



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.

ARTIFICIAL INTELLIGENCE AND LAW

~Sangita Roy

ABSTRACT

Artificial Intelligence (“AI”) is increasingly becoming embedded in activities that were traditionally governed by direct human judgment. Automated systems now assist in recruitment, credit assessment, healthcare, education, content generation, surveillance and public administration. The legal significance of this development lies not merely in the sophistication of the technology but in the possibility that consequential decisions may be produced through systems whose operation is difficult for affected individuals to understand or challenge. This creates questions concerning privacy, equality, discrimination, intellectual property, liability, procedural fairness and the allocation of responsibility among developers, deployers and users. India presently addresses these concerns through a combination of constitutional principles, information-technology legislation, data-protection law, sectoral regulation and policy initiatives rather than through a comprehensive AI statute. The Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, has strengthened India's data-governance architecture, but data protection alone cannot resolve the wider accountability problems created by AI. This article examines the principal legal challenges associated with AI and compares India's developing approach with the European Union's risk-based Artificial Intelligence Act and the United States' standards-oriented approach. It argues that India's future AI governance should preserve a legally traceable chain of responsibility whenever decision-making is delegated to automated systems. Such a framework should combine risk classification, meaningful human oversight, transparency, privacy safeguards, anti-discrimination measures, lifecycle accountability and effective remedies. The objective should not be to prevent technological development, but to ensure that automation does not become a means of diluting legal responsibility.

INTRODUCTION

The legal importance of Artificial Intelligence lies in a simple but consequential change: decisions that once required direct human assessment can increasingly be assisted, recommended or generated by computational systems. AI is now used to identify patterns in large datasets, predict outcomes, classify individuals, generate content and support decisions across both private and public institutions.

This transformation offers substantial benefits. AI can process information at a scale that is difficult for individuals to reproduce, assist medical and scientific research, improve administrative efficiency and create new forms of communication and economic activity. At the same time, the delegation of decision-making to automated systems creates a distinctive legal difficulty.

The central problem, therefore, is not simply whether AI is “safe” or “unsafe.” It is whether the legal system can continue to identify who exercised power, on what basis, subject to which safeguards, and with what avenue of redress when the immediate mechanism of decision-making is an algorithm.

This question is particularly important in India. The Indian legal system does not presently regulate AI through a single comprehensive AI statute. Instead, relevant principles are distributed across the Constitution, the Information Technology Act, 2000 (“IT Act”), the Digital Personal Data Protection Act, 2023 (“DPDP Act”), the Digital Personal Data Protection Rules, 2025 (“DPDP Rules”), intellectual-property law, consumer law and sector-specific regulatory frameworks¹.

The DPDP² framework is an important development, but it should not be mistaken for a complete AI-governance framework. Data protection addresses an essential part of the AI ecosystem, yet AI may create harms that occur even when data processing is otherwise lawful. An automated system can, for example, produce discriminatory recommendations, unreliable decisions or misleading content without the principal legal problem being reducible to unauthorized processing of personal data.

This article advances a specific proposition: Indian AI regulation should preserve a legally traceable chain of responsibility whenever human decision-making is delegated to an

¹ Information Technology Act, 2000, No. 21 of 2000, India Code; Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code.

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

automated system. The law should identify the duties of the actors who design, deploy and control AI according to the risks associated with their respective roles. Automation should alter the method of decision-making, not the possibility of legal accountability.

AI REQUIRES A DISTINCT LEGAL RESPONSE

AI should not be treated as a single legal category. A system recommending films and a system assessing whether a person should receive a loan may both technically involve AI, but their potential consequences are fundamentally different.

This distinction supports a risk-sensitive approach. The European Union's Artificial Intelligence Act ("EU AI Act") establishes a harmonized framework that differentiates obligations according to the risks associated with AI systems³. Certain practices are prohibited, while high-risk systems are subjected to more extensive requirements concerning matters such as risk management, data governance, documentation and human oversight.

The United States has pursued a comparatively decentralized approach. The National Institute of Standards and Technology ("NIST") AI Risk Management Framework 1.0 provides a voluntary framework for organizations developing or using AI systems and is intended to assist in identifying and managing risks while supporting trustworthy AI⁴.

These approaches demonstrate that effective AI governance need not be based upon a universal prohibition. A more proportionate model can impose stronger duties where the consequences of error, discrimination or misuse are greater.

For India, this distinction is crucial. Excessively broad regulation could burden low-risk innovation, while insufficient regulation could leave individuals inadequately protected when AI is used in areas involving fundamental rights or significant economic and social interests.

³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations and Directives, 2024 O.J. (L 1689) 1. The Regulation entered into force on Aug. 1, 2024, with its provisions applying according to a phased timetable

⁴ Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Nat'l Inst. Standards & Tech. 2023).

PRIVACY: FROM DATA COLLECTION TO MACHINE-GENERATED INFERENCES

AI's dependence upon data makes privacy one of its most significant legal dimensions. However, AI changes the traditional privacy problem.

Conventional data protection often focuses upon the collection, storage, use and disclosure of information. AI adds another layer: inference. A system can combine apparently unrelated information and derive predictions or classifications concerning an individual.

The constitutional significance of privacy in India was authoritatively recognized in Justice *K.S. Puttaswamy (Retd.) v. Union of India*, where the Supreme Court held that privacy is a constitutionally protected right associated with dignity, liberty and autonomy⁵. The Court's reasoning also placed proportionality within the constitutional analysis of restrictions upon fundamental rights.

The DPDP Act provides the principal statutory framework for digital personal data, while the DPDP Rules, 2025 provide additional implementation requirements. The Rules were notified on November 14, 2025, and provide for phased commencement of specified provisions⁶. The framework therefore represents a significant development in India's data-governance architecture.

Consequently, AI governance should move beyond a purely consent centered model and emphasize institutional responsibilities relating to purpose, necessity, security, minimization, retention and responsible use.

The legal concern is not simply: **“Was the data collected lawfully?”**

It is also:

“What was subsequently inferred, how was that inference used, and what consequences followed?”

That distinction should become increasingly important in future Indian privacy jurisprudence.

⁵ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

⁶ Digital Personal Data Protection Rules, 2025, Gazette of India, Ministry of Electronics & Information Technology (Nov. 14, 2025).

ALGORITHMIC DISCRIMINATION AND ARTICLE 14

An algorithm does not necessarily become neutral merely because it is mathematical.

AI systems learn from data, and data may reflect historical inequalities. If those patterns are treated as predictors of future behaviour, automated decision-making may reproduce an existing disparity while appearing technologically objective.

This creates a difficult question for equality law. Traditional discrimination often involves an identifiable decision-maker and an identifiable discriminatory criterion.

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws. Articles 15 and 16 provide additional constitutional safeguards in specified contexts⁷. Where the State uses AI in making decisions that affect individuals, the fact that a computational system produced the immediate result cannot place the decision beyond constitutional scrutiny.

The legal response should not be that every unequal statistical outcome is automatically unconstitutional. Nor should it require proof of intentional discrimination in circumstances where an automated system produces a demonstrably discriminatory effect.

A better approach would require high-impact AI systems to undergo appropriate testing and monitoring for foreseeable discriminatory outcomes.

THE “BLACK BOX” AND THE LEGAL VALUE OF EXPLANATION

One of the most important difficulties associated with AI is the limited interpretability of certain complex systems.

The legal problem becomes acute when an automated output affects a person's rights or substantial interests. If an individual is denied employment, credit, insurance or a public benefit, a statement that “the algorithm produced the result” is unlikely to provide a meaningful basis for challenge.

Reasons serve an important function in law. They allow a person to understand the basis of a decision, identify possible errors and seek review.

⁷ INDIA CONST. arts. 14-16

This does not mean that every AI system should be required to disclose its complete source code. Intellectual-property protection, cybersecurity and legitimate commercial confidentiality may justify restrictions on technical disclosure.

Where an AI system materially contributes to a consequential decision, the affected person should, subject to legitimate limitations, receive information sufficient to understand:

- that AI was used;
- the nature of its role in the decision;
- the principal factors that materially influenced the outcome;
- whether human review occurred; and
- how the decision can be challenged or corrected.

This approach would reconcile technological complexity with procedural fairness. It also reinforces the importance of human oversight.

WHO SHOULD BE LIABLE FOR AI-RELATED HARM?

Liability is perhaps the most difficult issue in AI governance because the technology distributes responsibility across multiple actors.

A modern AI system may involve a model developer, data supplier, infrastructure provider, application developer, deploying organization and end user.

Existing Indian law already contains doctrines capable of addressing portions of this problem, including negligence, contract, consumer protection and statutory liability.

A developer responsible for creating a high-risk model should have obligations relating to reasonable testing and risk identification. A deployer who chooses to use that system in a high-impact context should have separate responsibilities concerning appropriate deployment, supervision and monitoring. A user who intentionally manipulates the system for unlawful purposes should not automatically transfer responsibility to the developer.

This approach avoids two extremes.

The first is **absolute developer liability**, under which every harmful output becomes the responsibility of the person who created the underlying technology.

The second is **complete automation immunity**, under which no actor is responsible because “the system made the decision.”

Neither approach is satisfactory.

The better principle is that legal responsibility should follow the actor's **capacity to prevent, identify or mitigate the relevant risk.**

This would permit existing legal doctrines to evolve without requiring the law to treat AI as a separate legal person.

GENERATIVE AI AND INTELLECTUAL PROPERTY

Generative AI has created a particularly complex relationship between technology and intellectual-property law.

Traditional copyright law is substantially concerned with authorship, originality and protected expression. Generative AI complicates these concepts because an output may be produced through an interaction between a human user and a computational model.

At least three legally distinct questions arise.

First, what legal authority exists for using copyrighted works in the development or training of AI systems?

Second, what status should be given to an output generated substantially by an AI system?

Third, where a human substantially edits or transforms AI-generated material, what legal protection should attach to the resulting work?

Indian copyright law contains statutory concepts of “author” and protected works, but it was not enacted specifically to address generative AI⁸. Courts will therefore potentially have to determine how existing concepts apply to new forms of machine-assisted creativity.

A future regulatory framework should avoid assuming that either creators or AI developers possess an absolute claim.

⁸ Copyright Act, 1957, No. 14 of 1957, §§ 2(d), 13, India Code.

DEEPPAKES, SYNTHETIC CONTENT AND INDIVIDUAL HARM

Generative AI has significantly lowered the technical barrier to creating realistic synthetic content. This creates legal concerns involving impersonation, fraud, reputational injury, harassment and privacy.

The legal response, however, must distinguish harmful synthetic content from legitimate expression. AI-generated satire, artistic experimentation and fictional material should not automatically be placed in the same category as deceptive impersonation or non-consensual intimate imagery.

This distinction becomes especially important in light of Article 19(1)(a) of the Constitution.

In Shreya Singhal v. Union of India, the Supreme Court invalidated Section 66A of the IT Act, emphasizing the constitutional significance of freedom of speech and expression in the online environment⁹. The decision illustrates that regulation of digital technologies must remain consistent with constitutional requirements.

India's regulatory approach should consequently focus on the conduct, the harm and the responsibility of the relevant actor, rather than treating AI-generated content as inherently unlawful.

AI, SURVEILLANCE AND STATE POWER

The consequences of AI become particularly serious when the technology is used by the State.

Facial recognition, predictive analytics, automated risk assessment and large-scale data analysis can expand governmental capacity to identify, classify and monitor individuals. Such capabilities may assist legitimate public purposes, but they also increase the potential scale of interference with privacy and liberty.

The constitutional significance of this problem is reinforced by Puttaswamy. If governmental surveillance interferes with privacy, the existence of sophisticated technology does not itself provide constitutional justification. The legality and proportionality of the interference remain relevant.

⁹Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

INDIA'S PRESENT REGULATORY POSITION

India's AI governance is developing through several legal and policy layers rather than through a single AI statute.

The IT Act remains an important component of the country's digital legal framework. It addresses various forms of computer-related misconduct, intermediary liability and governmental powers concerning electronic information¹⁰.

The DPDP Act and DPDP Rules establish a more developed framework for digital personal-data governance. The Rules notified in November 2025 provide implementation mechanisms and a phased timeline for the operationalization of the data-protection framework¹¹.

At the policy level, the Ministry of Electronics and Information Technology has an AI and Emerging Technologies Group and has undertaken initiatives concerning AI development, research and deployment¹². The India AI Mission is part of this broader policy environment.

These developments demonstrate that India is not legally inactive in relation to AI. The difficulty is different: the existing framework does not yet form a single, coherent system for allocating responsibility across the entire AI lifecycle.

For example, data protection may regulate personal-data processing, but it does not by itself answer whether an algorithmic employment decision was discriminatory. Intellectual-property law may address copyright, but it does not necessarily determine responsibility for an AI-generated defamatory statement. Constitutional law may constrain State action, but a comprehensive procedural framework for challenging automated decisions remains important.

COMPARATIVE LESSONS FROM THE EUROPEAN UNION AND THE UNITED STATES

The EU AI Act represents a legislative model based upon differentiated risk. It establishes obligations that vary according to the characteristics and potential risks of AI systems¹³. Its

¹⁰ Information Technology Act, 2000, No. 21 of 2000, §§ 43, 69, 79, India Code.

¹¹ Digital Personal Data Protection Act, 2023, No. 22 of 2023; Digital Personal Data Protection Rules, 2025. The Ministry of Electronics and Information Technology states that the Rules were notified on Nov. 14, 2025 and provide for an eighteen-month phased compliance timeline.

¹² Ministry of Electronics & Information Technology, Government of India, AI & Emerging Technologies Group, available through the Ministry's official AI and Emerging Technologies materials.

¹³ Regulation (EU) 2024/1689, *supra* note 2.

significance for India lies in demonstrating how an AI framework can move beyond a one-size-fits-all approach.

The United States' NIST AI RMF offers a different model. It is voluntary and focuses upon organizational processes for identifying, evaluating and managing AI risks¹⁴. NIST describes the framework as intended for organizations designing, developing, deploying or using AI systems and emphasizes trustworthy and responsible AI.

India can draw from both approaches without copying either.

A possible Indian framework could establish mandatory statutory duties for high-risk AI while relying upon technical standards, codes and flexible guidance for lower-risk systems. This would preserve regulatory proportionality while permitting the framework to adapt as technology changes.

A PROPOSED ACCOUNTABILITY MODEL FOR INDIA

A coherent Indian AI framework should contain at least the following elements.

1. Risk Classification

AI systems should be classified according to potential impact. Systems affecting fundamental rights, employment, healthcare, education, credit, essential services, policing or other significant interests should receive greater regulatory scrutiny.

2. AI Impact Assessment

Before deploying high-risk systems, organizations should evaluate foreseeable effects on privacy, equality, security, reliability and individual rights.

3. Lifecycle Accountability

Responsibility should not be imposed exclusively at the point where harm occurs. Relevant duties should arise during design, training, testing, deployment, monitoring and retirement of the system.

4. Meaningful Human Oversight

¹⁴ Tabassi, supra note 3. NIST describes the AI RMF as voluntary and designed to assist organisations in managing AI risks while incorporating trustworthiness considerations throughout the design, development, use and evaluation of AI systems.

Human involvement should be substantive where an automated output can significantly affect rights or interests. A human reviewer should possess actual authority to reconsider the result.

5. Explanation and Contestability

Affected individuals should have an opportunity to understand and challenge consequential AI-assisted decisions.

6. Effective Remedies

Individuals should have accessible mechanisms for correction, review and, where legally justified, compensation. These principles would establish something more significant than a technology-specific statute. They would create a legal structure capable of following responsibility through the AI lifecycle.

CONCLUSION

Artificial Intelligence challenges law not because machines have suddenly become legal actors, but because human institutions are increasingly choosing to delegate parts of their decision-making to systems that may be difficult to understand and difficult to challenge.

That distinction is fundamental.

The central issue in AI governance should therefore not be whether a machine is intelligent enough to make a decision. The legal issue is whether the institution that chooses to rely upon that machine remains capable of explaining, defending and, where necessary, correcting the consequences of that decision.

India already possesses important foundations for this task. The constitutional protection of equality, liberty and privacy, the IT Act, the DPDP Act and the DPDP Rules, together with sector-specific regulation and emerging AI policy, provide components of a broader governance architecture. Yet these components do not by themselves establish a comprehensive mechanism for assigning responsibility when AI becomes part of consequential decision-making.

The next stage of Indian AI regulation should therefore move beyond the question of whether data was processed lawfully and ask the broader question of whether the entire decision-making process remained legally accountable.

This requires a shift from isolated regulation of technology to governance of responsibility.

AI should be permitted to assist human beings, but assistance should not become an excuse for institutional detachment. Developers should not be able to disregard foreseeable risks; deployers should not be able to rely blindly upon automated outputs; public authorities should not be able to avoid constitutional scrutiny by transferring decisions to software; and individuals harmed by consequential automated decisions should not be left without a meaningful route to challenge them.

The most appropriate legal principle is therefore not that AI must always remain under direct human control. Such a requirement may be impractical in every context. The more durable principle is that where AI exercises meaningful influence over legally significant outcomes, the human and institutional chain behind that system must remain identifiable, reviewable and accountable.