, the Supreme Court held that the duty to give reasons is a requirement of fairness and that recorded reasons enable judicial review to be effective.[14]

AI systems — particularly those based on machine learning — present a fundamental challenge to this duty. A system that denies a welfare payment, flags a tax return, or recommends a security classification does so by processing hundreds or thousands of variables through statistical models whose internal logic is not interpretable in human terms. An explanation that simply says 'the system determined you are ineligible' does not constitute reasons — it merely states the conclusion. Without the ability to understand the inputs, the model's weighting of those inputs, and the threshold applied, an affected individual cannot meaningfully challenge the decision before an appellate authority or a court.

B. Algorithmic Bias and Article 14

Machine learning systems learn patterns from historical data. Where that data reflects historical patterns of caste discrimination, gender bias, regional inequality, or economic exclusion — as is the case in much of India's administrative history — the algorithm may encode and amplify those patterns in its outputs. An AI system trained to predict creditworthiness, tax compliance, or welfare fraud using data from a society characterised by structural inequality may produce outputs that are facially neutral but discriminatory in effect.[15]

This form of indirect or structural discrimination is difficult to detect without access to the training data, model architecture, and disaggregated output statistics. In India, where socially sensitive data is simultaneously pervasive in administrative datasets and constitutionally protected from use in official classification (Article 15 prohibits discrimination on grounds including caste and religion), the risk of algorithmic bias is particularly acute. There is currently no statutory obligation on Indian government bodies to audit deployed AI systems for discriminatory impact across protected categories.

C. Accountability Deficit and Ultra Vires Action

A foundational principle of Indian administrative law is that all exercises of public power must be authorised by law. Action taken without legal authority is void as *ultra vires*. Most enabling statutes conferring administrative powers on government authorities contemplate decision-making by a human officer — not by an automated system. The question of whether an automated system can lawfully exercise statutory discretion in the absence of express legislative authorisation is unresolved in Indian law.

The Aadhaar authentication failures that resulted in exclusion from welfare schemes provide a concrete illustration. The Aadhaar Act, 2016 authorises the use of Aadhaar for identity verification but does not expressly authorise the automated denial of benefits on the basis of biometric authentication failure. Where such denials occurred, they may not have been authorised by law, potentially rendering them void — yet no effective administrative or judicial mechanism existed to provide timely redress to affected individuals.[16]

D. Data Privacy and Surveillance Risk

AI governance necessarily involves the large-scale collection, integration, and analysis of personal data. The aggregation of data from multiple government databases — tax records, biometric data, health records, travel histories, financial transactions — creates a *surveillance architecture* that poses profound risks to the right to privacy recognised in *Puttaswamy*. The *proportionality* test applied by the Supreme Court in *Puttaswamy* requires that any restriction on privacy must have a legitimate aim, be rationally connected to that aim, and be the least restrictive means of achieving it. Mass data integration for predictive governance may fail this test in many contexts.[17]

V. Evaluating the Legal Framework and Proposed Reforms

A. Adequacy of the Existing Framework

The existing Indian legal framework — the Constitution, the IT Act, the DPDPA, and judge-made administrative law — provides important but insufficient protection against the risks of AI-driven governance. The constitutional guarantees of Articles 14 and 21 are powerful but operate post hoc: they require a citizen to initiate litigation after harm has occurred, a burden that falls most heavily on the poorest and least resourced individuals who are most likely to be harmed by algorithmic governance. The DPDPA establishes data rights but does not specifically address automated decision-making. No Indian statute presently requires algorithmic impact assessments, mandates explainability, or provides a right against solely automated decisions in administrative contexts.

This gap is significant compared to international standards. The EU's Artificial Intelligence Act, 2024 classifies AI systems used in welfare, immigration, and justice administration as 'high risk', subjecting them to mandatory conformity assessments, transparency obligations, and human oversight requirements before deployment. The GDPR's Article 22 confers an explicit right not to be subject to solely automated decisions with significant legal effects. India's framework currently provides neither of these protections.

B. Proposed Statutory Reforms

This paper proposes three targeted statutory reforms, which could be enacted either as amendments to the DPDPA or as a standalone *Algorithmic Accountability in Public Administration Act*.

First, a mandatory *duty of explainability*:

> **Proposed Provision — Duty of Explainability in Automated Administrative Decisions**
> *No public authority shall use an automated or algorithmic system to make or materially inform any administrative decision affecting the rights, entitlements, or obligations of a person under any law for the*

> *time being in force, unless — (a) the system is capable of generating a clear, intelligible, and individualised explanation of the principal factors and their relative weight that determined the output; (b) such explanation is provided in writing to the affected person, in the official language of the State concerned, within fourteen days of the decision; and (c) the explanation discloses the right of the affected person to seek human review under the provisions of this Act.*

Second, a *right to human review*:

> **Proposed Provision — Right to Meaningful Human Review**
> *Any person aggrieved by an administrative decision made or materially informed by an automated system shall have the right to request a review of such decision by a qualified human officer within thirty days of receiving notice of the decision. Such review shall be — (a) conducted by an officer possessing the authority to reverse, vary, or affirm the decision; (b) undertaken on the merits of the individual case and not solely on the basis of the automated output; (c) recorded in writing with reasons; and (d) completed within sixty days of the request. No authority shall establish any policy, target, or incentive that systematically discourages a reviewing officer from departing from automated recommendations.*

Third, a *mandatory algorithmic impact assessment*:

> **Proposed Provision — Algorithmic Impact Assessment**
> *Before deploying any automated system for an administrative purpose specified in the Schedule to this Act, a public authority shall — (a) commission an independent algorithmic impact assessment evaluating the system's potential for discriminatory impact on persons belonging to Scheduled Castes, Scheduled Tribes, Other Backward Classes, women, persons with disabilities, and minorities; (b) ensure that such assessment is conducted by persons qualified in data science and law, independent of the authority and the system's developer; (c) publish the assessment on its official website; and (d) not deploy the system if the assessment identifies discriminatory impact that has not been remediated to the satisfaction of the designated regulatory authority.*

These provisions, taken together, would bring India's regulatory framework for AI in public administration substantially closer to international best practice, while remaining consistent with the constitutional guarantees of Articles 14 and 21 and the principles of natural justice embedded in Indian administrative law.

VI. Conclusion

Machine-made governance is not a distant prospect in India — it is a present reality. From Aadhaar-linked welfare delivery to AI-assisted tax enforcement, automated systems are already making or shaping decisions that determine the life circumstances of hundreds of millions of citizens. The legal and constitutional framework within which these systems operate has not kept pace with the speed of their deployment.

This paper has argued that AI-driven administrative decision-making gives rise to serious legal concerns under Articles 14 and 21 of the Constitution of India, and that existing statutory instruments — the IT Act, 2000 and

the DPDPA, 2023 — do not adequately address those concerns. The principal deficits are the absence of a duty of explainability, the absence of a right to meaningful human review, and the absence of mandatory pre-deployment impact assessment for discriminatory risk. Each of these deficits is capable of being addressed through targeted legislative reform without impeding the legitimate benefits of AI in public administration.

The use of AI in governance is neither inherently good nor inherently bad. Its value depends entirely on the quality of its design, the rigour of its oversight, and the strength of the legal framework within which it operates. A governance system that deploys algorithms without accountability is not more efficient — it is more dangerous. The rule of law demands that even when the State speaks through a machine, it must speak fairly, transparently, and subject to the law. The task for Indian legislators, courts, and policymakers is to ensure that this demand is met.

FOOTNOTES

[1] Ministry of Electronics and Information Technology, 'Digital India: Programme Overview' (Government of India, 2015); NITI Aayog, 'National Strategy for Artificial Intelligence — #AIforAll' (Government of India, 2018).

[2] Unique Identification Authority of India, 'Aadhaar: Transforming Governance' (UIDAI, 2022); see also Reetika Khera (ed), Dissent on Aadhaar: Big Data Meets Big Brother (Orient BlackSwan, 2019).

[3] Upendra Baxi, 'The Rule of Law in India: Theory and Practice' in Randall Peerenboom (ed), Asian Discourses of Rule of Law (Routledge, 2004) 324; see also Constitution of India, arts 14, 21.

[4] NITI Aayog, 'National Strategy for Artificial Intelligence' (2018) <https://niti.gov.in> accessed 15 April 2026.

[5] Income Tax Department, 'Project Insight' (Government of India, 2017); Central Board of Direct Taxes, Annual Report 2022–23 (Ministry of Finance, 2023).

[6] Jean Dreze and Reetika Khera, 'Aadhaar Failures: A Tragedy of Errors' (2017) 52(10) Economic and Political Weekly 12; see also Supreme Court Committee on Digital Exclusion, Report (2023).

[7] Justice K.S. Puttaswamy (Retd.) v Union of India, (2018) 1 SCC 809 (Constitution Bench); see especially Chandrachud J (concurring) on informational self-determination.

[8] E.P. Royappa v State of Tamil Nadu, (1974) 4 SCC 3, 38 (Bhagwati J); Maneka Gandhi v Union of India, AIR 1978 SC 597; see also Ajay Hasia v Khalid Mujib Sehravardi, (1981) 1 SCC 722.

[9] Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (nine-judge bench); DY Chandrachud J, at [643]–[650]; Kaul J, at [682]–[683].

[10] A.K. Kraipak v Union of India, AIR 1970 SC 150; Maneka Gandhi v Union of India, AIR 1978 SC 597; see also M P Jain and S N Jain, Principles of Administrative Law (8th edn, LexisNexis, 2019) ch 12.

[11] Information Technology (Amendment) Act, 2008, inserting s 43A into the Information Technology Act, 2000; see also IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[12] Digital Personal Data Protection Act, 2023, s 4; Statement of Objects and Reasons; see also Ministry of Electronics and Information Technology, 'Report of the Committee of Experts on a Non-Personal Data Governance Framework' (2020).

[13] Cf GDPR (EU) 2016/679, art 22; see Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018); Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(14) Economic and Political Weekly 10.

[14] S.N. Mukherjee v Union of India, (1990) 4 SCC 594, 620; see also Union of India v Mohan Lal Capoor, (1973) 2 SCC 836; Harinagar Sugar Mills Ltd v Shyam Sundar Jhunjhunwala, AIR 1961 SC 1669.

[15] Angwin J et al, 'Machine Bias' (ProPublica, 23 May 2016); see also Virginia Eubanks, Automating Inequality (St Martin's Press 2018); Safiya Umoja Noble, Algorithms of Oppression (NYU Press 2018).

[16] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, ss 7, 8; see Khera (n 6); Nikhil Dey, Jean Dreze and Reetika Khera (eds), 'Living Reality of MGNREGS Wages' (Mazdoor Kisan Shakti Sangathan, 2017).

[17] Puttaswamy (2017) (n 9), [179]–[180] (Chandrachud J): proportionality requires (i) legitimate aim, (ii) rational connection, (iii) necessity, (iv) balancing of rights; applied to data surveillance in Puttaswamy (2018) (n 7).

Select Bibliography

Constitutional Provisions

Constitution of India, arts 12–13, 14, 15, 19, 21, 32, 226

Legislation

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

Digital Personal Data Protection Act, 2023

Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008)

IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

General Data Protection Regulation (EU) 2016/679

Regulation (EU) 2024/1689 (Artificial Intelligence Act)

Cases

A.K. Kraipak v Union of India, AIR 1970 SC 150

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

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

Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (Right to Privacy — NineJudge Bench)

Justice K.S. Puttaswamy (Retd.) v Union of India, (2018) 1 SCC 809 (Aadhaar — Constitution Bench)

Maneka Gandhi v Union of India, AIR 1978 SC 597

S.N. Mukherjee v Union of India, (1990) 4 SCC 594

Union of India v Mohan Lal Capoor, (1973) 2 SCC 836

Rechtbank Den Haag, 5 February 2020, ECLI:NL:RBDHA:2020:1878 (SyRI — Netherlands)

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

Books and Reports

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

Jain MP and Jain SN, Principles of Administrative Law (8th edn, LexisNexis, 2019)

Khera R (ed), Dissent on Aadhaar: Big Data Meets Big Brother (Orient BlackSwan, 2019)

Matthan R, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018)

NITI Aayog, National Strategy for Artificial Intelligence — #AIforAll (Government of India, 2018)

Noble SU, Algorithms of Oppression: How Search Engines Reinforce Racism (New York University Press, 2018)

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

Articles and Chapters

Baxi U, 'The Rule of Law in India: Theory and Practice' in Peerenboom R (ed), Asian Discourses of Rule of Law (Routledge, 2004)

Coglianese C and Lehr D, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105(5) Georgetown Law Journal 1147

Dreze J and Khera R, 'Aadhaar Failures: A Tragedy of Errors' (2017) 52(10) Economic and Political Weekly 12

Ramanathan U, 'A Unique Identity Bill' (2010) 45(14) Economic and Political Weekly 10

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7(2) International Data Privacy Law 76

Zarsky T, 'The Trouble with Algorithmic Decisions' (2016) 41(1) Science, Technology & Human Values 118

Author Note: Correspondence to [Author Name], [Department], [Institution]. Email: [email@institution.edu]. Word count (body text, excluding abstract, footnotes and bibliography): approx. 3,000 words. The author declares no conflicts of interest.