
ARTIFICIAL INTELLIGENCE AND GOVERNANCE: OPPORTUNITIES, CHALLENGES AND THE NEED FOR A ROBUST LEGAL FRAMEWORK IN INDIA

***Poonam Prajapati**

B Wing 206, Madhav Residency 2, Dandiwad Faliya Balitha Vapi.

Article Received: 16 September 2026

***Corresponding Author: Poonam Prajapati**

Article Revised: 06 October 2026

B Wing 206, Madhav Residency 2, Dandiwad Faliya Balitha Vapi.

Published on: 26 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.4640>

ABSTRACT

Artificial Intelligence (AI) is increasingly influencing public administration, healthcare, education, finance, agriculture, transport, policing and commercial activity in India. AI can improve the speed, scale and accessibility of services, support evidence-based decision-making and stimulate innovation. At the same time, its use raises serious questions concerning privacy, discrimination, transparency, accountability, intellectual property, misinformation, cybersecurity and the right to an effective remedy. India's legal response is developing through existing laws, sectoral regulation and policy guidance rather than through one comprehensive AI statute. Important legal instruments include the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, consumer-protection and intellectual-property laws, and constitutional guarantees. The India AI Governance Guidelines released in November 2025 provide a principle-based framework built around seven guiding principles, while recommending institutional coordination and risk mitigation. This paper examines the opportunities and risks of AI, the relevant Indian legal framework, constitutional safeguards and judicial principles, and the need for reforms. It argues that India should adopt a proportionate, risk-based and human-centred model that protects rights without unnecessarily restricting beneficial innovation.

1. INTRODUCTION

Artificial Intelligence refers broadly to computer-based systems capable of performing tasks associated with human intelligence, such as recognising patterns, processing language, generating content, making predictions and supporting decisions. Modern AI includes

machine-learning systems, generative AI tools, facial-recognition technologies and automated decision-making systems. These tools are being introduced into both private and public institutions.

AI governance means the laws, policies, institutions, technical standards and accountability mechanisms used to guide the development and use of AI. Governance is not limited to preventing misuse; it also seeks to ensure that AI systems are safe, fair, explainable where appropriate, secure and beneficial to society. The challenge for India is to encourage innovation while protecting constitutional rights and public interests.

India has not adopted a single, comprehensive AI Act that regulates every AI system. Instead, AI-related issues are addressed through existing legislation, sectoral rules and government policy. The India AI Governance Guidelines, unveiled by the Ministry of Electronics and Information Technology (MeitY) in November 2025, represent an important policy development. They favour a flexible and principle-based approach, with the stated objective of enabling responsible adoption while mitigating harm [1]. Policy guidance, however, does not automatically create the same legal duties or remedies as legislation.

2. SCOPE AND OBJECTIVES OF THE ARTICLE

This article studies the opportunities and challenges created by AI in India and evaluates whether the existing legal framework provides adequate protection. Its objectives are: (i) to explain the meaning and uses of AI; (ii) to identify legal, ethical and social risks; (iii) to examine relevant legislation and constitutional principles; (iv) to discuss judicial decisions that guide privacy and online expression; and (v) to recommend reforms for accountable, inclusive and rights-respecting AI governance.

3. KEYWORDS: Artificial Intelligence; AI Governance; India; Digital Rights; Privacy; Algorithmic Bias; Accountability; Data Protection; Constitutional Law; Generative AI; Legal Framework.

4. STRUCTURE OF THE STUDY

1. Meaning, Nature and Uses of Artificial Intelligence
2. Opportunities Created by AI in India
3. Challenges and Risks of AI
4. Existing Legal and Policy Framework in India
5. Constitutional Principles and Judicial Decisions

6. Accountability, Liability and Remedies
7. Institutional Governance and Enforcement
8. Need for a Robust Legal Framework
9. Recommendations for Reform
10. Conclusion
11. Bibliography

5. MEANING, NATURE AND USES OF ARTIFICIAL INTELLIGENCE

AI systems use data and computational methods to generate predictions, recommendations, classifications or content. Some systems perform a narrow task, such as detecting a defect in a product. Others can generate text, images, audio or video in response to instructions. AI outputs are not necessarily accurate or neutral: they depend on training data, design choices, deployment conditions and the quality of human oversight.

In India, possible applications include assisting doctors with diagnostic screening, helping farmers analyse crop conditions, improving traffic management, supporting translation across Indian languages, detecting suspicious financial transactions, personalising educational material and processing routine government applications. AI can also assist legal research and document management, but it should not replace the independent judgment of judges, lawyers or public officials where rights and liberty are at stake.

6. OPPORTUNITIES CREATED BY AI IN INDIA

6.1 Public administration and delivery of services

AI may help public authorities process large volumes of information, identify service-delivery gaps, translate public information and make routine services more accessible. These benefits depend on accurate data, reliable systems and clear responsibility for decisions. A citizen should not lose access to a benefit merely because an automated system has made an error.

6.2 Healthcare, education and agriculture

In healthcare, AI can support screening, medical-image analysis and administrative work, subject to clinical validation and professional supervision. In education, it can support language learning and accessible educational resources, but it also raises concerns about student privacy, inaccurate answers and over-reliance. In agriculture, data analysis may assist with weather, irrigation, pest detection and market planning. Systems must be designed for local languages, rural connectivity and varied levels of digital literacy.

6.3 Economic growth and innovation

AI can improve productivity, create new products and services, and support start-ups and small businesses. India's IndiaAI Mission and AI governance policy seek to strengthen domestic capacity and broaden access to AI infrastructure. The regulatory goal should be to make safe innovation possible, not to impose identical burdens on every system regardless of its risk.

7. CHALLENGES AND RISKS OF AI

7.1 Privacy and data protection

AI systems may require large datasets containing personal information. Collection, reuse, inference and retention of such data can affect individual autonomy and confidentiality. Facial recognition, behavioural profiling and the combination of datasets can create risks even when information is not openly published. Developers and deployers should identify a lawful basis for processing, limit data to legitimate purposes, secure it and provide appropriate notices and grievance channels.

7.2 Bias and discrimination

If training data reflects historical inequality or excludes particular groups, an AI system may reproduce or intensify that inequality. A recruitment tool might disadvantage applicants whose backgrounds are under-represented in the data; a credit model may produce unfair outcomes for particular communities. Testing should examine disparate impacts, data quality and accessibility. High-impact decisions require meaningful human review and a way to challenge an adverse outcome.

7.3 Deepfakes, misinformation and manipulation

Generative AI can create realistic but false images, voices and videos. Such material may be used for fraud, impersonation, harassment, election-related manipulation or non-consensual intimate imagery. Legal responses must protect victims and address deceptive conduct while respecting legitimate expression, satire, journalism and artistic work. Content labels, provenance tools and rapid grievance mechanisms may help, but they cannot replace due process.

7.4 Accountability and explainability

AI decisions may be difficult to explain, particularly where several developers, cloud providers, data suppliers and deployers contribute to a system. If harm occurs, responsibility can become unclear. Affected persons may not know that AI was used, what data influenced

the decision or how to seek correction. Governance therefore requires documentation, audit trails, risk assessments and clearly assigned responsibility.

7.5 Cybersecurity, intellectual property and employment

AI may be used to automate cyberattacks, generate convincing phishing messages or discover system weaknesses. AI systems themselves can be attacked through data poisoning, prompt injection or unauthorised access. Generative models also raise unresolved questions about the use of copyrighted works for training, ownership of outputs and infringement. Automation may change employment patterns, making reskilling, fair workplace practices and worker consultation important parts of responsible deployment.

8. EXISTING LEGAL AND POLICY FRAMEWORK IN INDIA

8.1 Information Technology Act, 2000

The Information Technology Act, 2000 provides a foundational legal framework for electronic records, electronic transactions and specified computer-related offences. Depending on the facts, provisions concerning unauthorised access, identity theft, cheating by personation using computer resources, privacy violations and unlawful content may apply to AI-enabled conduct [2]. The Act was not designed as a complete AI-specific statute, so questions involving algorithmic bias, training data, model transparency and allocation of responsibility may not be fully resolved by it.

8.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 establishes a framework for processing digital personal data and recognises both individual data-protection interests and lawful purposes for processing [3]. It is relevant where AI development or deployment involves personal data. Its practical effect depends on the commencement of particular provisions, applicable rules and the facts of a case; therefore, organisations should verify the current commencement notifications and compliance requirements rather than assume every provision applies identically from the date of enactment.

8.3 India AI Governance Guidelines

The India AI Governance Guidelines were released by MeitY in November 2025. They set out seven guiding principles: (1) Trust is the Foundation; (2) People First; (3) Innovation over Restraint; (4) Fairness and Equity; (5) Accountability; (6) Understandable by Design; and (7) Safety, Resilience and Sustainability [1]. The framework recommends coordination among government bodies, risk assessment, common standards, incident reporting, regulatory sandboxes, grievance mechanisms and review of legal gaps. These guidelines are an

important policy framework, but they should be distinguished from binding statutory provisions.

8.4 Other relevant laws

The Bharatiya Nyaya Sanhita, 2023 may apply where AI is used to commit offences recognised under general criminal law, subject to the elements of the relevant offence. The Bharatiya Sakshya Adhiniyam, 2023 is relevant to the admissibility and proof of electronic and digital records. Consumer-protection law may be relevant to misleading AI-generated claims or deficient services. Copyright and other intellectual-property laws may apply to protected works and infringement, although AI training and AI-generated output can raise difficult questions that need clearer legal guidance. Sectoral regulators, including the Reserve Bank of India and the Securities and Exchange Board of India, may also regulate AI use within their respective fields.

9. CONSTITUTIONAL PRINCIPLES AND JUDICIAL DECISIONS

9.1 Equality under Article 14

Article 14 guarantees equality before the law and equal protection of the laws. Public authorities using AI must act lawfully and avoid arbitrary or discriminatory decisions. Automated systems used in welfare, policing, recruitment or public services should be tested for bias, and the authority should remain able to explain and review its decision. The use of an algorithm does not remove constitutional responsibility from the State.

9.2 Freedom of speech under Article 19(1)(a)

AI-generated speech, moderation systems and automated content ranking may affect freedom of expression. Restrictions must remain within the constitutional framework. In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the Information Technology Act for violating freedom of speech and expression [4]. Although the case was not about modern generative AI, it demonstrates that digital regulation must be sufficiently clear and constitutionally justified.

9.3 Privacy under Article 21: K.S. Puttaswamy

In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge bench recognised privacy as a fundamental right protected by the Constitution, including under Article 21 and Part III [5]. The judgment is important for AI because data-driven systems may collect, infer and process information about individuals at scale. State action affecting privacy must have a legal basis, pursue a legitimate aim and satisfy proportionality. Private-sector data processing is also subject to applicable statutory obligations.

These decisions provide constitutional principles for evaluating AI use, but they should not be described as direct rulings on AI systems. As AI-specific disputes reach courts, further guidance may develop on automated decision-making, facial recognition, deepfakes, training data and responsibility for algorithmic harm.

10. ACCOUNTABILITY, LIABILITY AND REMEDIES

A workable legal framework should distinguish the roles of developers, providers, deployers, intermediaries and end-users. Liability should depend on factors such as control over the system, foreseeability of harm, the nature of the duty breached, compliance with safety measures and the causal connection between conduct and injury. A developer should not automatically be liable for every misuse by a third party, but a deployer should not escape responsibility merely by saying that an algorithm made the decision.

For high-impact applications, organisations should maintain records of the purpose of use, data sources, testing, known limitations, human review and incidents. Individuals should receive meaningful notice when AI materially affects an important decision, subject to legitimate security and confidentiality limits. They should be able to seek correction, human reconsideration and an effective remedy. Criminal punishment should be imposed only where the applicable legal elements are established; ethical failure alone should not be treated as a criminal offence without legal authority.

11. INSTITUTIONAL GOVERNANCE AND ENFORCEMENT

AI governance cuts across technology, law, consumer protection, data protection, cybersecurity, finance, healthcare and education. No single regulator has all the necessary expertise. The 2025 India AI Governance Guidelines recommend a coordinated approach and propose bodies such as an AI Governance Group, a Technology and Policy Expert Committee, and an AI Safety Institute [1]. Their effectiveness will depend on clear mandates, resources, technical competence, transparency and coordination with existing regulators.

Institutional measures should include a national AI incident-reporting mechanism, public guidance for organisations, independent evaluation capacity, technical standards, and controlled regulatory sandboxes. Public authorities should publish clear policies on when AI is used in decisions affecting citizens. Procurement contracts should require security, audit access, data-protection safeguards and a clear allocation of responsibility.

12. NEED FOR A ROBUST LEGAL FRAMEWORK

The present framework offers useful legal tools, but it is distributed across laws that were enacted for different purposes. This can create uncertainty about risk classification, mandatory testing, disclosure, liability, copyright, synthetic media and the treatment of AI-generated evidence. Voluntary guidelines can support good practice, but they may not provide consistent remedies or enforceable duties in every situation.

A robust framework should not necessarily prohibit high-risk technologies or require a licence for every AI tool. Instead, it should be proportionate: low-risk uses should face lighter obligations, while systems capable of affecting liberty, health, employment, credit, education, essential services or fundamental rights should face stronger safeguards. Rules should be technology-neutral where possible, periodically reviewed and developed through consultation with industry, civil society, researchers and affected communities.

13. RECOMMENDATIONS FOR REFORM

13.1 Adopt risk-based obligations

Classify AI applications by the severity and likelihood of harm. Require impact assessments, independent testing and stronger oversight for high-impact uses.

13.2 Clarify responsibility and liability

Define the duties of developers, deployers and organisations using AI. Require a named responsible officer for high-risk deployments and clarify routes to compensation and grievance redressal.

13.3 Protect privacy and data rights

Require lawful data processing, purpose limitation, appropriate security, data minimisation and transparent handling of personal information. Establish practical safeguards for sensitive and inferred data.

13.4 Address discrimination and ensure human review

Use representative datasets, bias testing and ongoing monitoring. Provide human reconsideration when automated decisions significantly affect a person's rights or access to services.

13.5 Improve transparency and auditability

Require clear disclosures when AI materially shapes a decision or generated media could mislead the public. Maintain documentation and audit trails while protecting legitimate trade secrets and security.

13.6 Establish deepfake and AI-incident procedures

Create accessible reporting channels, evidence-preservation protocols and timely responses for impersonation, fraud and non-consensual synthetic content, with safeguards against wrongful takedowns.

13.7 Clarify copyright and evidence rules

Consult stakeholders and provide clearer standards on the use of copyrighted works in training, ownership of outputs and proof of AI-generated or altered digital evidence.

13.8 Build institutional and public capacity

Invest in AI safety research, judicial and law-enforcement training, public awareness, local-language resources and independent technical expertise. Use regulatory sandboxes for controlled experimentation.

13.9 Ensure democratic oversight

Publish public-sector AI inventories where feasible, disclose the purpose of high-impact systems, enable independent review and provide accessible appeal mechanisms.

13.10 Review the law periodically

Create a transparent review process with public consultation, measurable outcomes and scheduled reassessment as technology and evidence evolve.

14. CONCLUSION

Artificial Intelligence offers India substantial opportunities to improve public services, healthcare, education, agriculture, economic productivity and access to information. However, the same technology can intensify privacy violations, discrimination, fraud, misinformation, cyber threats and uncertainty about legal responsibility. The central question is not whether India should adopt AI, but how it can ensure that AI serves people and remains subject to the rule of law.

India's existing statutes, constitutional guarantees, sectoral regulation and India AI Governance Guidelines provide a foundation for responsible AI governance. Nevertheless, policy principles must be supported by clear duties, effective enforcement, accessible remedies and adequate institutional capacity. A proportionate, risk-based and human-centred legal framework—one that combines innovation with transparency, fairness, safety and accountability—would help India realise the benefits of AI while protecting dignity, equality, privacy and democratic values.

15. BIBLIOGRAPHY

1. Government of India, Ministry of Electronics and Information Technology, India AI Governance Guidelines (released 5 November 2025), Press Information Bureau. <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2186639>
2. The Information Technology Act, 2000, India Code, Government of India. <https://www.indiacode.nic.in/indiacode/handle/123456789/1999?locale=en>
3. The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, India Code. https://www.indiacode.nic.in/indiacode/handle/123456789/22037?view_type=browse
4. Shreya Singhal v. Union of India, (2015) 5 SCC 1, Supreme Court of India.
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, Supreme Court of India.
6. NITI Aayog, Responsible AI for All: Approach Document for India, Government of India (2021). <https://www.niti.gov.in/>
7. The Constitution of India, particularly Articles 14, 19 and 21.
8. The Bharatiya Nyaya Sanhita, 2023; the Bharatiya Sakshya Adhiniyam, 2023; and applicable consumer-protection and intellectual-property laws.