



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE IN INDIA

~ *Adv. Nitesh Madhavi*

Pravin Gandhi College of Law

ABSTRACT

Artificial intelligence is increasingly being used in India in areas ranging from financial services and healthcare to education, advertising, policing and content creation. The legal difficulty is that AI systems do not fit neatly within one existing legal category. They may process personal data, generate content, influence decisions, create cybersecurity risks and cause harm without a clear human actor at the point where the harm occurs. India currently addresses these issues through a combination of general statutes, sectoral regulation, judicial principles and policy initiatives rather than through one comprehensive AI statute.

This paper examines the principal legal aspects of artificial intelligence in India. It considers the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, constitutional rights, intellectual property, intermediary responsibility, contractual and consumer liability, deepfakes and automated decision-making. It also considers recent Indian judicial developments, including the Supreme Court's 2026 decision concerning AI-generated hallucinated case law and the Bombay High Court's 2026 proceedings involving AI-generated deepfakes and personality rights. The paper argues that India's present framework is capable of addressing many individual harms, but it leaves important questions concerning accountability, transparency, attribution and human oversight without a single, predictable legal standard.

I. INTRODUCTION

Artificial intelligence is no longer limited to research laboratories or specialised technology companies. Generative AI tools can produce text, images, audio and video within seconds, while other systems are used to make recommendations, detect fraud, assess risk, assist medical professionals and process large quantities of information. The legal significance of these developments is not simply that machines are becoming more capable. It is that decisions and outputs that once depended directly on identifiable human actors can now be influenced by systems whose operation may be difficult for an ordinary person to understand or challenge.

India has chosen a relatively flexible approach to AI governance. Rather than creating a single AI Act, the legal framework has developed through existing legislation and policy measures. The Information Technology Act, 2000 remains an important part of the technology-law framework. The Digital Personal Data Protection Act, 2023 creates a statutory framework for processing digital

¹Information Technology Act, No. 21 of 2000, India Code (2000).

personal data. 2 Constitutional rights provide another layer of protection, particularly where AI systems affect privacy, equality or freedom of expression. 3

At the policy level, India has also developed the IndiaAI Mission and earlier national strategies for responsible AI. NITI Aayog's National Strategy for Artificial Intelligence described AI as a technology requiring both innovation and attention to social and ethical concerns. 4 The IndiaAI Mission reflects the continuing policy effort to build AI capability and infrastructure while developing an ecosystem for responsible use. 5

The central legal question is therefore not whether India has any rules applicable to AI. It clearly does. The more difficult question is whether the existing rules are sufficiently clear when an AI system produces an unexpected output, uses personal data, generates infringing content, impersonates a person, or contributes to a decision that causes harm. This paper examines that question through the principal areas in which AI currently creates legal consequences.

II. RESEARCH OBJECTIVES AND METHODOLOGY

The primary objective of this research is to examine how existing Indian laws apply to artificial intelligence and to identify areas where the present framework creates uncertainty. The paper addresses four related questions: first, which existing statutes can presently regulate AI-related conduct; second, how constitutional rights constrain the use of AI; third, how responsibility should be approached when AI-generated outputs cause harm; and fourth, whether the present combination of legislation, sectoral regulation and policy guidance provides adequate accountability.

The research adopts a doctrinal methodology. It examines statutes, judicial decisions, government policy documents and selected legal scholarship. The focus is on Indian law, with international developments used only as contextual background rather than as the primary basis of the analysis.

III. CONSTITUTIONAL DIMENSIONS OF ARTIFICIAL INTELLIGENCE

AI systems can directly affect constitutional interests. Article 14 guarantees equality before the law and equal protection of the laws, Article 19 protects specified freedoms including speech and expression, and Article 21 protects life and personal liberty. 6 The relevance of these rights becomes clearer when AI is used for profiling, automated decision-making, surveillance, content moderation or public-sector administration.

Privacy is particularly important because AI systems often depend on large datasets. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a constitutionally protected right under Article 21 and the broader constitutional structure. 7 AI-based processing can increase the scale of data analysis because information from multiple sources can be combined to infer characteristics that an individual may never have expressly disclosed.

The legal concern is therefore not limited to whether data was originally collected lawfully. An AI system may derive new information from existing data. For example, a system may infer preferences, behavioural patterns or risk categories from seemingly ordinary information. Such

2Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

3Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

4NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll (2018).

5Ministry of Electronics & Information Technology, IndiaAI Mission, Government of India (2024–present).

6Constitution of India arts. 14, 19, 21.

inference raises questions about notice, purpose limitation, proportionality and the ability of an individual to understand or contest the result.

AI also raises equality concerns. If an automated system produces systematically different outcomes for similarly situated individuals, Article 14 principles may become relevant. The difficulty is evidentiary: a person affected by an AI system may not know what data was used, which variables influenced the outcome, or whether the system has produced a pattern of discrimination. This creates a transparency problem in addition to the substantive equality question.

Freedom of expression creates another tension. AI-generated content can be used for legitimate creative expression, but generative systems can also facilitate impersonation, fabricated videos and misleading content. The Supreme Court's decision in *Shreya Singhal v. Union of India* remains important to the constitutional discussion because restrictions on online speech must satisfy the constitutional framework rather than being justified simply by the fact that the speech occurs through technology. ⁸

IV. THE INFORMATION TECHNOLOGY ACT AND AI

The Information Technology Act predates modern generative AI by many years, but several of its provisions remain relevant to AI-related conduct. The Act addresses unauthorised access, damage to computer systems, data-related offences and intermediary liability. ⁹ These provisions can become relevant where AI is used as a tool in cybercrime, where an AI system is involved in the creation or distribution of unlawful content, or where digital systems are compromised.

Section 43 provides civil consequences for certain unauthorised acts involving computer systems, while Section 43A addresses compensation in specified circumstances involving failure by a body corporate to implement reasonable security practices in relation to sensitive personal data or information. The practical application of these provisions to AI depends on the facts. An AI system is not itself a legal person and cannot ordinarily be treated as the ultimate bearer of statutory responsibility. Responsibility therefore has to be connected to the persons or organisations that develop, deploy, control or misuse the system.

Section 79 and the intermediary framework also become relevant where AI-generated material is uploaded or disseminated through online platforms. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due-diligence obligations on intermediaries and have been amended over time. ¹⁰ The legal challenge is to distinguish between a platform merely hosting user content and a service whose own design or operation materially contributes to the creation, recommendation or dissemination of harmful AI-generated material.

The Information Technology Act therefore provides pieces of an AI liability framework, but it was not drafted specifically for autonomous or generative systems. It does not establish a general risk-classification regime for AI, nor does it create a comprehensive statutory right to explanation of automated decisions.

V. DATA PROTECTION AND ARTIFICIAL INTELLIGENCE

The relationship between AI and data protection is unavoidable. Training, fine-tuning and operating AI systems may involve large quantities of information. Some of that information can be personal data. The Digital Personal Data Protection Act, 2023 was enacted to regulate the

⁸*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹⁰Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, G.S.R. 139(E) (Feb. 25, 2021).

processing of digital personal data while recognising both the individual's interest in protecting personal data and the need for lawful processing. 11

The Act introduces concepts such as the Data Principal and Data Fiduciary and establishes obligations concerning lawful processing, consent and specified legitimate uses. 12 For AI deployment, the practical question is whether an organisation can identify a lawful basis for the relevant processing and whether its notices and practices adequately communicate the nature and purpose of the processing.

AI creates a further difficulty because the purpose for which data is collected and the purposes for which a trained system may later use patterns derived from that data are not always identical. A business may collect customer information for providing a service and later seek to use that information to train or improve an AI model. Whether the later use is compatible with the applicable legal basis, notice and purpose limitations requires careful legal analysis rather than a blanket assumption that all technologically possible uses are permissible.

Security is equally important. A model or AI-enabled application can become a new point of attack. Sensitive information may be exposed through insecure integrations, prompt-based attacks, excessive data retention or poor access controls. The data-protection framework therefore needs to operate together with cybersecurity safeguards rather than treating privacy and security as separate concerns.

The constitutional privacy principles recognised in Puttaswamy remain relevant in interpreting the broader legal environment. 13 The statutory framework supplies specific obligations, while constitutional principles provide a higher-level basis for examining whether state or private-sector data practices disproportionately interfere with individual autonomy and privacy.

VI. INTELLECTUAL PROPERTY AND AI-GENERATED CONTENT

Intellectual property is one of the most unsettled areas of AI law because generative systems raise questions at both the input and output stages. At the input stage, copyrighted books, articles, images, music or software may be included in datasets or otherwise processed by AI systems. At the output stage, the system may generate material that resembles existing protected works or may produce a new work at the direction of a human user.

Under the Copyright Act, copyright subsists in specified categories of original works, and the statutory scheme defines authorship, ownership and infringement through human legal concepts. 14 The Act does not contain a comprehensive statutory regime expressly addressing whether an autonomous AI system can itself be an author. This creates uncertainty when a work is generated with minimal human creative contribution.

The Supreme Court's decision in *Eastern Book Co. v. D.B. Modak* is useful because it explains the Indian approach to originality. The Court held that copyright protection requires a work to originate from the author and involve the requisite degree of skill and judgment; mere copying or trivial alteration is insufficient. 15 Applied to AI-generated material, the difficult question is

14Copyright Act, No. 14 of 1957, §§ 2(d), 13, 14, 51, 52, India Code (1957).

15*Eastern Book Co. v. D.B. Modak*, (2008) 1 SCC 1.

therefore the extent of human contribution. A user who merely enters a short instruction may stand in a different legal position from a person who selects, arranges, edits and substantially transforms the generated material.

Ownership is another question. Even if an AI-assisted work qualifies for protection, the person or entity entitled to claim that protection must be identified under the Copyright Act and the contractual arrangements governing the AI service. Terms of service may allocate rights differently, but private contractual allocation cannot automatically answer every statutory question about authorship or originality.

AI also complicates infringement analysis because a generated image, text or audio may reproduce protected expression without the user knowing precisely which training material influenced the output. This raises difficult questions about proof of copying, substantial similarity and the responsibility of developers and users. Indian courts will likely have to apply established copyright principles to increasingly complex technical facts.

VII. DEEPFAKES, PERSONALITY RIGHTS AND REPUTATION

Generative AI has made it easier to create realistic images, videos and voices of real people without their consent. This can affect privacy, reputation, publicity or personality interests even where the generated content does not fit neatly within traditional copyright infringement.

The Bombay High Court's 2026 proceedings in *Preity G. Zinta v. Google LLC* illustrate the emerging problem. The petition concerned alleged AI-generated deepfake videos, manipulated images, AI-generated chatbot personas and other digital content, with claims including infringement of copyright, moral rights and personality-related interests.¹⁶ The proceeding is significant because it shows how existing legal rights can be invoked against synthetic content even in the absence of a dedicated Indian deepfake statute.

Indian privacy jurisprudence also provides a constitutional background for this issue. *Puttaswamy* recognises privacy as including interests connected with autonomy and control over personal information.¹⁷ *R. Rajagopal v. State of Tamil Nadu* also forms part of the Indian privacy and publication jurisprudence concerning an individual's interest in controlling the use of personal information.¹⁸

The difficulty is enforcement. Deepfake content can be generated in one jurisdiction, uploaded through another, and replicated across multiple platforms before a person can obtain relief. By the time a court order is obtained, copies may already exist elsewhere. The legal response therefore requires not only substantive rights but also effective notice, takedown, preservation of evidence and cross-platform enforcement mechanisms.

VIII. AI, CONTRACTS, CONSUMER PROTECTION AND LIABILITY

AI systems are increasingly incorporated into commercial services. A consumer may interact with an AI chatbot, receive an AI-generated recommendation, rely on an automated fraud alert, or purchase a product whose operation depends on an AI-enabled system. The resulting legal relationship may involve contract law, consumer protection law and sector-specific regulation.

The Indian Contract Act, 1872 provides general principles governing contractual relationships.¹⁹ If an AI-enabled service fails to perform according to contractual commitments, the ordinary law of contract can apply, although the question of whether an AI output was erroneous may create a factual dispute.

¹⁶*Preity G. Zinta v. Google LLC*, Leave Petition (L) No. 19882 of 2026 (Bom. H.C. June 16, 2026).

¹⁷*K.S. Puttaswamy*, (2017) 10 SCC 1.

¹⁸*R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632.

¹⁹Indian Contract Act, No. 9 of 1872, India Code (1872).

The Consumer Protection Act, 2019 may also become relevant where AI-enabled products or services cause harm or involve deficient service, unfair trade practices or misleading representations. ²⁰ A company should not be able to avoid responsibility merely by saying that an algorithm produced the result. The legal question is more appropriately directed toward the organisation's obligations, representations, supervision and control.

Sectoral regulation is especially important in high-impact fields. The Reserve Bank of India has issued technology governance requirements for regulated entities, including governance, risk management, controls and assurance. ²¹ Securities regulation also addresses the use of technology and AI/ML tools by regulated entities. ²² These examples demonstrate that India is developing a sectoral approach in which responsibility is placed on regulated organisations rather than on AI systems themselves.

The broader issue is attribution. Where an AI system makes an error, a legal framework must determine whether responsibility lies with the developer, deployer, service provider, operator, data provider or some combination of them. Existing laws can answer parts of this question, but they do not provide a single general rule for AI-related harm.

IX. AI IN THE JUDICIAL SYSTEM: THE 2026 SUPREME COURT DEVELOPMENT

The legal profession itself has been affected by generative AI. Lawyers may use AI tools to search authorities, prepare drafts or summarise judgments. The risk becomes serious when an AI system produces fabricated case names, incorrect citations or non-existent passages and those materials are presented to a court as genuine authorities.

In *Pooja Ramesh Singh v. Jammu & Kashmir Bank Ltd.*, the Supreme Court considered a case in which the NCLT and NCLAT had relied upon six AI-generated citations that were subsequently found to be non-existent or to contain attributed paragraphs that did not exist. The Supreme Court's landmark judgment summary identifies the issue as involving the consequences of AI-generated fake or hallucinated case law and the need for directions to prevent reliance on such material. ²³

The case has significance beyond the immediate procedural facts. It shows that AI-generated information cannot be treated as a substitute for professional verification. Legal research is ultimately a professional activity for which lawyers and judges remain responsible. The fact that an AI system produced a citation does not transfer that responsibility to the machine.

This development also raises a broader principle for AI governance: human oversight is particularly important where an automated output can directly affect legal rights. The higher the consequence of an AI-assisted decision, the stronger the case for verification, traceability and accountability.

X. INDIA'S POLICY APPROACH TO AI GOVERNANCE

India's policy approach has developed around responsible AI, innovation and sectoral governance rather than a single comprehensive AI statute. NITI Aayog's National Strategy for Artificial Intelligence proposed an approach centred on social and inclusive development and

²⁰Consumer Protection Act, No. 35 of 2019, India Code (2019).

²¹Reserve Bank of India, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (Nov. 7, 2023).

²²Securities and Exchange Board of India, Guidelines / circular framework applicable to artificial intelligence and machine learning tools used by regulated entities, as amended from time to time.

²³*Pooja Ramesh Singh v. Jammu & Kashmir Bank Ltd.*, 2026 INSC 668 (S.C. July 2, 2026), Supreme Court of India, Landmark Judgment Summary.

identified areas such as healthcare, agriculture, education, smart cities and infrastructure for AI adoption. 24

NITI Aayog later published Responsible AI for All, which examined principles and use cases for responsible AI. 25 The IndiaAI Mission represents a more recent institutional effort to strengthen India's AI ecosystem, including infrastructure, datasets, innovation and skills. 26

Policy documents are valuable because they can respond faster than primary legislation to technological change. Their limitation is legal enforceability. A policy framework can guide institutions and industry without necessarily creating the same rights, duties and remedies that a statute provides.

This distinction matters for businesses. An organisation may voluntarily adopt transparency, human oversight and risk-management principles, but voluntary compliance does not always provide a clear remedy to a person harmed by an AI system. A mature AI governance framework therefore needs coordination between policy principles and enforceable legal obligations.

XI. RESEARCH FINDINGS AND LEGAL GAPS

The first finding is that India already has a substantial body of law capable of addressing many AI-related harms. Privacy law, data protection, copyright, cyber law, consumer protection, contract law and sectoral regulation can all apply depending on the facts.

The second finding is that these laws were largely designed before the present generation of generative AI. They regulate particular conduct rather than AI as a technology. This creates uncertainty when one AI system simultaneously implicates privacy, copyright, cybersecurity and consumer protection.

The third gap concerns responsibility. Existing law generally assumes that a human or legal entity can be identified as the actor. AI systems complicate that assumption because multiple participants may contribute to the final output: the model developer, data provider, deployer, platform and user.

The fourth gap concerns transparency. A person affected by an automated decision may have difficulty discovering why a particular outcome occurred. Existing legal remedies may provide routes to challenge the decision, but there is no single cross-sector right to an explanation of an AI decision.

The fifth gap concerns deepfakes and synthetic identity. Existing privacy, copyright, defamation, intermediary and personality-rights principles can provide relief, but enforcement can be slow compared with the speed at which synthetic content spreads.

The sixth gap concerns professional use. The Supreme Court's 2026 decision concerning AI-generated case law demonstrates that professional verification remains essential. 27 Similar concerns may arise in medicine, finance, education and other sectors where users may over-rely on automated outputs.

25Digital India Corporation, Responsible AI for All: Adopting the Framework—A Use Case Approach (NITI Aayog, 2021).

XII. CRITICAL ANALYSIS

India's present approach has an important advantage: it does not require every new AI application to wait for a completely new statute before existing law can operate. A deepfake may already implicate privacy or personality interests. Unauthorised access to an AI system may already fall within cyber law. Misuse of personal data may already raise data-protection questions. An AI-assisted service may already be subject to consumer or sectoral obligations.

The weakness is fragmentation. A person harmed by AI may have to identify which existing legal category best describes the harm. That may be difficult when a single incident involves several legal interests at once. For example, a deepfake may involve privacy, reputation, personality rights, copyright, intermediary liability and potentially criminal law. A fragmented framework can increase uncertainty about the appropriate remedy and the responsible party.

In my assessment, the immediate legal priority should not necessarily be to regulate every AI system in the same way. A better approach would distinguish between low-risk and high-impact uses and place stronger obligations on systems that can materially affect rights, safety, finances or access to essential services. Such an approach would also allow ordinary consumer uses of AI to remain subject to existing legal rules without creating unnecessary regulatory burdens.

Human accountability should remain central. AI should not become a legal shield behind which a developer or organisation can avoid responsibility. Where an entity chooses to deploy an AI system for a business or public function, it should remain responsible for reasonable governance, testing, security, documentation and supervision appropriate to the risk involved.

The law should also encourage explainability and auditability. This does not necessarily mean requiring developers to disclose every technical detail of a model. It means preserving enough information about the system, data use and decision process to allow a legitimate complaint to be investigated. Without such records, legal rights can exist on paper while becoming difficult to enforce in practice.

XIII. SUGGESTIONS

First, India should continue developing a coherent, risk-based governance framework for high-impact AI while retaining the flexibility of sectoral regulation. The framework should identify clear responsibilities for developers, deployers and operators.

Second, high-impact AI systems should be subject to stronger documentation and audit requirements. Organisations should maintain records sufficient to identify the model or system used, the relevant data sources where legally appropriate, material changes to the system, and significant decisions or outputs.

Third, AI-related data processing should be integrated with privacy-by-design and security-by-design practices. Organisations should not wait for a data breach or regulatory complaint before examining whether their AI systems process personal data lawfully and securely.

Fourth, legal remedies for deepfakes and synthetic identity misuse should be made faster and more accessible. Existing remedies can be useful, but rapid dissemination requires rapid procedures for notice, preservation and removal while still protecting legitimate expression.

Fifth, professional bodies and educational institutions should develop clear standards for responsible use of generative AI in legal research and drafting. The 2026 Supreme Court development concerning fabricated authorities shows why verification cannot be delegated to an AI system. 28

Finally, legislation and policy should preserve human responsibility. The objective should not be to assign legal personality to AI, but to ensure that identifiable human or institutional actors remain accountable for how AI is designed, deployed and used.

XIV. CONCLUSION

Artificial intelligence presents India with a legal problem that cuts across existing areas of law rather than fitting into a single statutory category. The Information Technology Act, Digital Personal Data Protection Act, constitutional rights, copyright law, consumer protection, contract law and sector-specific regulations already provide significant tools for addressing AI-related conduct. 29 30 31 32

At the same time, the present framework has limitations. It does not provide one general rule for responsibility when an AI system causes harm, nor does it establish a uniform standard for transparency, explainability or human oversight across sectors. The problems are particularly visible in deepfakes, automated decisions, AI-generated intellectual property and professional reliance on generated information.

Recent Indian judicial developments demonstrate that these issues are no longer theoretical. The Supreme Court's decision concerning AI-generated case law shows the risks of relying on machine-generated information without verification. 33 The Bombay High Court's 2026 proceedings involving AI-generated deepfakes show how existing personality, copyright and related rights are being tested by synthetic media. 34

India therefore does not begin from a legal vacuum. The more realistic task is to connect the existing legal framework with the characteristics of modern AI. A future governance model should preserve innovation while requiring proportionate accountability, data protection, security, transparency and human oversight. The central legal principle should remain simple: the use of an AI system should not remove the responsibility of the person or institution that chooses to deploy it.

REFERENCES AND AUTHORITIES

Statutes and Regulations

1. Bharatiya Sakshya Adhiniyam, 2023.
 2. Copyright Act, 1957.
 3. Digital Personal Data Protection Act, 2023.
-

4. Information Technology Act, 2000.
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
6. Indian Contract Act, 1872.
7. Consumer Protection Act, 2019.

Cases

8. Eastern Book Co. v. D.B. Modak, (2008) 1 SCC 1.
9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
10. Pooja Ramesh Singh v. Jammu & Kashmir Bank Ltd., 2026 INSC 668.
11. Preity G. Zinta v. Google LLC, Leave Petition (L) No. 19882 of 2026 (Bom. H.C. June 16, 2026).
12. R. Rajagopal v. State of T.N., (1994) 6 SCC 632.
13. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Government and Policy Materials

14. NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll (2018).
15. NITI Aayog, Responsible AI for All: Adopting the Framework—A Use Case Approach (2021).
16. Ministry of Electronics & Information Technology, IndiaAI Mission.
17. Reserve Bank of India, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (Nov. 7, 2023).

Selected Literature

18. Adhyan Rastogi, Legal Aspects of Artificial Intelligence in India, 3 Indian J. for Research in L. & Mgmt., Issue 10 (2026).
19. Subhasri Roy, Legal Aspects of Artificial Intelligence in India, 3 Indian J. for Research in L. & Mgmt., Issue 9 (2026).