INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJLAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

ALGORITHMIC BIAS AND ARTICLE 14 OF THE INDIAN CONSTITUTION: RETHINKING EQUALITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

AUTHORED BY - PRIYA S

ABSTRACT

Artificial intelligence is increasingly influencing decisions involving employment, credit, education, policing, healthcare, welfare distribution and access to digital services. Although these systems are often presented as neutral and efficient, their outputs may reproduce or intensify social inequalities embedded in historical data, institutional practices and design choices. In India, this concern has a particularly a constitutional character. Article 14 guarantees equality before law and equal protection of laws, while Article 15 protects life, Personal liberty, dignity and privacy. Together, these provisions create a Constitutional framework within which automated decision-making must be assessed.

This Article examines whether algorithmic bias can be understood as a violation of Constitutional equality in India. It argues that the traditional distinction between intentional discrimination and apparently neutral classification is insufficient for algorithmic systems, because discriminatory outcomes may arise without human intention and may remain concealed with complex technical processes. The article analyses the Constitutional principles of reasonable classification, arbitrariness, proportionality, dignity, privacy, natural, justice and judicial review. It also considers the digital data protection Act, 2023 and the comparative value of the European Union's risk-based model of artificial- intelligence regulation. The article proposes a right based Indian framework requiring impact assessments, meaningful explanations, independent audits, human oversight, accessible remedies and special protection for historically disadvantaged communities. It concludes that artificial intelligence should be treated merely as a technological instrument, where it affects rights, it must remain subject to Constitutional morality and accountable public power.

Key words.1) **Artificial Intelligence**, 2) **Algorithmic Bias**, 3) **Constitutional Equality** 4) **Article 14**, 5) **Automated Decision-Making**

1. INTRODUCTION

Artificial intelligence has moved from research laboratories into ordinary Social and governmental life. Algorithms now assists organisations in identifying fraud, assessing risk, screening applications, moderating online content, recommending medical treatment and allocating public benefits. Their attraction is understandable. Automated system can process large volumes of information quickly, identify patterns that may escape human attention and reduce certain form of administrative delay. Yet the speed and apparent objectivity of algorithmic decision-making can conceal serious risks.

An algorithm does not begin from a socially empty space. It is developed by people, trained on data generated by society, deployed through institutional priorities and evaluated according to selected objectives. If the underlying data reflects caste, gender, religious, regional linguistic, disability-related or economic inequality, the resulting system may reproduce those inequalities. A system can therefore discriminate even when its designers do not expressly instruct it to discriminate. The problem may appear through the choice of variable, the equality of training data, the definition of success, or the equal consequence of an apparently uniform ruler.

In India, algorithmic bias must be examined through the constitution. Equality is not restricted to a formal promise that the state must treat everyone identically. Article 14 requires that the state action be non-arbitrary, based on intelligible criteria and rationally connected to a legitimate objective. Constitutional equality also responds to substantive disadvantage. The Supreme Court has repeatedly developed Article 14 beyond a narrow classification test, treating manifest arbitrariness and unjustified state action as constitutionally suspect.

The significance of this issue is heighted by India's digital transformation. Public and private entities increasingly collect extensive personal information and use automated tools to make decision about individuals. The Digital personal Act,2023, recongises the need to protect personal data while permitting lawful processing. A system may process data lawfully and still produce discriminatory outcomes. Consent alone cannot systems in order to obtain employment, education, credit, healthcare and welfare.

This Article argues that India requires a constitutional approach to algorithmic governance. Such an approach must combine innovation with accountability and should insist that efficiency cannot override equality, dignity, privacy or the right to a fair opportunity to challenge an adverse decision.

2. UNDERSTANDING ALGORITHMIC BIAS:

Algorithmic bias refers to systematic and unjustified differences in the outputs or effects of an automated system upon individuals or groups. Bias may be introduced at several stages.

First, historical data must be reflect unequal social conditions. For example, if a recruitment system is trained on past appointments from an industry where women were underrepresented, it may be learn to associate successful employment with characteristics more commonly found among male applicants. The system may not use gender directly, yet it may rely on correlated indicators such as career interruptions, location, educational history, or employment patterns.

Second, bias may arise from data imbalance. A facial-recognition system trained primarily on one population may perform less accurately for other populations. A language model developed mainly from dominant-language material may inadequately understand regional languages, dialects or culturally specific expressions.

Third, the design object may be incomplete. An institution may ask an algorithm to maximize the detection of fraud or the probability of loan repayment. If fairness is not included in the design, the system may treat accuracy as the only value worth protecting. The outcome may be efficient from the institution's perspective while unfair to affected individuals.

Fourth, bias may result from the context of de4ployment. A model that performs adequately in one location may be inappropriate in another. A predictive-system developed using urban data may make unreliable assumptions about rural communities. Similarly, a tool used for low-stakes recommendations may become harmful when used to deny bail, employment, medical treatment or public benefits.

Algorithmic bias should therefore not be understood merely as a coding error. It is often a governance problem. The essential questions are: who designed the system, whose data was used, which values were prioritized, who bear the risk of error, and what remedy is available when the system is wrong?

3.ARTICLE 14 AND AUTOMATED DECISION-MAKING

Article 14 contains two closely connected guarantees; equality before law and equal protection of laws. The first expression a principle of formal equality, while the second permits reasonable differentiation where a distinction serves a legitimate purpose. The classic test requires an intelligible differentia and a rational nexus between the classification and the objective sought.

Automated decision-making complicates this test because the relevant classification may not

be visible. A system may not explicitly classify people by caste, religion or gender, yet variables such as residential location, language, income history, educational institution, surname or online behaviour may operate as proxies. The legal question should therefore focus not only on the stated variables but also on the actual effects and structure of the decision-making process.

Reasonable classification and indirect discrimination

A classification produced by an algorithm must satisfy the same constitutional requirements as a classification produced by a human official. The State cannot avoid Article 14 scrutiny by outsourcing the decision to a private vendor or describing the output as a statistical prediction. If a model systematically disadvantages a protected or vulnerable group, the authority relying on it should be required to demonstrate the legitimacy, necessity and proportionality of the distinction.

This approach is especially important for indirect discrimination. A facially neutral rule may have a disproportionate adverse effect on a particular group. Indian constitutional law has increasingly recognised that equality is concerned with substantive impact, not merely with the presence or absence of an openly discriminatory intention. In algorithmic systems, an effects-based inquiry is indispensable because discriminatory patterns may result from data and design rather than conscious human purpose.

Manifest arbitrariness

The doctrine of manifest arbitrariness permits constitutional review of State action that is capricious, irrational, disproportionate or lacking an adequate determining principle. An automated system may be manifestly arbitrary where it relies on poor-quality data, opaque proxies, unstable correlations or an objective unrelated to the legal purpose for which it is deployed. A decision cannot become rational merely because it is generated by software.

The use of a complex model also creates a risk of “automation deference”, under which officials and courts assume that a technical output is more objective than a human judgment. Constitutional review must resist that assumption. The decision-maker remains responsible for explaining why the system was used, how it was validated and why its output was treated as sufficiently reliable in the particular case.

4. ARTICLES 15 AND 21: DIGNITY, PRIVACY AND FAIRNESS

Article 14 cannot be isolated from Articles 15 and 21. Article 15 prohibits discrimination on specified grounds and permits constitutionally authorised affirmative action. Article 21 protects life and personal liberty, which the Supreme Court has interpreted to include dignity, autonomy, privacy and fair procedure. Together, these provisions support a substantive understanding of equality in digital governance.

Algorithmic systems often depend on extensive personal data. Data about health, financial behaviour, location, language, disability, family relationships and online activity can be combined to generate profiles and predictions. Even where the final decision does not expressly disclose sensitive information, the system may infer sensitive characteristics from apparently ordinary data. This creates risks to informational privacy and decisional autonomy.

The constitutional right to privacy requires more than a formal legal basis for collecting data. State interference must satisfy legality, a legitimate aim, proportionality and procedural safeguards. A system deployed for welfare fraud detection, for example, should be demonstrably necessary for a legitimate purpose, use data proportionately, minimise intrusion and provide safeguards against error. Indefinite retention, function creep and unreviewable profiling are difficult to reconcile with these requirements.

Natural justice is equally important. A person affected by an automated decision should ordinarily receive notice that automation was used, information sufficient to understand the decisive reasons, an opportunity to submit relevant material and access to an independent review. A purely formal human sign-off is inadequate if the official is unable or unwilling to question the algorithmic recommendation.

5. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data and recognises both the individual's interest in protecting personal data and the need to process data for lawful purposes. It requires lawful processing, notice, consent or specified legitimate uses, security safeguards, correction and erasure rights, grievance redressal and institutional oversight. The Act's structure is significant because algorithmic systems commonly depend on automated processing and profiling.

However, data protection is not identical to equality protection. A system may comply with notice and consent requirements while producing discriminatory results. The Act does not, by itself, create a comprehensive right to an explanation of an automated decision, a general

prohibition on discriminatory profiling or a detailed framework for algorithmic impact assessments. Its protections should therefore be read alongside Articles 14, 15 and 21 and other applicable anti-discrimination and sectoral rules.

The distinction also matters because consent can be illusory. Individuals may have no realistic alternative to accepting data processing when applying for a job, seeking credit or accessing a public service. In such situations, constitutional scrutiny must focus on necessity, fairness, accountability and remedy rather than treating consent as conclusive.

6. COMPARATIVE PERSPECTIVE: THE EUROPEAN UNION AI ACT

The European Union's Artificial Intelligence Act adopts a risk-based regulatory model. Regulation (EU) 2024/1689 identifies certain systems as high risk where they may significantly affect health, safety or fundamental rights. It requires safeguards such as risk management, data governance, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity. The Regulation specifically recognises that systems used in employment, access to essential services, law enforcement, education and credit assessment can perpetuate historical discrimination and therefore require heightened scrutiny.

The European model offers useful lessons for India, particularly its focus on the entire lifecycle of a system rather than only the moment of deployment. It also demonstrates the value of classifying uses according to potential harm. Nevertheless, India should not simply copy the EU framework. Indian regulation must account for constitutional reservations, caste-based exclusion, linguistic diversity, unequal digital access, public-sector procurement and the extensive role of government in welfare and identity infrastructure.

7. TOWARDS AN INDIAN FRAMEWORK

A constitutional framework for algorithmic governance in India should contain the following elements:

Algorithmic impact assessments:- Before deploying a system that may significantly affect rights, the responsible authority should identify the purpose, affected communities, data sources, foreseeable harms, alternatives and mitigation measures.

Equality and bias testing:- Systems should be tested across relevant groups, including caste, gender, disability, language, region and socio-economic status where legally and ethically appropriate. Testing should examine both accuracy and disparate impact.

Meaningful explanation:- Affected persons should receive an intelligible explanation of the

decisive factors, the role of automation and the steps available to challenge the outcome. Protection of trade secrets should not become a blanket justification for secrecy.

Human oversight:- A trained and authorised human decision-maker should have genuine power to review, reject or modify the automated output. Human review must not be a ceremonial endorsement.

Independent audits and documentation:- High-impact systems should be subject to independent technical, legal and social audits. Authorities should preserve records concerning training data, model changes, validation, error rates, complaints and corrective action.

Accessible remedies:- Individuals should be able to seek correction, reconsideration, compensation or judicial review without bearing an impossible burden of proving the internal operation of a proprietary model. Courts should be willing to order disclosure, suspension or re-evaluation where constitutional risk is shown.

Public participation and procurement safeguards:- Communities likely to be affected should be consulted before deployment. Government contracts should impose audit, transparency, data-quality, security and remedy obligations on vendors.

Protection against exclusion:- Essential public services should not be denied solely because an automated system produces a negative result. Alternative channels, human assistance and offline access should remain available.

These safeguards should be calibrated according to risk:- A spelling assistant and an automated welfare eligibility system should not face identical obligations. But whenever a system materially influences a person's access to liberty, livelihood, education, healthcare, credit or public benefits, constitutional safeguards should apply at their strongest.

8. JUDICIAL REVIEW AND INSTITUTIONAL RESPONSIBILITY

Indian courts can play a central role in developing these principles through judicial review. The first responsibility lies with the public authority that adopts or relies upon the system. It must establish that the use is authorised, pursues a legitimate purpose, is proportionate, uses reliable data and provides procedural safeguards. A court need not reproduce the entire source code to review legality. It can examine procurement documents, impact assessments, validation studies, error rates, audit reports, reasons given to the affected person and the availability of human review.

The burden should not rest entirely on an individual who cannot access the model or the relevant datasets. Where the claimant establishes a credible pattern of disparate impact or an

unexplained adverse decision, the authority and vendor should be required to provide sufficient information to justify the system. This does not mean that every statistical disparity automatically proves a constitutional violation. It means that secrecy cannot prevent meaningful scrutiny when fundamental rights are at stake.

Courts should also distinguish between an algorithmic recommendation and an algorithmic determination. The greater the system's influence over the final outcome, the stronger the duties of explanation, audit and review. A system that merely organises files presents a different constitutional risk from one that determines whether a person receives a benefit, is selected for investigation or is denied employment.

9. CONCLUSION

Algorithmic bias presents a new form of an old constitutional problem: the unequal distribution of opportunity and power. Its distinctive danger lies in the combination of scale, opacity and the appearance of objectivity. An automated system can reproduce historical inequality while making responsibility difficult to locate.

Article 14 provides a powerful basis for responding to this danger. Its commitments to equality, non-arbitrariness and rational State action can apply to algorithmic systems just as they apply to statutes, policies and administrative decisions. Articles 15 and 21 strengthen this protection by addressing discrimination, dignity, privacy, autonomy and fair procedure. The Digital Personal Data Protection Act, 2023 is relevant but cannot substitute for a broader constitutional framework.

India should therefore move towards rights-based algorithmic governance. High-impact systems should be assessed before deployment, monitored throughout their lifecycle and subject to meaningful human oversight, independent audit and accessible remedies. The objective is not to prevent technological innovation. It is to ensure that technology remains accountable to the Constitution. Artificial intelligence may assist public power, but it cannot replace constitutional morality, reasoned decision-making and the equal dignity of every person.

BIBLIOGRAPHY

1. The Constitution of India, Articles 14, 15 and 21.
2. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, India Code.
3. 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).
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
5. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.
6. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
7. Shayara Bano v. Union of India, (2017) 9 SCC 1.

DETAILS OF AUTHOR

1. NAME OF THE AUTHOR: PRIYA S (V BALLB)
2. EMAIL ID: jayanthipriya179@gmail.com
3. CONTACT NUMBER: 7558121401
4. NAME OF THE INSTITUTION: GOVERNMENT LAW COLLEGE, TRICHY
5. DESTINATION OF AUTHOR: IV BALLB-STUDENT
6. OFFICIAL ADDRESS: QMHW 848, RACE COURSE ROAD, NEAR ANNA STADIUM, KAJAMALAI COLONY, TIRUCHIRAPPALLI-620023
7. THEME: ALGORITHMIC BIAS AND ARTICLE 14 OF THE INDIAN CONSTITUTION: RETHINKING EQUALITY IN THE AGE OF ARTIFICIAL INTELLIGENCE