

International Journal Research Publication Analysis

Page: 01-16

ARTIFICIAL INTELLIGENCE (AI) AND CONSTITUTIONAL GOVERNANCE

*Aman Tandon (L. L. M.)

India.

Article Received: 14 September 2026

*Corresponding Author: Aman Tandon

Article Revised: 04 October 2026

India.

Published on: 24 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.7828>

ABSTRACT

Government agencies in India are increasingly relying on algorithm-based systems for tasks such as identifying beneficiaries for welfare schemes and policing; yet, there is no law in India governing the use of artificial intelligence at the government level. This article examines whether the Constitution of India, as interpreted by the Supreme Court, provides adequate standards for the review of such systems, and whether the existing legal and policy framework renders that standard enforceable. Employing legal principles and comparative methods, this analysis covers Articles 14, 19, and 21; the 'proportionality jurisprudence' established in the *Puttaswamy Aadhaar* case, and *Anuradha Bhasin* case; the Digital Personal Data Protection Act, 2023, and its 2025 rules; and the India AI Governance Guidelines, 2025. Additionally, these are compared with the frameworks of the European Union, the Netherlands, the United Kingdom, Canada, and the United States. This article finds that constitutional principles are largely adequate, but their implementation is hindered by information asymmetry, exemptions granted to the executive under data protection laws, the lack of a right to challenge automated decisions, and a reliance on voluntary principles. It is argued that this shortcoming is essentially procedural rather than substantive. Furthermore, it proposes a limited and risk-based legal framework for public-sector AI, incorporating elements such as impact assessments, public registers, reasoned explanations, meaningful human review, and a 'burden-shifting' rule for judicial review. The conclusion is that constitutional control over the power of algorithms depends less on new rights and more on making existing rights legally enforceable.

KEYWORDS: Artificial Intelligence; Constitutional Governance; Proportionality; Algorithmic Accountability; Article 21; Comparative Public Law.

I. INTRODUCTION

Government officials in India are increasingly using algorithms to determine who receives benefits from welfare schemes, who is subjected to scrutiny, and who is identified within a crowd. Constitutional limits do not cease to apply simply because a decision is based on a score rather than the judgment of an official. If an individual is denied an entitlement, excluded from a scheme, or stopped by the police due to an algorithm, the result constitutes 'State action,'¹ and it must satisfy the requirements of Articles 14, 19, and 21 of the Constitution.

This article addresses a question far more specific than how artificial intelligence ("AI") should be regulated. It asks whether a constitutional standard already exists for the review of government decisions based on algorithms, and where the law fails to apply that standard. The Supreme Court has recognized privacy as a fundamental right,² adopted 'proportionality' as the test for measures that restrict rights,³ and held arbitrariness to be an independent ground for invalidation under Article 14.⁴ What is not clear is whether an affected individual can invoke these principles against a system whose logic is opaque, whose data has not been vetted, and whose operator is often a private vendor.

This question has now become crucial. India has enacted the 'Digital Personal Data Protection Act, 2023' ("DPDP Act"), announced the 'Digital Personal Data Protection Rules, 2025' ("DPDP Rules") in November 2025,⁵ and issued the 'India AI Governance Guidelines' ("MeitY Guidelines") in the same month; the drafting committee for these concluded that there is currently no need for a separate law for AI.⁶ Meanwhile, the European Union has implemented comprehensive regulations⁷ for AI, and European courts have already struck down algorithm-based welfare and policing systems. Thus, India faces a choice between relying on principles within existing laws and pursuing targeted legal interventions.

The scope of this article is limited to AI used by or on behalf of the state; private-sector AI is discussed only insofar as it affects regulations concerning the state. This article first examines the adequacy of the constitutional principle (Part VIII), then looks at the legal and policy framework for its implementation (Part IX), and finally compares India with the European Union, the Netherlands, the United Kingdom, Canada, and the United States (Part X) before offering conclusions and suggestions.

II. STATEMENT OF THE PROBLEM

The problem lies in the shortcomings of its implementation. While constitutional principles can be invoked to challenge arbitrary, discriminatory, or excessively harsh algorithm-based decisions, three aspects of the current system hinder their effective application. First,

information asymmetry: the affected individual cannot view the model, data, or criteria, and the DPDP Act narrows, rather than expands, the scope of information disclosure under the Right to Information Act, 2005. Secondly, legal silence: The DPDP Act does not provide any right to challenge fully automated decisions and grants broad exemptions for government processing. Third, the relaxation of rules: MeitY's guidelines and NITI Aayog's documents are voluntary and do not create any legal obligations that could be challenged in court. Consequently, while rights are granted, there is no recourse in the event of their violation; this allows the government to implement high-impact systems without prior assessment, public record, or any stated, concrete justification.

III. RESEARCH QUESTIONS

1. To what extent do Articles 14, 19, and 21, read in conjunction with the Supreme Court's 'doctrine of proportionality' (proportionality jurisprudence), provide an adequate and robust standard for the judicial review of decisions taken by the State based on algorithms?
2. To what extent do the DPDP Act, 2023 (along with the 2025 Rules) and the MeitY Guidelines, 2025 transform that standard into enforceable rights, duties, and remedies?
3. Regarding addressing the shortcoming identified under the second question, what do the judicial and regulatory approaches of the European Union, the Netherlands, the United Kingdom, Canada, and the US teach India?

IV. RESEARCH OBJECTIVES

1. To determine whether existing principles regarding arbitrariness, indirect discrimination, privacy, and proportionality can be applied to algorithm-based systems without requiring any new principles.
2. To evaluate the implementation capacity of India's existing legal and policy frameworks and identify the gaps within them.
3. Developing design features through appropriate comparisons that can be incorporated into the Indian framework for the use of AI by states.

V. RESEARCH METHODOLOGY

This study is based on legal principles and comparative analysis. Primary sources include the Constitution, statutes, regulations, government policy documents, and Supreme Court judgments; the analysis focuses on the underlying reasoning rather than merely the outcomes. Meanwhile, secondary sources comprise books, peer-reviewed articles, and reports from the United Nations and government bodies.

Examples for comparison are selected based on appropriate criteria. The European Union possesses a highly developed legal system and examines the "principle versus law" dilemma that India is currently facing. The examples of the Netherlands and the United Kingdom are significant because courts there applied a standard akin to proportionality specifically Article 8(2) of the European Convention on Human Rights to government algorithmic systems; this standard is structurally similar to India's proportionality review. Canada employs a Westminster-style system that regulates government algorithms through a binding executive directive; India could adopt this approach without enacting legislation. On the other hand, the United States exemplifies the practice of judicial caution in the absence of specific laws. This comparison is based on similarities, differences, causes, consequences, and lessons learned. No empirical or experience-based study was conducted for this purpose. The issues pertain to the adequacy of legal provisions rather than the conduct of the concerned parties; furthermore, this article does not claim to measure exclusion rates or administrative operations evidence regarding these matters has been drawn from secondary reports. This limitation is acknowledged. The legal position is stated as of September 20, 2026.

VI. RESEARCH HYPOTHESIS

This article examines the hypothesis that existing constitutional standards are sufficient for reviewing the use of AI by the state, but the legal and policy framework for implementing those standards is procedurally inadequate; therefore, the focus of reform should be on transparency, assessment, and mechanisms for improvement rather than on creating new rights.

VII. LITERATURE REVIEW

There are four aspects to the literature surrounding this issue. The first is research on algorithmic accountability. Citron argues that information, meaningful hearings, and reviewable records⁸ are essential for automated decisions; Pasquale demonstrates how opacity is maintained through trade secrecy;⁹ and O'Neil explains how scoring models exacerbate discrimination.¹⁰ Barocas and Selbst demonstrate that data appearing neutral on the surface produces disparate impacts effects that anti-discrimination doctrine (which focuses on intent) fails to adequately grasp or address.¹¹ Regarding explanation, Wachter, Mittelstadt, and Russell argue that counterfactual explanations can meet explanation-related requirements without disclosing the underlying code,¹² whereas Selbst and Barocas caution that explanations cannot substitute for substantive rules.¹³ Wachter and Mittelstadt further advocate for the right to reasonable inference, which forms the basis for the concept of 'inferential privacy' used below.¹⁴

The second aspect concerns Indian research on data-driven governance. Marda identifies the limitations of data-driven decision-making within India's AI policy,¹⁵ Parsheera examines facial recognition,¹⁶ and the literature on Aadhaar compiled by Khera highlights the exclusion—or denial of services—resulting from authentication failures.¹⁷ The third aspect relates to courts and welfare algorithms: Van Bakkum and Zuiderveen Borgesius analyze the Dutch SyRI ruling and warn that its immediate impact is limited,¹⁸ while the UN Special Rapporteur cautions against the emergence of "digital welfare states."¹⁹ The fourth aspect encompasses government policy documents, primarily those from NITI Aayog and MeitY.

What remains unresolved is whether India's existing constitutional doctrine is sufficient. In Indian scholarship, ethics, data protection, and bias are often viewed in isolation, with principles discussed only at the end; comparative literature rarely asks what Indian doctrine is already capable of achieving. While considering the government exemptions under the DPDP Act and the 2025 guidelines, no detailed study has been conducted to examine the feasibility of applying these principles to government algorithmic systems. This article addresses this gap by distinguishing between the feasibility of procedural implementation and actual adequacy.

VIII. The Essence of Adequacy: Constitutional Standards

A. Article 14: Classification, Arbitrariness and Indirect Discrimination

Under a classification test, the distinction must be based on a clear and rational ground that has a logical connection to the objective sought to be achieved.²⁰ Algorithm-based risk scores create distinct categories, yet the basis for these categories may emerge abruptly—in ways that even the implementer cannot fully explain. A category that neither the government nor the courts can clearly define cannot be considered easily comprehensible. Therefore, under Article 14, it can be argued that a model whose operational variables cannot be articulated fails to meet the test for valid categorization.

In various cases, *Royappa* treated arbitrariness as the antithesis of equality,²¹ while *Shayara Bano* extended this concept to "manifest arbitrariness."²² Any automated decision that disregards relevant circumstances, or is based on irrelevant or unreliable connections, falls within this ambit. Most importantly, *Nitisha* recognized indirect discrimination under Articles 14 and 15(1): criteria that appear neutral on the surface but disproportionately disadvantage a group and exacerbate pre-existing disadvantages are unconstitutional, regardless of intent.²³ This directly addresses the issue of proxy variables. Even if caste is not explicitly used in a welfare eligibility model, factors such as postal codes, name patterns, or data on past beneficiaries can lead to the same outcome. The necessary methodology exists; the only

missing element is evidence, as proving disparate impact requires outcome data that is held exclusively by the government.

B. Article 21: Procedure, Privacy and Proportionality

In the *Maneka Gandhi* case, it was established that any procedure depriving a person of their liberty must be just, fair, and reasonable;²⁴ meanwhile, in the *Puttaswamy-I* case, informational privacy was recognized under Article 21, and it was held that any interference with it requires legal validity, a legitimate aim, and proportionality.²⁵ Subsequently, the four-step formula adopted in the 'Modern Dental' case (legitimate goal, suitability, necessity, and proportionality) was applied in the Aadhaar judgment;²⁶ this framework is derived from comparative constitutional studies.²⁷

Two aspects of that ruling are significant for AI. First, to establish 'necessity,' it is essential to demonstrate that a less restrictive alternative would not be equally effective; this is an evidentiary requirement. Second, the ruling also highlights a limitation. It could be argued that the majority upheld the scheme largely based on the State's assertions regarding the system's security and accuracy, whereas the dissenters emphasized the risks of exclusion and profiling. Where the state controls the facts, proportionality review risks becoming a review of the state's own account. Proportionality is only as robust as the information provided beforehand.

AI adds another dimension: inference. A model can detect information such as health status or political leanings that the individual has never disclosed.²⁸ If informational privacy safeguards control over personal information, then inferred information must fall within its scope, and profiling for state purposes must independently satisfy the test of proportionality. This follows from the reasoning in *Puttaswamy I* and does not require the creation of any new right. Facial recognition technology which can operate without the individual's involvement is the most prominent example of this: there is no specific Indian law governing it,²⁹ making it difficult to satisfy the criteria for legal validity established in the *Puttaswamy I* case.

C. Article 19(1)(a): Automated Speech Control

Shreya Singhal modified the intermediary liability provision so that the obligation to remove content arises only upon a court order or government notification, thereby preventing the excessive private removal of lawful expression.³⁰ This argument applies even more forcefully to large-scale automated moderation, where over-blocking is a systematic process. Anuradha Bhasin applied the principle of proportionality to restrictions on expression and mandated that restrictive orders be published and open to judicial review.³¹ Therefore, government directives mandating or promoting automated filtering including for deepfakes must be grounded in a solid basis, made public, and be reasonable; while regulating harmful synthetic media is

appropriate, these standards apply in this context as well.

D. Reasons and Natural Justice

Under administrative law, it is mandatory to provide reasons for decisions that have consequences for citizens.³² "The algorithm made the decision" does not constitute a reason. This obligation does not require the disclosure of source code; rather, it necessitates a clear explanation of the factors considered and their respective roles, which can be provided through a hypothetical explanation.³³

Therefore, in accordance with legal principles, Articles 14, 19, and 21 already prohibit arbitrary, discriminatory, and excessive algorithm-based measures. The answer to the first research question is 'yes', but with a caveat: each principle requires information that the claimant does not possess.

IX. PROCEDURAL DEFICIENCY: THE STATUTORY AND POLICY FRAMEWORK

A. The DPDP Act, 2023

The DPDP Act imposes certain obligations on data fiduciaries (data handlers), but its significance regarding the oversight of government AI is limited for four reasons. First, Section 17(2)(a) empowers the Central Government to exempt government entities from the Act on grounds such as security and public order;³⁴ consequently, the implementation of safeguards mandated by the *Puttaswamy I* judgment is left to executive notification (government order). Secondly, Section 7 recognizes "legitimate use" without consent³⁵ for state-provided subsidies, benefits, and services; consequently, systems implementing welfare schemes largely operate outside the scope of consent. Thirdly, the Act does not grant the right to challenge a decision based entirely on automated processing or to obtain a human review of such a decision. In accordance with the nearest provision, Section 8(3), a trustee must ensure the completeness, accuracy, and consistency of the data used to make decisions affecting the data principal;³⁶ this pertains to the duty regarding data quality, not the authority to review decisions. Fourth, Section 44(3) amends Section 8(1)(j) of the Right to Information Act, 2005, to allow for the exemption of personal information without the prior public interest override,³⁷ this could hinder the work of journalists, researchers, and affected individuals who wish to understand how government systems treat people. Since the main responsibilities will only begin in 2027, there is currently no experience regarding its functioning.³⁸

B. Policy Instruments

NITI Aayog's documents articulate the principles of equity, transparency, and accountability, and identify facial recognition as an application that could impact fundamental rights;³⁹

however, these documents are clearly not binding. MeitY's guidelines propose the establishment of a governance group, an expert committee, and a safety institute at the institutional level and beyond, and adopt seven "principles," including "People First" and "Understandable by Design."⁴⁰ These remain voluntary; while the committee's view that existing laws suffice might be justified for private-sector innovation, it does not hold true for government use. As previously noted, current laws mandate neither transparency nor accountability mechanisms. Furthermore, the principle of "prioritizing innovation over regulation" is not a constitutional rule. Where fundamental rights are concerned, regulation is a legal requirement—not something that stands on par with, or competes against, those rights.

C. Assessment

Thus, while India's framework is grounded in principles, it cannot be enforced against the government. The answer to the second research question is 'no': none of these mechanisms create a legal obligation mandating assessment, disclosure of information, explanation, or human review. Courts can still enforce Articles 14 and 21 through writ jurisdiction, but they can only do so by examining each case individually, after harm has occurred, and while taking into account the aforementioned evidentiary gaps. As shown in the next section, courts abroad intervened when the legal framework was inadequate; India's situation comprising government-notified exemptions and voluntary guidelines bears a greater resemblance to such frameworks than to one based on mandatory rules.

X. COMPARATIVE ANALYSIS

A. Similarities

Courts and lawmakers accept a proportionality-based inquiry and transparency as prerequisites for this. Regarding the Syrian Republic, the District Court of The Hague ruled that a system flagging fraud risks in welfare schemes violated Article 8 of the European Convention because the legislation failed to meet the requirements of necessity and proportionality; the risk model was not disclosed, thereby hindering verification.⁴¹ In the *Bridges* case, the English Court of Appeal ruled live facial recognition unlawful. The court held that the legal framework granted excessive discretion regarding who could be placed on a watchlist and where the technology could be deployed; furthermore, the equality assessment was inadequate.⁴² *Puttaswamy II* articulates the same argument: legitimacy, necessity, and safeguards. Even in the *Loomis* case, the Wisconsin Supreme Court permitted the use of a proprietary risk score subject to written warnings regarding its limitations—at the time of sentencing, holding that its proprietary nature did not, in itself, violate due process.⁴³

B. Differences

The methods for implementing this responsibility vary across different jurisdictions. The EU has adopted a horizontal law: the AI Act classifies systems based on risk, prohibits certain types of activities, mandates human oversight for high-risk systems, requires government bodies to assess the impact on fundamental rights and register systems in a public database, and grants affected individuals the right to obtain an explanation.⁴⁴ Under the 'General Data Protection Regulation' (GDPR), there is a general right not to be subject solely to automated decisions.⁴⁵ In the SCHUFA case, the 'Court of Justice' interpreted this right broadly to include credit scores, upon which a lender relies to a significant extent.⁴⁶ Canada employs a binding executive instrument: under the Directive on Automated Decision-Making, federal departments are required to complete an Algorithmic Impact Assessment; safeguards such as peer review, transparency, and human involvement are categorized across four impact levels, and publication is mandatory.⁴⁷ There is no general legislation regarding AI in the United Kingdom or at the federal level in the United States; instead, they rely on post-hoc reviews based on human rights, equality, and administrative law.

C. Reasons for the Differences

These differences reflect the respective constitutional frameworks. The EU's charter-based system and the logic of the internal market favor uniform laws. Canada, through its Westminster executive parliamentary process, can bind its departments by issuing directives without the need for legislation. Britain and the US prioritize incremental reform under common law and are reluctant to enact legislation before harm is proven. India's situation is mixed: like the European Union, it has a constitutional court that applies the principle of proportionality; like Britain, its executive prioritizes policy over legislation.

D. Practical and Legal Consequences

When the enforcement of rights is left solely to the courts, solutions tend to be slow and limited. In the SyRI case, a law was struck down without fully resolving the issue of automated fraud detection,⁴⁸ while in the Bridges case, the demand was for a better policy rather than the abandonment of the technology. In countries like Canada, under 'ex-ante' rules, the onus is on the implementing entity to prove the system's soundness before any harm occurs; however, such a directive applies solely to the executive branch which also holds the sole authority to amend it and provides no grounds for legal action to those affected by it. EU law grants stronger rights, but high-risk obligations for stand-alone systems have now been postponed until December 2027,⁴⁹ highlighting the risks involved in implementing comprehensive regulations.

E. Lessons for India

Three lessons emerge from this. First, the primary approach for high-impact government systems should be 'ex-ante assessment' and 'public registration,' rather than relying on post-facto legal battles. Second, wherever freedoms or rights are affected, there must be a statutory basis rather than merely an executive (administrative) one; the lack of adequate "law" was the central issue in the '*Bridges*' and '*SyRI*' cases paralleling the requirement for legal validity established in the '*Puttaswamy I*' case. Thirdly, India need not adopt the scope of the AI Act verbatim. A targeted law at the government level limited to high-impact systems is appropriate for addressing identified gaps; this would avoid imposing hasty regulations on private innovation and aligns with the MeitY committee's view favoring less stringent rules for the private sector.

XI. ANTICIPATED OBJECTIONS

Three objections need to be addressed. The first is that existing laws are sufficient, a conclusion also reached by the MeitY committee. While this holds true for the actions the law prohibits, it does not apply to the grounds upon which an individual might substantiate a claim. Evidence regarding exclusion in Aadhaar-related matters indicates that legal provisions remain ineffective in the absence of obligations to provide information, conduct assessments, or offer clarifications.⁵⁰ Secondly, making the information public could compromise security and trade secrets. However, this proposal does not require the source code to be made public. This requires assessment records, register entries, an explanation of the factors employed, and where confidentiality is claimed a confidential review by a court or an independent authority. Anuradha Bhasin and Kranti Associates already recognize that reasoned and reviewable government action is compatible with appropriate confidentiality.⁵¹

Thirdly, regulation can have an adverse impact on innovation. A targeted law applying only to government systems that exceed a certain impact threshold does not affect private or low-risk innovation. At the same time, it provides vendors with certainty regarding the standards required by government clients; Canada's tiered model demonstrates that security measures can be scaled up or down based on impact.⁵²

XII. FINDINGS

1. Substantive standard: Articles 14 (classification, manifest arbitrariness, and indirect discrimination), 21 (procedural fairness and proportionality, including the presumption of privacy), and 19(1)(a) apply to the State's algorithm-based decisions without the need for any new doctrine.

2. Enforcement framework: Due to factors such as the exemptions granted to states under the DPDP Act, the absence of rights against fully automated decisions, the curtailment of the RTI Act's scope, and the voluntary nature of instruments issued by NITI Aayog and MeitY, affected individuals are left without any legal recourse to seek assessment, disclosure, clarification, or review.

3. Comparative lessons: Effective systems rely on prior assessments, public registers, human oversight, and a legal basis, but they determine their scope based on risk.

4. Hypothesis: This hypothesis holds true with a modification: since the *Puttaswamy II* case demonstrates that the State's position may be prioritized during a proportionality review when the facts are within its control, the modification must encompass not only the obligation to disclose information but also a rule regarding the burden of proof.

XIII. RECOMMENDATIONS

1. Narrow statute: Enact a public sector algorithmic accountability law covering the state and bodies performing public functions, applicable to systems whose outputs affect freedoms, entitlements, or legal rights, and featuring impact levels modeled on Canadian guidelines.

2. Impact assessment: Before implementing this, it is essential to assess aspects related to equality and privacy and to document the reasoning regarding proportionality (such as objective, suitability, less intrusive alternatives, and balancing).

3. Public register: Maintain a register of critical systems that clearly defines security-related exemptions, and ensure these are reviewed by an independent authority rather than being approved without due consideration.

4. Explanation and human review: Ensure reasoned explanations and human review for decisions primarily based on AI; furthermore, the reviewer must possess the authority and information to make a decision that differs from the AI's output.

5. Burden of proof: A provision should be made requiring the State to justify a measure once a claimant establishes, *prima facie*, a disproportionate impact or exclusion without a clear reason; furthermore, courts should be empowered to appoint technical amici (friends of the court).

6. Amend the DPDP framework: It should be made mandatory to state reasons, set timeframes, and publish notifications issued under Section 17(2)(a); additionally, the provision for 'disclosure in the public interest' regarding the state's algorithmic systems should be restored under the RTI Act.

7. Procurement: It is essential to enter into contracts with vendors that secure audit and

access rights, ensuring there are no impediments to disclosing confidential business information to courts and regulators.

8. Facial recognition and interim measure: The use of facial recognition technology by the state should be banned in the absence of specific legal authorization, and an executive directive based on the Canadian model should be issued until legislation is enacted.

XIV. CONCLUSION

This article argues that Indian constitutional standards are largely sufficient to review the state's algorithm-based decision-making processes. Articles 14, 19, and 21 enforced through principles such as non-arbitrariness, indirect discrimination, procedural fairness, and proportionality already serve to curb the state's use of AI when it is opaque, discriminatory, or disproportionate. The shortcoming lies elsewhere: in the information asymmetry that the DPDP Act further exacerbates, in the absence of any right to challenge automated decisions, and in a policy framework that is based on principles yet remains voluntary.

Comparative experience shows that while courts can invalidate flawed systems, they cannot prevent their implementation on their own. Therefore, alongside judicial review, India should introduce a law that is both limited in scope and risk-based, mandating that the government undertake assessments, registration, transparency measures, and human oversight. The measure of success is not whether India regulates AI more than others do, but rather whether an individual excluded by an algorithm can understand why that happened and find redress through a court equipped with the necessary evidence to uphold the Constitution.

BIBLIOGRAPHY

Books

1. Barak, Aharon, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press, Cambridge, 2012).
2. Khera, Reetika (ed.), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, Hyderabad, 2019).
3. O'Neil, Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown, New York, 2016).
4. Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge, 2015).
5. Articles and Working Papers
6. Barocas, Solon & Selbst, Andrew D., "Big Data's Disparate Impact" 104 *Cal. L. Rev.* 671 (2016).

7. Citron, Danielle Keats, "Technological Due Process" 85 *Wash. U. L. Rev.* 1249 (2008).
8. Marda, Vidushi, "Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making" 376 *Phil. Trans. R. Soc. A* 20180087 (2018).
9. Parsheera, Smriti, "Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?" Data Governance Network Working Paper 05 (2019).
10. Selbst, Andrew D. & Barocas, Solon, "The Intuitive Appeal of Explainable Machines" 87 *Fordham L. Rev.* 1085 (2018).
11. Van Bekkum, Marvin & Zuiderveen Borgesius, Frederik, "Digital Welfare Fraud Detection and the Dutch SyRI Judgment" 23 *Eur. J. Soc. Sec.* 323 (2021).
12. Wachter, Sandra & Mittelstadt, Brent, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" 2019 *Colum. Bus. L. Rev.* 494.
13. Wachter, Sandra, Mittelstadt, Brent & Russell, Chris, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR" 31 *Harv. J.L. & Tech.* 841 (2018).

Constitution and Statutes

14. The Constitution of India, 1950.
15. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
16. The Digital Personal Data Protection Rules, 2025 (notified November 2025). The Right to Information Act, 2005 (Act 22 of 2005).
17. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act).
19. Regulation (EU) 2026/1744 (Digital Omnibus on AI), amending Regulation (EU) 2024/1689.

Cases

20. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
21. *P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.
22. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
23. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.
24. *Kranti Associates (P) Ltd. v. Masood Ahmed Khan*, (2010) 9 SCC 496.
25. *Lt. Col. Nitisha v. Union of India*, 2021 SCC OnLine SC 261.
26. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
27. *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.
28. *Shayara Bano v. Union of India*, (2017) 9 SCC 1.

29. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
30. *Shri Ram Krishna Dalmia v. Justice S.R. Tendolkar*, AIR 1958 SC 538.
31. Case C-634/21, *OQ v. Land Hessen (SCHUFA Holding (Scoring))*, Court of Justice of the European Union, judgment of 7 December 2023.
32. *NJCM c.s. v. The Netherlands (SyRI)*, District Court of The Hague, ECLI: NL: RBDHA:2020:1878 (5 February 2020).
33. *R (Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058 (Eng.).
34. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

Government, Institutional and International Materials

35. Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (5 November 2025).
36. NITI Aayog, *Approach Document for India, Part 1: Principles for Responsible AI* (Government of India, February 2021).
37. NITI Aayog, *Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology* (Government of India, November 2022).
38. Report of the Special Rapporteur on Extreme Poverty and Human Rights, *Digital Welfare States and Human Rights*, UN Doc. A/74/493 (11 October 2019).
39. Treasury Board of Canada Secretariat, *Directive on Automated Decision-Making* (in force 1 April 2019, as amended).
40. The Constitution of India, art. 12 (defining “the State” to include the Government, Parliament, the legislatures and all local and other authorities).
41. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (hereinafter “*Puttaswamy I*”).
42. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar) (hereinafter “*Puttaswamy II*”).
43. *Shayara Bano v. Union of India*, (2017) 9 SCC 1.
44. The Digital Personal Data Protection Rules, 2025 (notified November 2025).
45. Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (5 November 2025).
46. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
47. Danielle Keats Citron, “Technological Due Process” 85 *Wash. U. L. Rev.* 1249 (2008).
48. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge, 2015).
49. Cathy O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and*

- Threatens Democracy* (Crown, New York, 2016).
50. Solon Barocas & Andrew D. Selbst, “Big Data’s Disparate Impact” 104 *Cal. L. Rev.* 671 (2016).
 51. Sandra Wachter, Brent Mittelstadt & Chris Russell, “Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR” 31 *Harv. J.L. & Tech.* 841 (2018).
 52. Andrew D. Selbst & Solon Barocas, “The Intuitive Appeal of Explainable Machines” 87 *Fordham L. Rev.* 1085 (2018).
 53. Sandra Wachter & Brent Mittelstadt, “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI” 2019 *Colum. Bus. L. Rev.* 494.
 54. Vidushi Marda, “Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making” 376 *Phil. Trans. R. Soc. A* 20180087 (2018).
 55. Smriti Parsheera, “Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?” Data Governance Network Working Paper 05 (2019).
 56. Reetika Khera (ed.), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, Hyderabad, 2019). ¹⁸Marvin van Bekkum & Frederik Zuiderveen Borgesius, “Digital Welfare Fraud Detection and the Dutch SyRI Judgment” 23 *Eur. J. Soc. Sec.* 323 (2021).
 57. Report of the Special Rapporteur on Extreme Poverty and Human Rights, *Digital Welfare States and Human Rights*, UN Doc. A/74/493 (11 October 2019).
 58. *Shri Ram Krishna Dalmia v. Justice S.R. Tendolkar*, AIR 1958 SC 538.
 59. *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.
 60. *Shayara Bano*, *supra* note 4.
 61. *Lt. Col. Nitisha v. Union of India*, 2021 SCC OnLine SC 261.
 62. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
 63. *Puttaswamy I*, *supra* note 2.
 64. *Puttaswamy II*, *supra* note 3; *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.
 65. See generally Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press, Cambridge, 2012).
 66. Wachter & Mittelstadt, *supra* note 14.
 67. NITI Aayog, *Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology* (Government of India, November 2022).
 68. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
 69. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
 70. *Kranti Associates (P) Ltd. v. Masood Ahmed Khan*, (2010) 9 SCC 496.

71. Wachter, Mittelstadt & Russell, *supra* note 12.
72. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17(2)(a).
73. *Id.*, s. 7.
74. *Id.*, s. 8(3).
75. The Digital Personal Data Protection Act, 2023, s. 44(3); The Right to Information Act, 2005 (Act 22 of 2005), s. 8(1)(j).
76. The Digital Personal Data Protection Rules, 2025.
77. NITI Aayog, *Approach Document for India, Part 1: Principles for Responsible AI* (Government of India, February 2021); NITI Aayog, *Facial Recognition Use Case*, *supra* note 29.
78. MeitY, *AI Governance Guidelines*, *supra* note 6.
79. *NJCM c.s. v. The Netherlands (SyRI)*, District Court of The Hague, ECLI:NL:RBDHA:2020:1878 (5 February 2020).
80. *R (Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058 (Eng.).
81. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
82. Regulation (EU) 2024/1689, arts. 5, 14, 27, 49, 86.
83. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art. 22.
84. Case C-634/21, *OQ v. Land Hessen (SCHUFA Holding (Scoring))*, Court of Justice of the European Union, judgment of 7 December 2023.
85. Treasury Board of Canada Secretariat, *Directive on Automated Decision-Making* (in force 1 April 2019, as amended).
86. Van Bakkum & Zuiderveen Borgesius, *supra* note 18.
87. Regulation (EU) 2026/1744 (Digital Omnibus on AI), amending Regulation (EU) 2024/1689 (in force 27 July 2026).
88. Khera (ed.), *supra* note 17.
89. *Kranti Associates*, *supra* note 32; *Anuradha Bhasin*, *supra* note 31.
90. Treasury Board of Canada, *Directive on Automated Decision-Making*, *supra* note 47.