2026 Volume: 02 Issue: 09 www.ijrpa.com ISSN 2456- Review Article

International Journal Research Publication Analysis

Page: 01-10

ARTIFICIAL INTELLIGENCE AND LAW IN INDIA: REGULATING INNOVATION, ACCOUNTABILITY AND EMERGING AI RISKS

***Khushi Mohammed Suleman Patel**

India.

Article Received: 07 August 2026
Article Revised: 27 August 2026
Published on: 17 September 2026

***Corresponding Author: Khushi Mohammed Suleman Patel**
India.

DOI: https://doi-doi.org/101555/ijrpa.7572

1. ABSTRACT

Artificial intelligence (AI) is rapidly becoming an important component of governance and public administration in India. It can improve public service delivery, automate routine bureaucratic functions, assist evidence-based policymaking, and support sectors such as healthcare, agriculture and urban administration. At the same time, the deployment of AI by public authorities raises significant legal and constitutional questions concerning privacy, equality, transparency, accountability, data protection, employment, and the right to an effective remedy. This article examines the emerging legal framework for AI governance in India through constitutional principles, particularly Articles 14, 19 and 21 of the Constitution. It considers the Digital Personal Data Protection Act 2023, the Information Technology framework, the Bharatiya Nyaya Sanhita 2023, the 2026 India AI Governance Guidelines, and recent policy developments. It also examines algorithmic bias, deepfakes and synthetic information, the black-box problem, AI-related liability, intellectual property, autonomous AI agents and judicial review of AI-assisted administrative action. It argues that India should pursue a proportionate, risk-based and rights-oriented framework rather than either unregulated innovation or excessive prohibition. AI should remain a tool for public welfare while identifiable human institutions continue to bear legal responsibility for decisions made with its assistance.

2. KEYWORDS: Artificial Intelligence; AI Governance; Constitutional Law; Data Protection; Algorithmic Accountability.

3. INTRODUCTION

Artificial intelligence has moved from being a specialised technological innovation to a significant instrument of contemporary governance. Governments increasingly use machine-learning systems, predictive analytics, automated decision-support tools, facial recognition, natural-language systems and other forms of AI to improve administrative efficiency. In India, the potential applications are particularly extensive because public administration operates at a vast scale and frequently deals with complex datasets relating to citizens, welfare delivery, taxation, healthcare, agriculture, policing and urban development.

The attraction of AI is understandable. Automated systems can process large quantities of information more quickly than human officials, identify patterns that may not be immediately visible, assist in allocating public resources and reduce repetitive administrative work. AI can therefore contribute to more responsive and evidence-based governance. However, technological efficiency cannot by itself determine the legality of governmental action. When an algorithm influences a decision affecting an individual's liberty, privacy, livelihood, reputation or access to public benefits, constitutional requirements governing State action remain applicable.

The legal problem is therefore not simply whether India should use AI, but how it should use AI consistently with the rule of law. A system may be technically accurate and still be legally problematic if the affected person does not know that an automated process was used, cannot challenge the relevant information, or has no meaningful avenue for human review. Similarly, an algorithm trained on historical data may reproduce existing social inequalities while appearing neutral because its output is expressed mathematically.

India's emerging approach is distributed across constitutional principles, existing legislation, sectoral regulation and policy instruments rather than a single comprehensive AI statute. The India AI Governance Guidelines released in 2026 reflect a principle-based approach that seeks to encourage innovation while promoting safe, trusted and inclusive AI. The challenge is to convert these broad principles into enforceable safeguards where AI exercises or materially influences public power.

4. Rise of AI and the New Legal Landscape

AI is increasingly being used in areas traditionally associated with governmental decision-making. In agriculture, predictive systems can assist with crop assessment, weather analysis and resource allocation. In healthcare, AI can support diagnostics, triage and population-level planning. In smart-city administration, algorithmic tools can assist with traffic management,

infrastructure planning and public-service optimisation. In welfare administration, automated systems can help identify beneficiaries and detect irregularities. These applications demonstrate that AI is not confined to private commercial activity; it can directly shape the relationship between citizens and the State.

The legal significance of this development lies in the nature of governmental power. An error by a private recommendation system may cause inconvenience, but an error by a government algorithm can result in denial of a benefit, adverse classification, surveillance, investigation or other serious consequences. Consequently, AI used by public authorities should be assessed not merely through the lens of technological performance but through legality, fairness, proportionality and accountability.

The 2026 India AI Governance Guidelines indicate a preference for a flexible governance architecture rather than immediate reliance on a single omnibus AI statute. Their principle-based approach recognises that AI technology develops quickly and that rigid legislation can become obsolete. At the same time, the framework contemplates institutional mechanisms, technical standards, targeted legal amendments, sandboxes and safety-oriented oversight. This approach provides a useful foundation, but its success will depend on implementation and the extent to which rights-protective principles become operational safeguards.

5. India's Present AI Governance Approach

India presently regulates AI through a combination of general laws, constitutional doctrine, sector-specific rules and government policy. The Information Technology Act 2000 and rules made under it remain important for online harms and intermediary responsibilities. The Digital Personal Data Protection Act 2023 provides a general statutory framework for processing digital personal data, subject to its scope and exemptions. The Bharatiya Nyaya Sanhita 2023 and other criminal laws may apply where AI-assisted conduct results in recognised offences. Intellectual property legislation also remains relevant to AI-generated and AI-assisted works.

The Office of the Principal Scientific Adviser's 2026 white paper on strengthening AI governance through a techno-legal framework describes India's existing architecture as a combination of baseline regulations, sectoral guidelines, policy measures and intellectual-property laws. It recognises that the immediate issue is not necessarily the creation of a completely separate AI Act, but timely adaptation of existing law, effective enforcement and the development of governance institutions capable of addressing emerging risks.

This incremental model has advantages. It avoids unnecessary duplication and allows established legal doctrines to evolve with technology. However, it can also produce regulatory uncertainty. Different harms may fall under different statutes, while questions concerning algorithmic transparency, auditability, explainability and allocation of responsibility may not be directly addressed by existing provisions. A coherent framework is therefore necessary even if it does not take the form of one comprehensive statute.

6. Deepfakes and Synthetic Information

Generative AI has created a particularly urgent legal problem through deepfakes and other forms of synthetic information. AI can generate convincing images, audio and video that falsely depict individuals as saying or doing things that never occurred. Such material can affect privacy, reputation, elections, commercial interests and public trust. It can also complicate the evidentiary process because the mere existence of a digital recording no longer necessarily establishes its authenticity.

Indian regulation has increasingly recognised the need to impose responsibilities on intermediaries in relation to synthetically generated information. The broader legal response must nevertheless address the entire chain of responsibility, including creators, deployers, platforms and persons who knowingly distribute harmful synthetic content. Effective regulation should distinguish between legitimate creative or educational uses and deceptive material designed to cause harm.

Courts will also need to develop practical evidentiary standards for determining authenticity. Digital forensic verification, provenance mechanisms, metadata, secure logging and expert testimony may become increasingly important. The law must balance these safeguards with freedom of expression and legitimate technological experimentation.

7. AI, Privacy and Data Protection

Privacy is one of the most significant constitutional issues arising from AI. Machine-learning systems often require large datasets, and the value of AI may depend on the ability to combine, analyse and infer information about individuals. The constitutional right to privacy recognised in Justice K.S. Puttaswamy v. Union of India therefore provides a central framework for assessing intrusive uses of AI.

The constitutional analysis requires attention to legality, legitimate State purpose and proportionality. An AI system used for surveillance cannot be justified merely because it is technologically capable. There must be a lawful basis for the interference, a legitimate

objective and a rational and proportionate relationship between the means adopted and the purpose pursued. Less intrusive alternatives, retention limits, access controls and safeguards against misuse are therefore relevant to legality.

The Digital Personal Data Protection Act 2023 strengthens India's data-protection architecture, but its operation must be understood together with its statutory exemptions and the particular context in which government agencies process data. AI governance should ensure that exemptions designed for legitimate public purposes do not become a substitute for accountability. Independent oversight, security safeguards and clear limitations on secondary use of personal data remain essential.

8. AI and Article 14: Equality and Non-Arbitrariness

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws. Its relevance to AI is substantial because algorithmic systems can reproduce discriminatory patterns hidden in training data. A model may appear neutral while systematically producing worse outcomes for particular groups because the historical data on which it was trained reflects unequal access, biased enforcement or structural disadvantage.

The Supreme Court's jurisprudence has developed Article 14 beyond formal classification to include protection against arbitrariness. In E.P. Royappa v. State of Tamil Nadu and subsequent decisions, equality has been understood as inconsistent with arbitrary State action. This principle is highly relevant where a government agency relies upon an opaque automated score without being able to explain the factors that materially affected the outcome.

Algorithmic equality therefore requires more than removing explicitly discriminatory variables. Authorities should test outcomes for disparate effects, assess the quality and representativeness of training data, conduct periodic audits and maintain mechanisms for correcting erroneous classifications. Where a system materially affects fundamental rights, the burden of justification should rest with the public authority using the technology.

9. AI and Article 21: Life, Liberty and Human Dignity

Article 21 protects life and personal liberty and has been interpreted broadly to encompass dignity, autonomy, privacy and procedural fairness. In Maneka Gandhi v. Union of India, the Supreme Court connected procedure with fairness, reasonableness and non-arbitrariness. The use of AI in governance must therefore be consistent not merely with formal statutory authority but with fair procedure.

An automated administrative decision may affect employment, welfare, education, healthcare or liberty. If an individual receives an adverse decision without knowing the basis on which it was produced, the practical ability to challenge the decision may be severely limited. Human review is therefore not merely a technological preference; in high-impact situations it can be a component of constitutional fairness.

The principle of human dignity also requires caution where AI systems attempt to predict behaviour or classify individuals. Prediction is inherently probabilistic. Treating a statistical probability as a conclusive determination about a person can undermine individual autonomy and the presumption that each person must be judged on relevant facts rather than stereotypes.

10. The Black-Box Problem: Transparency and Explainability

Many modern AI systems are difficult for ordinary users, administrators and even technical experts to interpret. This is commonly described as the 'black-box' problem. When a government decision is based materially on such a system, opacity can conflict with the basic requirements of accountable administration.

Explainability should not necessarily mean disclosure of proprietary source code in every case. A more practical legal requirement is meaningful explanation: the authority should be able to state why the system was used, what category of data influenced the outcome, what limitations or error rates exist, who validated the system, and how a person can challenge the result. Courts and regulators should also have access to sufficient technical information to conduct independent review.

Transparency is especially important when public authorities procure AI systems from private vendors. Government cannot outsource constitutional responsibility to a contractor. Procurement agreements should therefore contain audit rights, documentation requirements, security standards, incident reporting obligations and mechanisms for independent testing.

11. Liability for AI-Related Harm

One of the most difficult questions in AI law is determining who is responsible when an AI system causes harm. A single outcome may involve the developer who designed the model, the supplier who provided the system, the public authority that deployed it, the officer who relied on its recommendation and the person who supplied or manipulated the underlying data.

Traditional liability rules are based on identifiable human conduct, but AI systems can complicate causation because an output may result from interactions among training data, model architecture, deployment settings and user instructions. This does not justify creating a responsibility vacuum. Where the State deploys AI, the relevant public authority should remain accountable for decisions taken in its name, even when technical functions have been outsourced.

Legal reform should therefore focus on traceability and responsibility allocation. Records should identify the system used, the version deployed, the relevant data sources, material human interventions and the final decision-maker. Such documentation can assist courts in determining causation and prevent public authorities from treating algorithmic output as an unchallengeable fact.

12. AI and Intellectual Property

AI raises important intellectual-property questions. Generative systems can be trained on large quantities of copyrighted material, while their outputs may resemble existing works. Indian copyright law was developed before generative AI became widespread and therefore does not answer every contemporary question with certainty.

Key issues include the lawful use of copyrighted works for training, ownership of AI-generated outputs, originality, infringement, attribution and the rights of human creators. A balanced approach should protect legitimate creative incentives without preventing socially beneficial research and technological development. Policymakers should also consider transparency concerning training data and contractual arrangements between creators and AI developers.

13. AI Agents and Emerging Autonomous Decision-Making

The next stage of AI development involves systems capable of taking actions rather than merely generating information. AI agents may interact with software, initiate transactions, communicate with users and execute multi-step tasks. This creates new legal questions concerning authority, consent, authentication and liability.

Where an AI agent performs a transaction or makes a consequential decision, the law must identify whose act it legally represents. An agent should not be treated as a separate legal person merely because it operates autonomously. Responsibility should remain traceable to the human or institution that authorised and deployed the system, subject to appropriate contractual and statutory allocation of risk.

These questions are becoming practically relevant in financial and digital services. Governance mechanisms such as identity registries, transaction limits, authentication protocols, logging and rapid dispute resolution can reduce the risk of unauthorised or erroneous automated actions.

14. Human Oversight and Judicial Review

Human oversight should be a core principle of high-impact AI governance. The presence of a human somewhere in the process is not enough if that person simply accepts the algorithmic recommendation without meaningful review. Effective oversight requires competence, authority to disagree with the system and access to the information necessary to understand its limitations.

Judicial review provides an additional safeguard. Courts can examine whether an authority had legal power to use an AI system, whether relevant considerations were taken into account, whether the process was arbitrary, whether fundamental rights were disproportionately affected and whether the decision was supported by reliable evidence. The traditional grounds of judicial review therefore remain relevant even when the administrative process becomes technologically sophisticated.

The courts may increasingly need technical assistance through independent experts, amicus submissions and disclosure obligations. The objective should not be for judges to become programmers, but to ensure that technological complexity does not become a shield against legal scrutiny.

15. Critical Analysis: Does India Need a Separate AI Law?

The question whether India needs a separate AI statute cannot be answered simply by choosing between legislation and no legislation. A comprehensive standalone law may provide clarity and institutional coordination, but it could also become rigid in a rapidly changing technological environment. Conversely, reliance entirely on existing statutes may leave important gaps concerning algorithmic accountability.

A preferable approach may be a layered framework. General principles can be established through legislation, while technical standards and sector-specific rules can be updated more frequently. High-risk applications should attract stronger safeguards than low-risk uses. This would allow innovation to continue while recognising that an AI system used to recommend a movie and an AI system used to influence a person's liberty should not be regulated in the same manner.

The 2026 governance approach is significant because it moves the debate toward risk-based and principle-based regulation. However, voluntary guidance alone may be insufficient for applications that materially affect fundamental rights. In such areas, enforceable duties, independent oversight and effective remedies are necessary.

16. Suggestions and Reforms

1. Adopt a clear risk-based classification system distinguishing low-risk, limited-risk and high-impact AI applications.
2. Establish mandatory algorithmic impact assessments before deployment of AI systems that may materially affect fundamental rights.
3. Guarantee meaningful human review and an effective mechanism to challenge high-impact automated decisions.
4. Require public authorities to maintain audit trails, technical documentation, model versions, data-governance records and incident reports.
5. Introduce independent algorithmic audits, including testing for discriminatory outcomes and security vulnerabilities.
6. Strengthen transparency in public procurement by requiring government contracts with AI vendors to contain audit, disclosure, security and accountability clauses.
7. Ensure that privacy exemptions for legitimate State functions remain subject to necessity, proportionality, security and independent oversight.
8. Develop clear evidentiary standards for AI-generated or AI-assisted material, including authentication and provenance mechanisms.
9. Create accessible remedies for individuals harmed by erroneous or discriminatory AI-assisted decisions.
10. Promote regulatory sandboxes and technical standards so that innovation can be tested safely before large-scale deployment.

17. CONCLUSION

Artificial intelligence presents India with both a governance opportunity and a constitutional challenge. It can make public administration faster, more responsive and more capable of handling complex datasets, but the same systems can amplify bias, invade privacy, obscure responsibility and make it difficult for citizens to challenge decisions. The appropriate legal response is neither unrestricted technological optimism nor blanket prohibition. India needs a

proportionate framework in which the intensity of regulation corresponds to the risk created by the application.

The constitutional values of equality, liberty, dignity, privacy and non-arbitrariness should remain the foundation of AI governance. Existing legislation can provide much of the legal infrastructure, but high-impact applications require clearer statutory duties, independent auditing, meaningful human oversight and effective remedies. Most importantly, AI must remain a tool of government rather than a substitute for governmental responsibility. An authority should not be able to avoid legal accountability by saying that 'the algorithm decided'. The guiding principle should therefore be simple: innovate responsibly, regulate proportionately and keep human institutions accountable for the exercise of public power.

18. REFERENCES / BIBLIOGRAPHY

A. Primary Legislation and Constitutional Sources

1. Constitution of India 1950, arts. 14, 19, 21, 32 and 226.
2. Information Technology Act 2000.
3. Digital Personal Data Protection Act 2023.
4. Bharatiya Nyaya Sanhita 2023.
5. Bharatiya Nagarik Suraksha Sanhita 2023.
6. Bharatiya Sakshya Adhiniyam 2023.
7. India AI Governance Guidelines 2026, Government of India.

B. Case Law

8. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.
9. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
10. A.K. Kraipak v. Union of India, (1969) 2 SCC 262.
11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

C. Policy and Secondary Sources

12. Office of the Principal Scientific Adviser, Government of India, White Paper: Strengthening AI Governance Through Techno-Legal Framework (2026).
13. Government of India, India AI Governance Guidelines (2026).
14. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act).
15. European Union, Directive (EU) 2016/680 (Law Enforcement Directive).
16. Regulation (EU) 2016/679 (General Data Protection Regulation).