

Algorithmic Arbitrariness Under Article 14: Reconstructing Judicial Review for Automated State Action in India

Kumar KR¹ and Dr. Rajiv Khare²

¹Research Scholar, Department of Law

²Research Guide, Department of Law
Sabarmati University, Ahmedabad

Abstract: *The expansion of automated decision-making in public administration has altered the conditions under which constitutional power is exercised. Welfare eligibility, taxation, policing, recruitment, education, health administration, digital identity and regulatory enforcement increasingly depend on data-driven systems whose reasoning may be opaque, probabilistic and difficult to contest. Indian constitutional doctrine under Article 14 has long prohibited arbitrary State action, but its principal tests were fashioned for decisions attributable to identifiable human authorities. This article argues that automated State action requires a reconstructed form of judicial review capable of examining not merely the stated purpose of a governmental decision but also the design, data, operation and institutional governance of the system that produced it. It develops the concept of algorithmic arbitrariness and proposes a structured constitutional test built around legality, legitimate purpose, data relevance, non-discrimination, transparency, explainability, accuracy, procedural fairness, human oversight, auditability, proportionality and effective remedy. The article situates this framework within Indian equality jurisprudence while drawing limited comparative guidance from developments in Europe, the United Kingdom, the United States and international soft-law instruments. It concludes that Article 14 is sufficiently flexible to regulate automated State action, provided courts shift from reviewing only the final administrative outcome to reviewing the entire algorithmic decision architecture.*

Keywords: Article 14; algorithmic arbitrariness; automated State action; artificial intelligence; judicial review; explainability; procedural fairness

I. INTRODUCTION

1. The Indian administrative State increasingly depends on digital infrastructures that classify, rank, predict and recommend. Decisions once reached through files, hearings and recorded reasons may now be shaped by databases, scoring systems, matching tools, facial-recognition systems or machine-learning models. In constitutional terms, the decisive question is not whether technology is used, but whether public power remains subject to legality, equality and reasoned justification. Article 14 declares that the State shall not deny equality before the law or equal protection of the laws. Its reach has developed far beyond formal classification and now includes a prohibition against arbitrariness in State action. This doctrinal development offers a foundation for reviewing automated decisions, yet conventional review often assumes that the challenged act can be traced to a human decision-maker who understood the relevant facts, applied an intelligible standard and can explain the result.¹

2. Automated systems disturb each of those assumptions. The operative rule may be dispersed across source code, training data, vendor documentation, risk thresholds and post-deployment adjustments. A public officer may accept a system-

¹E.P. Royappa v State of Tamil Nadu, (1974) 4 SCC 3; Ajay Hasia v Khalid Mujib Sehravardi, (1981) 1 SCC 722.

generated output without understanding the pathway by which it was produced. The affected person may receive only a conclusory rejection, even where the system relied upon inaccurate, incomplete or historically biased data. Algorithmic opacity is therefore not merely a technical inconvenience; it can disable the constitutional functions of notice, reasons, hearing and judicial scrutiny. When the State cannot explain why a person was selected, excluded, ranked or flagged, equality review risks becoming formal rather than effective.²

3. This article uses the expression ‘automated State action’ to include any governmental decision in which an algorithmic system materially determines, recommends or structures an outcome affecting rights, benefits, burdens or opportunities. The expression includes fully automated decisions as well as nominally human decisions in which officials routinely defer to machine-generated recommendations. The central claim is that Article 14 should review the entire decision architecture: statutory authority, objective, data selection, model design, deployment context, human supervision, audit trail, explanation and remedial process. The final output is constitutionally significant, but it is only the visible end of a longer chain of public power.

II. FROM CLASSIFICATION TO ARBITRARINESS UNDER ARTICLE 14

1. Early Article 14 doctrine centered on reasonable classification. A classification was constitutionally valid when founded on an intelligible differentia and when that differentia bore a rational nexus to the object of the law. That formulation remains important for algorithmic systems because every model classifies: it distinguishes high risk from low risk, eligible from ineligible, suspicious from ordinary, and priority from non-priority. Yet an algorithm may satisfy a superficially intelligible classification while still operating through unreliable proxies, skewed data or unjustified thresholds. Classification review alone may therefore miss defects embedded in the process by which categories are generated.³

2. The transformation began with the recognition that equality is antithetical to arbitrariness. In *E.P. Royappa v State of Tamil Nadu*, the Supreme Court rejected a narrow, compartmentalised view of equality and held that arbitrariness and equality are sworn enemies. *Maneka Gandhi v Union of India* strengthened the relationship between Articles 14, 19 and 21 and required State procedure to be fair, just and reasonable rather than fanciful, oppressive or arbitrary. These cases matter for automated governance because they direct judicial attention to the quality of State reasoning and procedure, not merely to the existence of a formal category.⁴⁵

3. *Ajay Hasia v Khalid Mujib Sehravardi* reaffirmed that wherever State action is arbitrary, Article 14 is attracted. Later decisions developed review of manifest arbitrariness, particularly where a measure is capricious, irrational, excessive or without an adequate determining principle. Although doctrinal formulations vary with context, the underlying constitutional demand is consistent: coercive public power must be capable of rational justification. An automated decision cannot escape this demand merely because the immediate cause of the outcome is a computational process rather than a written order.⁶⁷

4. Article 14 review should therefore ask two linked questions. First, does the legal framework authorise the relevant decision and identify an intelligible objective? Secondly, does the algorithmic mechanism pursue that objective through rational, reliable and fair means? A system may have a legitimate purpose but use irrelevant data; it may use relevant data but generate intolerable error rates; it may be statistically accurate overall but impose systematic disadvantages on

²Danielle Keats Citron, “Technological Due Process” (2008) 85 Washington University Law Review 1249, 1253–58.

³*State of West Bengal v Anwar Ali Sarkar*, AIR 1952 SC 75; *Ram Krishna Dalmia v Justice S.R. Tendolkar*, AIR 1958 SC 538.

⁴*Maneka Gandhi v Union of India*, (1978) 1 SCC 248, paras 56–57.

⁵*E.P. Royappa v State of Tamil Nadu*, (1974) 4 SCC 3, paras 85–86.

⁶*Shayara Bano v Union of India*, (2017) 9 SCC 1, paras 101–01; *Joseph Shine v Union of India*, (2019) 3 SCC 39.

⁷*Ajay Hasia v Khalid Mujib Sehravardi*, (1981) 1 SCC 722, para 16.

a protected or vulnerable group. Each defect implicates equality because each weakens the rational connection between public purpose and individual burden.

III. THE DISTINCTIVE CHARACTER OF ALGORITHMIC STATE ACTION

1. Algorithmic decision-making is distinctive because it transforms administrative discretion without eliminating it. Human choices enter at every stage: defining the problem, selecting variables, choosing a dataset, assigning labels, setting thresholds, procuring software and deciding how much authority to give the output. The apparent neutrality of computation may conceal these normative choices. As scholars of algorithmic systems have shown, data-driven models can reproduce structural inequalities even where no programmer intends discrimination. The constitutional concern is consequently broader than intentional bias; it includes unjustified disparate effects, defective proxies and institutional indifference to foreseeable harm.⁸
2. Opacity arises in several forms. Technical opacity may result from model complexity. Organisational opacity may arise from fragmented responsibility between departments, contractors and vendors. Legal opacity may be asserted through claims of confidentiality, intellectual property or national security. Practical opacity may occur when an explanation is technically available but unintelligible to the person affected. Burrell's account of opacity and Pasquale's analysis of black-box institutions illuminate why formal access to a system does not necessarily produce meaningful accountability. For Article 14 purposes, the relevant standard should be functional: can the State provide an intelligible account sufficient to test legality, relevance, consistency and fairness?⁹
3. Data dependency creates a second difficulty. Administrative datasets are often collected for purposes different from the later algorithmic use. They may contain errors, omissions, duplicate records or historically patterned disparities. A predictive model trained on enforcement data, for example, may reproduce prior enforcement priorities rather than measure underlying misconduct. A welfare-fraud system may treat poverty-associated behaviours as indicators of deception. The use of a proxy becomes arbitrary when the State cannot demonstrate that it is sufficiently related to the legally relevant fact and that less harmful alternatives were considered.
4. Automation bias creates a third difficulty. Officials may over-trust machine outputs because they appear objective, scientific or precise. A formal human-in-the-loop safeguard is inadequate where the officer lacks training, time, authority or information to disagree with the system. Meaningful human oversight requires the capacity to understand the basis of the recommendation, to examine contrary evidence, to depart from the recommendation without penalty, and to record reasons. Otherwise, the human reviewer becomes a constitutional façade for automated power.
5. Finally, algorithmic systems are dynamic. Models may be retrained, recalibrated or updated after deployment. Their performance can deteriorate when social conditions change or when data distributions shift. Judicial review that examines only the original procurement decision will therefore be insufficient. Constitutional compliance must be continuous, supported by periodic testing, documented updates, impact assessments and accessible complaint mechanisms.

IV. ALGORITHMIC ARBITRARINESS AS A CONSTITUTIONAL WRONG

1. Algorithmic arbitrariness may be defined as automated or algorithmically assisted State action that imposes a benefit, burden, classification or risk designation through a process lacking lawful authority, rational connection, reliable data, fair procedure, adequate explanation, effective oversight or proportionate safeguards. This definition does not constitutionalise every technical defect. It identifies defects that undermine the State's capacity to justify differential treatment or adverse action under Article 14.
2. The concept contains substantive and procedural dimensions. Substantive arbitrariness concerns objectives, variables, proxies, thresholds, error distribution and discriminatory effects. Procedural arbitrariness concerns notice, reasons,

⁸Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact" (2016) 104 California Law Review 671, 677–94.

⁹Jenna Burrell, "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms" (2016) 3 Big Data & Society 1; Frank Pasquale, *The Black Box Society* (Harvard University Press 2015).

hearing, disclosure, human review, audit and remedy. The two dimensions interact. An unexplained decision prevents the individual from identifying inaccurate data; the absence of audit records prevents a court from determining whether a threshold was consistently applied; inadequate human review allows a substantively defective model to operate unchecked. Technological due process scholarship correctly emphasises that procedural design is integral to the legitimacy of automated government.¹⁰

3. The wrong is also institutional. Public authorities cannot avoid constitutional responsibility by outsourcing design or operation to a private vendor. Where a system is procured, adopted or relied upon by the State, the resulting decision remains State action. Contractual secrecy cannot displace constitutional disclosure. Procurement agreements should preserve governmental access to source documentation, validation reports, change logs and audit rights. A department that purchases an inscrutable system and then claims inability to explain it has created the very opacity on which it seeks to rely.

4. At the same time, constitutional review should avoid a simplistic demand that all source code be publicly disclosed. Source code may be useful in some cases, but it is not always necessary or sufficient. Courts should focus on the information required to test the decision: the governing rule, relevant variables, data provenance, validation method, performance measures, error rates, threshold rationale, group impacts, human override process and reasons for the individual outcome. Protective orders, confidentiality rings and court-appointed experts can address legitimate security or commercial concerns without sacrificing reviewability.

V. A STRUCTURED TEST OF ALGORITHMIC ARBITRARINESS

1. A structured test can convert general constitutional principle into a workable method of review. The proposed test has twelve elements. They are not rigid compartments; their weight will vary with the severity, scale and reversibility of the decision. A low-impact administrative triage tool may require fewer safeguards than a system affecting liberty, livelihood, welfare subsistence or access to essential services. Nevertheless, the State should bear an evidential burden to demonstrate compliance once an affected person raises a credible challenge to an automated decision.

2. First, legality requires clear statutory or regulatory authority for the decision and for the material use of automation. General administrative power should not automatically authorise opaque profiling where the system changes the practical criteria of eligibility or enforcement. Second, legitimate purpose requires a precisely identified public objective rather than an abstract invocation of efficiency. Third, data relevance requires the State to establish that each material variable is reasonably connected to the legally relevant criterion and is not an impermissible proxy.

3. Fourth, data quality and accuracy require documented measures for completeness, correction, timeliness and validation. Constitutional adequacy cannot be assessed through aggregate accuracy alone; false positives and false negatives must be examined in relation to the burden imposed. Fifth, equality and non-discrimination require testing for disparate impact across constitutionally relevant and vulnerable groups. Barocas and Selbst have shown that apparently neutral data practices can generate discriminatory outcomes through proxies, labels and historical patterns. Where a significant disparity appears, the State should explain its cause, necessity and mitigation.¹¹

4. Sixth, transparency requires public disclosure of the system's existence, purpose, legal basis, institutional owner and general operating logic. Seventh, explainability requires an individualised statement of the principal factors that produced the challenged outcome. A generic statement that a model identified 'high risk' is not an explanation. The affected person must be able to understand what information mattered, what rule or threshold was applied and how an error may be corrected.

5. Eighth, procedural fairness requires timely notice, an opportunity to contest adverse data and access to the material necessary for meaningful representation. The Supreme Court's insistence on fairness in administrative procedure supplies

¹⁰Danielle Keats Citron, "Technological Due Process" (2008) 85 Washington University Law Review 1249, 1301–13.

¹¹Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact" (2016) 104 California Law Review 671, 691–714.

the constitutional foundation for these protections. Ninth, meaningful human oversight requires an authorised and competent officer to review the case rather than merely affirm a system output. Tenth, auditability requires logs sufficient to reconstruct the decision, including the model version, input data, score, threshold, human interventions and later changes.¹²

6. Eleventh, proportionality requires the intensity of automation and the intrusiveness of data use to be necessary and balanced against the rights affected. Even where proportionality doctrine is formally associated with specific fundamental rights, its structured reasoning assists Article 14 analysis by testing rational connection, necessity and balancing. Twelfth, effective remedy requires prompt correction, reversal where appropriate, reasons for the remedial decision and compensation or other relief where serious harm has resulted. A right to challenge that cannot identify the decision pathway is illusory.¹³

7. The test should be applied with a risk-sensitive presumption. Where automated action affects liberty, policing, citizenship, access to subsistence benefits, medical treatment, education, public employment or essential identity infrastructure, courts should demand stronger justification and closer scrutiny. The greater the consequence and the weaker the individual's bargaining power, the stronger the State's duty to document, explain and independently validate the system.

VI. PROCEDURAL DUTIES OF THE STATE

1. A constitutional framework must begin before deployment. Public authorities should conduct an algorithmic impact assessment identifying the legal basis, purpose, categories of affected persons, data sources, anticipated benefits, foreseeable risks, alternatives and mitigation measures. High-impact systems should undergo independent testing before use. The assessment should not be a confidential internal formality; a public summary should enable democratic and judicial scrutiny while protecting genuinely sensitive details.

2. During operation, the State should provide a clear notice whenever an automated system materially influences a decision. The notice should identify the responsible authority and explain how to seek human review. Records must be retained for a period proportionate to the seriousness of the decision. Regular audits should test accuracy, drift, disparate impact, override patterns and complaint outcomes. A system that performs acceptably at launch may become arbitrary if later evidence reveals persistent error or discriminatory impact and the authority fails to respond.

3. Reasons require special attention. The constitutional function of reasons is not satisfied by revealing every mathematical operation. What matters is whether the explanation enables the person and the court to understand the decisive considerations. In an eligibility case, the State should identify the data relied upon, the rule applied and the basis of any mismatch. In a risk-scoring case, it should identify the principal factors, threshold and consequences. Where a model is too complex to generate a usable explanation for a high-impact decision, that limitation may itself demonstrate that the model is unsuitable for the governmental purpose.

4. Judicial remedies should be calibrated to the defect. Courts may quash an individual decision, direct fresh human determination, order disclosure, require data correction, suspend a system, mandate independent audit or prescribe interim safeguards. In systemic cases, structural directions may be necessary because repeated individual litigation cannot effectively address a common algorithmic defect. The principle should remain remedial proportionality: the order must restore legality and prevent recurrence without converting the court into a permanent technical administrator.

VII. COMPARATIVE AND INTERNATIONAL GUIDANCE

1. Comparative materials do not determine the meaning of Article 14, but they reveal recurring regulatory concerns. The European Union's data-protection framework recognises safeguards concerning certain solely automated decisions, while

12A.K. Kraipak v Union of India, (1969) 2 SCC 262; Maneka Gandhi v Union of India, (1978) 1 SCC 248.

13Modern Dental College and Research Centre v State of Madhya Pradesh, (2016) 7 SCC 353; K.S. Puttaswamy v Union of India, (2017) 10 SCC 1.

the European Union's artificial-intelligence regime adopts a risk-based approach to prohibited practices, high-risk systems, documentation, human oversight and post-market monitoring. These developments support the proposition that high-impact automation requires ex ante governance and continuing supervision rather than after-the-fact explanation alone.¹⁴

2. United Kingdom litigation concerning automated and data-driven public systems demonstrates the importance of lawful authority, transparency and impact assessment. In *R (Bridges) v Chief Constable of South Wales Police*, the Court of Appeal found deficiencies in the legal framework governing live automated facial recognition and in the assessment of equality impacts. The case illustrates that discretion delegated to a technical system must be bounded by sufficiently clear criteria and that equality duties must be operational rather than ceremonial.¹⁵

3. In the United States, disputes involving risk-assessment tools, benefits systems and automated fraud detection have exposed tensions between efficiency and due process. *State v Loomis* permitted the use of a proprietary risk assessment at sentencing but required caution regarding its limitations. Other controversies surrounding automated benefit termination and fraud detection show that large-scale error can result when governments deploy systems without adequate notice, validation and human review. The lesson for India is not to import a foreign doctrinal rule, but to recognise common institutional failure modes.¹⁶

4. International principles converge around fairness, transparency, accountability, robustness and human-centred oversight. The OECD Principles on Artificial Intelligence, UNESCO's Recommendation on the Ethics of Artificial Intelligence and Council of Europe instruments provide useful benchmarks. Their legal status varies, but they can inform the content of reasonableness and good administration where domestic law is open-textured. Article 14 remains the controlling norm; international materials assist in identifying feasible safeguards and emerging standards of responsible governance.¹⁷

VIII. APPLICATIONS IN THE INDIAN PUBLIC SECTOR

1. The proposed framework is particularly relevant to welfare administration. Digital identity matching, duplicate detection and fraud analytics may protect public resources, yet erroneous exclusion can threaten subsistence. A system that automatically suspends benefits because of a mismatch should trigger notice, disclosure of the mismatch, an accessible correction mechanism and temporary protection against severe hardship. Aggregate efficiency cannot justify an individual deprivation produced by inaccurate data and inaccessible procedures.

2. Policing and security applications require heightened scrutiny because predictions can generate self-reinforcing feedback loops. If deployment is concentrated in neighbourhoods already subject to intensive policing, resulting data may appear to confirm the system's prediction. Facial-recognition errors can disproportionately affect certain groups, while watchlist construction may be opaque. Legality, necessity, independent validation, strict retention limits and meaningful human confirmation should therefore be treated as minimum safeguards rather than optional policy choices.

3. Automated recruitment, examination, taxation, education and health administration raise related concerns. A screening system may penalise unconventional career paths; an examination-proctoring tool may misclassify disability-related behaviour; a tax-risk model may target lawful patterns associated with particular occupations; a health-priority model may encode unequal historical access to care. In each field, constitutional analysis must distinguish between legitimate administrative assistance and substitution of unreviewable statistical inference for legally relevant judgment.

¹⁴Regulation (EU) 2016/679, art 22; Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.

¹⁵*R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

¹⁶*State v Loomis*, 881 N.W.2d 749 (Wis. 2016).

¹⁷OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019); UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021); Council of Europe, Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems.

4. Digital identity systems present a cross-cutting problem because an error can affect multiple services simultaneously. Where one database becomes the gateway to welfare, banking, taxation or mobility, data correction must be rapid and interoperable. The Supreme Court's privacy jurisprudence recognises that informational power requires legality, legitimate aim and proportionality. These principles complement Article 14 by requiring the State to justify why particular data are collected, linked and used in a decision.¹⁸

IX. JUDICIAL METHOD AND EVIDENTIARY BURDENS

1. Courts need not become programmers to review algorithmic action. They routinely assess specialised evidence in medicine, finance, environment and engineering. The judicial task is to identify the legal standard, require the State to produce relevant documentation and test whether the decision process is rational, fair and reviewable. Independent experts or amici may assist in technically complex cases, but the ultimate constitutional judgment must remain with the court.
2. Information asymmetry justifies a modified evidentiary approach. The claimant may know only that an adverse decision was automated and appears inconsistent or discriminatory. The State controls the model, data and audit records. Once the claimant establishes a plausible basis for challenge—such as unexplained inconsistency, significant error, group disparity or denial of reasons—the burden of production should shift to the authority to disclose the system's legal basis, validation and decision record. Adverse inference may be appropriate where required logs were not retained.
3. Trade secrecy should not operate as a constitutional trump card. The State may protect sensitive material through redaction, restricted inspection or expert review, but it must still establish the legality and rationality of its action. A vendor that refuses necessary disclosure should not be eligible to supply a high-impact public system. Public procurement law and tender conditions should therefore incorporate transparency, audit access, data-governance duties, cybersecurity standards and responsibility for discriminatory or inaccurate performance.
4. Judicial review should also distinguish between facial and as-applied challenges. A system may be constitutionally defective in design because it uses an impermissible variable or lacks any mechanism for human review. Alternatively, a generally lawful system may produce an arbitrary result because incorrect data were used in a particular case. The remedy and evidentiary scope will differ, but both forms of challenge are necessary to prevent systemic defects from being reduced to isolated administrative mistakes.

X. OBJECTIONS AND LIMITS

1. One objection is that stringent review will inhibit innovation. The answer is that constitutional safeguards can improve rather than obstruct public innovation by clarifying responsibility, reducing harmful error and increasing public trust. The proposed test does not prohibit automation. It requires the State to match the safeguards to the risk and to demonstrate that the system is suitable for the legal task. A system that cannot meet basic standards of accuracy, explanation or oversight should not be used merely because it is technologically advanced.
2. A second objection is that explainability may reduce predictive accuracy. That trade-off cannot be resolved in the abstract. In high-impact public decisions, marginal gains in statistical performance may not justify a system that cannot provide a legally intelligible reason. The relevant question is not whether the most accurate model is explainable in every technical detail, but whether the State can defend the decisive factors and afford effective contestation. Constitutional administration values legitimacy and fairness alongside efficiency.
3. A third objection is that Article 14 is too general to regulate complex technology. Indian equality doctrine has repeatedly adapted to new forms of State power. The prohibition of arbitrariness is deliberately open enough to examine context, purpose and effect. What is required is disciplined application, not doctrinal abandonment. The structured test

¹⁸Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1; K.S. Puttaswamy (Aadhaar-5J.) v Union of India, (2019) 1 SCC 1.

proposed here channels judicial discretion by identifying concrete questions while preserving flexibility across sectors and technologies.

4. The framework also has limits. It cannot replace sector-specific legislation, technical standards, data-protection enforcement or democratic oversight. Nor can courts alone supervise thousands of systems. Administrative rules should classify high-risk uses, require registration and impact assessment, create audit institutions, establish procurement standards and provide specialised complaint mechanisms. Article 14 supplies the constitutional floor against which those arrangements must be measured.

XI. CONCLUSION

1. Automated State action does not create a constitutional vacuum. It changes the form in which familiar dangers appear: irrelevant considerations become data features, undisclosed policy becomes model architecture, inconsistent discretion becomes variable error, and absence of reasons becomes algorithmic opacity. Article 14 can respond because its central demand is that State power be non-arbitrary, rationally justified and fairly exercised.

2. The proposed Test of Algorithmic Arbitrariness reconstructs judicial review around twelve elements: legality, legitimate purpose, data relevance, data quality, equality, transparency, explainability, procedural fairness, human oversight, auditability, proportionality and effective remedy. Applied with risk-sensitive intensity, the test would enable courts to examine both the individual outcome and the system that produced it. It would also encourage public authorities to build constitutional safeguards into procurement, design and deployment rather than treating rights as an afterthought.

3. The future of digital governance should not be framed as a choice between innovation and constitutionalism. Legitimate innovation in government is innovation that remains answerable to law. Where an algorithm materially shapes access to rights, benefits, liberty or opportunity, the State must be able to show not only that the system works, but that it works lawfully, fairly, transparently and with effective avenues of challenge. That is the minimum promise of equality before the law in an automated age.

BIBLIOGRAPHY

1. Barocas, Solon and Andrew D. Selbst, "Big Data's Disparate Impact" (2016) 104 California Law Review 671.
2. Burrell, Jenna, "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms" (2016) 3 Big Data & Society 1.
3. Citron, Danielle Keats, "Technological Due Process" (2008) 85 Washington University Law Review 1249.
4. Pasquale, Frank, *The Black Box Society* (Harvard University Press 2015).
5. Supreme Court of India decisions concerning Article 14, arbitrariness, procedural fairness, privacy and proportionality.
6. OECD, *Recommendation of the Council on Artificial Intelligence* (2019).
7. UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).