INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

REGULATING ARTIFICIAL INTELLIGENCE IN INDIA: CONSTITUTIONAL CHALLENGES TO PRIVACY, EQUALITY, AND DUE PROCESS

AUTHOR - BALAMURUGAN S* & NIKITHA SREE**

* STUDENT AT VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES (VISTAS)

** ASSISTANT PROFESSOR AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

BEST CITATION – BALAMURUGAN S & NIKITHA SREE**,** REGULATING ARTIFICIAL INTELLIGENCE IN INDIA: CONSTITUTIONAL CHALLENGES TO PRIVACY, EQUALITY, AND DUE PROCESS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (7) OF 2026, PG. 164-170, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I718

ABSTRACT

The rapid proliferation of Artificial Intelligence (AI) technologies across governance, criminal justice, healthcare, and financial services has precipitated a constitutional crisis in India that existing legal frameworks are ill-equipped to resolve. AI systems — through algorithmic decision-making, predictive policing, biometric surveillance, and automated data profiling — directly impinge upon the fundamental rights guaranteed under Part III of the Constitution of India. This article undertakes a systematic doctrinal and comparative legal analysis of the constitutional dimensions of AI regulation, focusing on the right to privacy under Article 21, the right to equality under Articles 14 and 15, and the right to due process under Article 21. The study critically evaluates the Digital Personal Data Protection Act 2023 (DPDPA) and existing policy instruments against the proportionality framework established in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), identifies five structural constitutional lacunae in the current regulatory architecture, and proposes a rights-centred Constitutional AI Framework Act for India. The research argues that meaningful AI regulation must satisfy the fourfold test of legality, legitimate aim, necessity, and proportionality as enunciated in Puttaswamy, and must be institutionalised through an independent Artificial Intelligence Regulatory Authority of India (AIRAI).

Keywords: artificial intelligence regulation, constitutional law, right to privacy, algorithmic discrimination, due process, Puttaswamy, DPDPA 2023, facial recognition, India

I. INTRODUCTION

Artificial Intelligence (AI) represents the most transformative technological development of the twenty-first century. India — with over 900 million internet users and an ambitious Digital India programme — has enthusiastically adopted AI-driven systems in tax administration (TRACES), welfare delivery (Aadhaar-linked Direct Benefit Transfer), policing (the NCRB's Automated Facial Recognition System), and adjudication (SUPACE in High Courts).1 Yet the constitutional guarantees of privacy, equality, and due process that undergird India's democratic republic remain significantly under-protected against the risks posed by these technologies.

The Supreme Court of India's landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India2 recognised the right to privacy as an intrinsic component of Article 21 and articulated a proportionality standard for evaluating state interference with that right. Four years later, the Digital Personal Data Protection Act 2023 (DPDPA) — India's first

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

comprehensive data protection statute — has been widely criticised for failing to operationalise those constitutional imperatives.3 India has neither a dedicated AI regulatory statute nor an independent regulatory authority, leaving a critical vacuum in constitutional governance.

This article addresses that vacuum. It analyses three inter-related constitutional challenges: AI and privacy (Section II), AI and equality (Section III), and AI and due process (Section IV). Section V critically evaluates the existing regulatory framework and proposes the essential elements of a Constitutional AI Framework Act. Section VI presents findings and recommendations.

II. ARTIFICIAL INTELLIGENCE, PRIVACY, AND ARTICLE 21

A. The Puttaswamy Proportionality Framework

The nine-judge Constitution Bench in Puttaswamy unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution, overruling M.P. Sharma v. Satish Chandra4 and Kharak Singh v. State of Uttar Pradesh5 to the extent they had denied privacy constitutional status. Justice Chandrachud articulated a tripartite conception: (a) restitutional privacy (protection from physical intrusion); (b) informational privacy (control over personal data); and (c) decisional privacy (autonomy over life choices).6 All three dimensions are directly engaged by AI systems.

Critically, Puttaswamy adopted a proportionality standard drawn from German constitutional law: any state action interfering with privacy must satisfy (i) legality — authorisation by law; (ii) a legitimate aim — a constitutionally permissible objective; (iii) necessity — the least restrictive means available; and (iv) proportionality stricto sensu — public benefit not disproportionate to privacy harm.7 This fourfold test is the central constitutional yardstick against which all AI applications must be measured.

B. AI Surveillance and Data Profiling

The National Crime Records Bureau's Automated Facial Recognition System (AFRS), proposed in 2019, envisages real-time facial recognition across CCTV networks, crime databases, passport records, and social media — enabling mass civilian surveillance without judicial authorisation.8 Applying the Puttaswamy test: the AFRS lacks a specific statutory basis (legality fails); population-wide surveillance is not the least restrictive means of achieving crime-prevention objectives (necessity fails); and the chilling effect on freedom of expression and assembly is disproportionate to any demonstrated security benefit (proportionality stricto sensu fails). The AFRS is therefore constitutionally impermissible in its current form.

The 'aggregation problem' identified by Solove is equally acute: individually innocuous data points — location, purchasing behaviour, mobile usage — when combined by AI systems, reveal intimate details of an individual's life without their knowledge or consent.9 AI credit-scoring, health-risk assessment, and CV-screening systems routinely engage in this form of covert profiling, implicating informational privacy under Article 21.

C. Constitutional Inadequacy of the DPDPA 2023

The DPDPA introduces obligations of notice and consent, data minimisation, purpose limitation, and rights of access and erasure.10 However, it exhibits four critical constitutional deficiencies when evaluated against Puttaswamy. First, Section 17(2)(a) grants the central government sweeping exemptions from the Act's provisions for state instrumentalities 'in the interests of sovereignty and integrity of India,' without proportionality safeguards or judicial oversight — placing the AFRS, Aadhaar-AI integrations, and predictive policing beyond the Act's reach. Second, the DPDPA contains no

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

provision equivalent to Article 22 of the GDPR conferring a right not to be subject to solely automated decisions of significant effect.11 Third, the Data Protection Board is constituted entirely by executive appointment, compromising the independence that the rule of law requires. Fourth, the consent framework is structurally inadequate for AI-driven covert profiling.

The EU AI Act 2024's risk-based framework — which prohibits real-time public facial recognition in law enforcement, imposes mandatory Fundamental Rights Impact Assessments for high-risk systems, and requires data protection by design — represents a far more constitutionally adequate model.12

III. ARTIFICIAL INTELLIGENCE AND EQUALITY: ARTICLES 14 AND 15

A. Algorithmic Discrimination and the Constitutional Equality Code

Article 14 guarantees equality before law and equal protection of the laws. The Supreme Court's jurisprudence develops two parallel doctrinal streams: the reasonable classification doctrine (equality as rationality — requiring an intelligible differentia bearing a rational nexus to the object of the classification) and the arbitrariness doctrine established in E.P. Royappa v. State of Tamil Nadu13 (equality as non-arbitrariness). Algorithmic decision-making implicates both. An algorithm using a proxy variable — postcode, educational institution — that correlates strongly with caste or religion fails the rational nexus test because the proxy is not a constitutionally permissible differentia. An algorithm whose outputs cannot be explained or scrutinised is, by constitutional definition, arbitrary.

Article 15 prohibits discrimination on grounds 'only of religion, race, caste, sex, place of birth, or any of them.' Where an AI system uses proxy variables that serve as surrogates for prohibited grounds — dietary preferences as a proxy for religion, maternal language as a proxy for caste — the resulting discrimination engages Article 15 even if the algorithm does not explicitly use the prohibited ground.

B. Predictive Policing and the Presumption of Innocence

State police forces in Telangana, Delhi, and Maharashtra have deployed predictive policing systems without statutory authorisation.14 These systems are trained on historical crime data that reflects existing patterns of discriminatory policing against Scheduled Caste communities and Muslim minorities — producing predictions that systematically over-identify members of these groups as prospective offenders, contrary to Article 15. Furthermore, preventive detention or enhanced surveillance justified by algorithmic probability assessments rather than individualised evidence violates the presumption of innocence embedded in Article 21's due process guarantee as articulated in Maneka Gandhi v. Union of India.15

C. AI in Employment and Financial Services

CV-screening algorithms trained predominantly on the CVs of historically successful employees — disproportionately from upper-caste urban backgrounds — systematically penalise Dalit, Adivasi, and OBC applicants.16 AI-driven credit assessment systems relying on mobile usage patterns and social media activity as proxies for creditworthiness encode socio-economic status correlations that, in India's stratified society, translate directly into caste-based financial exclusion.17 Neither employment nor credit AI systems are currently subject to any non-discrimination obligation under Indian law — a constitutional lacuna that demands urgent legislative remedy.

The disproportionate impact of biometric authentication requirements on women is also well-documented: authentication failure rates among women enrolled in MGNREGS and PDS are significantly higher than among men, reflecting differences in skin condition caused by agricultural labour,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

lower enrolment rates, and lesser digital literacy.18 This constitutes indirect discrimination on the ground of sex contrary to Article 15(1).

IV. ARTIFICIAL INTELLIGENCE AND DUE PROCESS: ARTICLE 21

A. Procedural Fairness in Automated Administrative Decisions

Since Maneka Gandhi, it is settled law that any procedure depriving a person of rights must be 'just, fair and reasonable.'19 The principle of audi alteram partem — one of the twin pillars of natural justice — requires notice of the case against a person and a meaningful opportunity to present their case before a decision is made. When the Income Tax Department's INSIGHT platform or the GSTN's automated scrutiny systems flag a taxpayer's return algorithmically and initiate proceedings without advance notice, without disclosure of the algorithm's reasoning, and without meaningful human review, they violate the procedural requirements of Article 21. This analysis applies equally to AI-driven welfare denial, automated immigration decisions, and algorithmic regulatory enforcement.

B. Explainability and the Right to Reasons

The right to a reasoned decision — constitutionally grounded in the Article 14 arbitrariness doctrine and Article 21's due process guarantee — requires that a decision-maker provide an intelligible explanation sufficient to enable the affected party to understand the decision and challenge it effectively if erroneous.20 The most powerful AI systems — deep neural networks — are characterised by high predictive accuracy but low interpretability. Their internal workings cannot map onto the kind of rule-based reasoning that courts and tribunals can scrutinise. Constitutional compliance therefore requires what Wachter, Mittelstadt, and Russell term 'actionable counterfactual explanations': statements of the form 'your application would have been approved if your income had been 15% higher and your repayment history had shown fewer delays.'21

C. AI in the Judicial Process

The Supreme Court's deployment of SUPACE as an AI research assistant for judges raises distinct due process concerns. If an AI tool systematically surfaces certain legal authorities and omits others — even inadvertently — it influences judicial reasoning without the knowledge or consent of the parties. The parties' right to a fair trial under Article 21 includes a right to be heard on the legal authorities that will govern the decision. Constitutional minimum requirements include: (a) independent audit of judicial AI tools; (b) notification to parties when AI tools have been used; and (c) an opportunity to comment on AI-generated research outputs before judgment. None of these safeguards currently exist.

V. THE REGULATORY FRAMEWORK: CRITIQUE AND PROPOSED REFORMS

A. Structural Deficiencies in the Existing Architecture

India's existing AI regulatory architecture — the IT Act 2000, the DPDPA 2023, NITI Aayog's non-binding policy documents, and sector-specific instruments from SEBI, RBI, and IRDAI — exhibits five structural deficiencies: (i) fragmentation, with no single instrument addressing AI comprehensively; (ii) absence of risk-based categorisation; (iii) reliance on aspirational rather than legally enforceable commitments; (iv) regulatory gaps in automated decision-making, algorithmic discrimination, and judicial AI; and (v) institutional deficit — no independent AI regulatory authority exists. The Vidhi Centre for Legal Policy's comprehensive mapping of India's AI governance landscape confirms these conclusions.22

B. Comparative Lessons

Three models inform India's reform agenda. The EU AI Act 2024 classifies AI systems by risk — prohibited (mass facial recognition,

social credit scoring), high-risk (criminal justice, welfare administration, healthcare AI), limited risk, and minimal risk — and imposes graduated compliance obligations including mandatory Fundamental Rights Impact Assessments and human oversight requirements.23 Canada's Directive on Automated Decision-Making provides the most detailed operationalisation of due process requirements: Level IV decisions with irreversible, life-altering impacts require mandatory human review.24 The UK's pro-innovation, sector-specific approach — while offering regulatory flexibility — is inadequate for India's weaker sectoral regulatory infrastructure.

C. Proposed Constitutional AI Framework Act

Drawing on the constitutional analysis above and the comparative lessons identified, this article proposes that the Parliament of India enact a Constitutional AI Framework Act incorporating the following essential elements:

- A Risk Classification System: AI systems classified into prohibited risk (mass biometric surveillance, social credit scoring), high risk (criminal justice, welfare, immigration, judicial processes, healthcare diagnostics), limited risk, and minimal risk. Prohibited-risk applications banned; high-risk applications subject to pre-deployment conformity assessments.
- A Statutory Explanation Right: For all high-risk AI decisions, the affected individual must receive (a) notice that an algorithmic system has been used; (b) a meaningful plain-language explanation of the decision basis; and (c) information about the right to seek human review.
- Mandatory Equality Impact Assessments: Prior to deployment, all high-risk public AI systems must undergo a published Equality Impact Assessment evaluating differential impacts on constitutionally protected groups.
- Fundamental Rights Impact Assessments: A constitutionally grounded FRIA evaluating compatibility with Articles 14, 15, and 21 and the Puttaswamy proportionality standard must precede every high-risk state AI deployment.
- An independent Artificial Intelligence Regulatory Authority of India (AIRAI): Constituted with security of tenure, financial independence, and multi-stakeholder appointment processes insulated from executive control; empowered to investigate, audit, direct, and sanction.
- Data Protection by Design: AI systems must incorporate privacy protections — data minimisation, purpose limitation, access controls — at the design stage. The DPDPA must be amended to impose this obligation.

VI. FINDINGS AND RECOMMENDATIONS

A. Major Findings

This research establishes the following conclusions:

- The constitutional framework — privacy under Article 21 (Puttaswamy), equality under Articles 14 and 15, and due process under Article 21 (Maneka Gandhi) — is fully applicable to state AI deployments and provides a robust foundation for evaluating their legality.
- Several AI applications currently deployed by Indian government agencies — the AFRS, predictive policing systems, and automated welfare denial through Aadhaar-linked biometrics — manifestly fail the Puttaswamy proportionality standard and are constitutionally impermissible.
- The DPDPA 2023 is constitutionally inadequate: its broad state exemptions, absence of automated decision-making rights, executive-controlled regulator,

and deficient consent framework render it insufficient as an AI governance instrument.

- AI systems trained on historically biased data systematically reproduce caste, gender, and religious discrimination in hiring, lending, policing, and welfare delivery — violating the substantive non-discrimination mandate of Articles 14 and 15.
- Automated administrative decisions in India are made without adequate notice, hearing, or explanation, violating Article 21's procedural guarantees. India lacks an effective constitutional due process framework for algorithmic governance.

B. Recommendations

On the basis of the foregoing findings, eight recommendations are advanced. First, the Parliament must enact a Constitutional AI Framework Act incorporating risk classification, explanation rights, impact assessments, and mandatory human review. Second, an independent AIRAI must be established by statute. Third, the DPDPA must be amended to remove blanket state exemptions, introduce automated decision-making rights, reconstitute the Data Protection Board through independent appointment, and extend coverage to aggregated and derived data used in profiling. Fourth, MeitY and the AIRAI must jointly develop an Equality Impact Assessment framework. Fifth, the Supreme Court and High Courts must formulate procedural rules for judicial AI disclosure. Sixth, the deployment of the NCRB's AFRS must be suspended until a specific statutory framework satisfying the Puttaswamy proportionality standard is enacted. Seventh, the National Commissions for Scheduled Castes, Women, and Minorities must be empowered to receive complaints about algorithmic discrimination. Eighth, AI literacy programmes for judges, administrative tribunals, and regulatory agencies must be established through the National Judicial Academy and the National Law Universities.

VII. CONCLUSION

Artificial Intelligence is not merely a technological phenomenon — it is a constitutional event. When the state deploys AI systems to make decisions about the liberty, welfare, and dignity of its citizens, it exercises governmental power in a form that existing constitutional frameworks were not designed to govern. This article has demonstrated that the constitutional tools for that governance are already available: the proportionality standard of Puttaswamy, the arbitrariness doctrine of Article 14, the anti-discrimination mandate of Article 15, and the procedural fairness requirements of Maneka Gandhi together constitute a robust constitutional framework for regulating AI.

What India currently lacks is not constitutional doctrine but legislative will — the will to translate constitutional commitments into enforceable legal obligations, independent institutional infrastructure, and effective remedies. An India that embraces AI-driven governance without constitutional guardrails risks building a surveillance state that violates the privacy of 1.4 billion citizens, an algorithmic caste system that perpetuates the inequalities the Constitution sought to dismantle, and an administrative machine that makes consequential decisions about human lives without accountability or recourse.

The constitutional vision of a free, equal, and dignified republic demands a Constitutional AI Framework Act. The doctrinal foundation and normative direction for that project are provided in this research. The time for legislative action is now.

REFERENCES

1 Ministry of Electronics and Information Technology, 'Digital India Programme: Annual Report 2023-24' (MeitY 2024) 12-18.

2 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Constitution Bench).

3 Internet Freedom Foundation, 'Analysis of the Digital Personal Data Protection Act, 2023' (IFF Working Paper 2023) 3-9.

4 M.P. Sharma v. Satish Chandra AIR 1954 SC 300.

5 Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295.

6 Puttaswamy (n 2) para 310 (Chandrachud J).

7 ibid para 325; Shreya Singhal v. Union of India (2015) 5 SCC 1, para 74.

8 National Crime Records Bureau, 'Request for Proposal: Automated Facial Recognition System' (NCRB 2019) 4-7.

9 Daniel J. Solove, Understanding Privacy (Harvard University Press 2008) 140-146.

10 Digital Personal Data Protection Act 2023, ss 5-16.

11 Regulation (EU) 2016/679 (GDPR), art 22.

12 Regulation (EU) 2024/1689 (EU AI Act), arts 5-7, 9, 13, 14.

13 E.P. Royappa v. State of Tamil Nadu AIR 1974 SC 555, para 85.

14 Bedavyasa Mohanty, 'Policing India's Streets with Artificial Intelligence' (2021) 56 Economic and Political Weekly 17.

15 Maneka Gandhi v. Union of India AIR 1978 SC 597, para 56.

16 Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women' Reuters (London, 10 October 2018).

17 Shyam Divan and Arghya Sengupta, 'Digital Credit, Caste and Constitutional Equality' (2022) 57 Economic and Political Weekly 23.

18 Reetika Khera (ed), Dissent on Aadhaar: Big Data Meets Big Brother (Orient Blackswan 2019) 112-130.

19 Maneka Gandhi (n 15).

20 S.N. Mukherjee v. Union of India (1990) 4 SCC 594 [reasons necessary for administrative decisions].

21 Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box' (2018) 31 Harvard Journal of Law & Technology 841.

22 Vidhi Centre for Legal Policy, 'Mapping India's AI Governance Landscape' (Vidhi Report 2022) 4-12.

23 EU AI Act 2024 (n 12), arts 5-7.

24 Treasury Board of Canada Secretariat, 'Directive on Automated Decision-Making' (Government of Canada 2019, as amended 2023), s 6.3.