IMPACT FACTOR 5.397 (SJIF USA)

BIHAR SHODH SAMAAGAM

Multidisciplinary, Multi-Lingual, Peer Reviewed /Refereed Open Access Journal
Vol. 4, Issue 1, January-March, 2026
Available online : https://www.biharshodhsamaagam.com/

ISSN : 3048-6971

Cyber Law, Artificial Intelligence, and Data Privacy in India: Bridging an Incomplete Regulatory Architecture

AUTHOR : GAURAV PANIA

CO AUTHOR: APOORVA JINDAL

https://doi.org/10.5281/zenodo.19408793

Abstract

Artificial intelligence is no longer peripheral to India's digital ecosystem; it is embedded within its administrative, financial, and social infrastructures. This shift has sharpened long-standing concerns around privacy, surveillance, and legal accountability. While the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) and the enactment of the Digital Personal Data Protection Act, 2023 signal meaningful progress, the regulatory response remains uneven. This article argues that India's current framework, though increasingly rights-oriented, remains insufficiently attentive to the distinct risks posed by AI systems—particularly opacity, automated decision-making, and diffuse liability. Drawing on doctrinal analysis and comparative developments, it suggests that India's legal architecture is evolving, but not yet coherently aligned with the realities of algorithmic governance.

Keywords: Artificial Intelligence, Data Privacy, Cyber Law, Algorithmic Governance, India

1. Introduction

There is now little ambiguity about the role artificial intelligence plays in India's governance model. Whether in welfare distribution, digital payments, or predictive analytics in policing, AI is not merely an auxiliary tool—it is becoming infrastructural. Programmes such as Aadhaar and the expansion of real-time payment systems illustrate how deeply data-centric logics have been internalised within the state.

Yet the legal framework has not kept pace in any straightforward way. The Information Technology Act, 2000, conceived in a very different technological moment, continues to operate as the backbone of cyber regulation. Even with subsequent amendments and the introduction of the DPDP Act, 2023, one senses a certain disjuncture: the law speaks fluently about data, but only indirectly about the systems that process it.

This article proceeds from a simple claim. India's regulatory model is not static—it is adapting—but its adaptation remains partial. The emphasis on data protection, while necessary, does not fully capture the legal implications of AI-driven decision-making. What emerges, therefore, is a framework that is normatively ambitious but operationally incomplete.

2. Constitutional and Statutory Foundations

Any discussion of data governance in India must begin with *Puttaswamy*. The judgment did more than recognise privacy; it reorganised the terms in which state power over information is evaluated. By embedding privacy within Article 21 and articulating proportionality as a governing standard, the Court created a vocabulary that now shapes debates well beyond surveillance.

Subsequent decisions—particularly the Aadhaar litigation and *Anuradha Bhasin*—extend this logic, albeit unevenly. They suggest a judiciary increasingly attentive to the implications of digital infrastructures, even if not always explicitly engaging with AI as such. What is notable is not doctrinal completeness, but a gradual shift in judicial sensitivity.

On the statutory side, the picture is more fragmented. The IT Act continues to prioritise cybersecurity and intermediary regulation. It is, in many respects, reactive—designed to address identifiable harms rather than systemic risks. The DPDP Act, 2023 marks a departure, introducing a more structured approach to personal data processing. Consent, purpose limitation, and fiduciary responsibility now occupy a central place.

Even so, the Act remains curiously silent on certain questions. It regulates data flows, but not quite the logic of decision-making built upon them. There is no explicit engagement with automated decisions, nor with the interpretability of algorithmic outputs. This silence is not accidental; it reflects a legislative choice to remain technologically neutral. Whether that neutrality is sustainable is another matter.

3. AI-Specific Legal Challenges

What complicates matters is that AI systems do not fit neatly within existing legal categories. They generate harms that are often indirect, probabilistic, and difficult to trace.

Opacity is perhaps the most frequently cited concern, and for good reason. When decisions—credit approvals, risk

assessments, eligibility determinations—are mediated through models that resist explanation, traditional notions of accountability begin to fray. One cannot meaningfully challenge what one cannot understand.

Then there is the question of bias. In a society as stratified as India's, the risk that algorithmic systems will reproduce existing inequalities is not merely theoretical. Constitutional protections exist, certainly, but their reach into privately deployed AI systems remains uncertain. The result is a regulatory gap that is difficult to ignore.

Surveillance presents a different, though related, problem. The increasing use of facial recognition and predictive tools in law enforcement raises familiar concerns, but at a different scale. The issue is no longer isolated intrusion; it is the normalisation of continuous monitoring. Here, constitutional doctrine provides a framework, but not always a clear answer.

Liability, finally, remains unsettled. When harm results from an AI system, responsibility is rarely singular. Developers, deployers, and users are entangled in ways that traditional legal doctrines were not designed to address. The law, in this respect, appears to be catching up after the fact.

4. Comparative and Institutional Perspectives

A comparative glance is instructive, if only to highlight what is missing. The European Union, through the GDPR and the proposed AI Act, has moved toward a more explicit engagement with algorithmic systems. The emphasis on risk classification, transparency, and human oversight signals a willingness to regulate not just data, but decision-making processes themselves.

India's approach is more cautious, perhaps deliberately so. Sectoral regulators have begun to respond—particularly in finance—but these interventions remain limited in scope. They address immediate risks without necessarily contributing to a broader regulatory philosophy.

International principles, such as those articulated by the OECD, have found rhetorical acceptance. Yet their translation into binding norms remains tentative. This is not unusual; legal systems often absorb such principles gradually. Still, the gap between articulation and implementation is noticeable.

5. Conclusion

It would be inaccurate to suggest that India lacks a framework for governing AI. What exists, however, is better described as an assemblage—constitutional principles, statutory provisions, and sectoral regulations that do not always align neatly.

The challenge, then, is one of integration. Data protection, as currently conceived, addresses only part of the problem. AI systems raise questions that extend beyond privacy—questions of fairness, accountability, and institutional competence.

A more coherent approach would likely involve a combination of general principles and sector-specific rules, supported by regulatory capacity that is, at present, still developing. Whether this takes the form of dedicated AI legislation or incremental reform is, in some ways, a secondary question.

What matters more is the direction of travel. If the law continues to engage with AI only indirectly, the gap between technological capability and legal oversight will persist. Closing that gap is not simply a matter of regulatory design; it is central to maintaining public trust in an increasingly automated state.

References.

1. *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1
2. *Anuradha Bhasin v Union of India* (2020) 3 SCC 637
3. Information Technology Act 2000
4. Digital Personal Data Protection Act 2023
5. NITI Aayog, *National Strategy for Artificial Intelligence* (2018)
6. OECD, *Principles on Artificial Intelligence* (2019)
7. CERT-In, *Annual Report 2022* (MeitY 2023)