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.

AI WITHOUT ACCOUNTABILITY? RETHINKING LEGAL LIABILITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Ayesha khan

ABSTRACT

Artificial Intelligence, with all its potential for innovation and efficiency, is becoming deeply ingrained in healthcare, finance, education, employment, governance and other areas of our everyday life. However, the integration of technologies based on artificial intelligence presents us with a number of difficult legal questions concerning liability for injuries inflicted by intelligent machines. The situation is complicated by introducing such systems since responsibility for their damage is diffused among many economic actors. This article explores the emerging accountability gap around artificial intelligence and this also investigates whether Indian laws are ready to grapple with the unique challenges posed by technologies based on AI. The article analyzes the application of the concepts of negligence, product liability and constitutional rights, as well as the relevant provisions of the Consumer Protection Act, 2019, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023 in the context of artificial intelligence.[1] Particular attention is drawn to the issues of opacity, causality, personal d

[1] Consumer Protection Act, No. 35 of 2019, §§ 82–87, India Code (2019); Information Technology Act, No. 21 of 2000, §§ 43, 43A, 72, 72A, 79, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, § 8, India Code (2023); Bharatiya Nyaya Sanhita, No. 45 of 2023, § 336, India Code (2023); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, India Code (2023).

data protection, human monitoring and evidence. A brief overview is given to the risk-based approach being developed in the European Union, which may serve as a model for Indian legislation.[2] The article advocates for a balanced and technology-neutral approach according to which liability for damage would be determined on the basis of factors such as control, causality, reasonable care and the ability to prevent damage. The article concludes by stating that technological autonomy should not lead to legal immunity and emphasizes the importance of innovation without leaving accountability behind.

KEYWORDS: Artificial Intelligence; AI Liability, Legal Accountability, Algorithmic Decision -Making, Negligence, Product Liability, Data Protection; Consumer Protection, Digital Personal Data, Algorithmic Transparency, Human Oversight, Indian Technology Law.

INTRODUCTION

Artificial Intelligence has rapidly transformed from an emerging technology into a important component of modern economic and social life. AI systems are increasingly used in healthcare, finance, education, recruitment, transportation, law enforcement and content creation. While these technologies offer significant benefits, their increasing autonomy also raises a fundamental legal question: when an AI system causes harm, who should be held legally responsible?

Traditional notions of legal liability generally attribute a harmful act or omission to an

[2] 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 2024/1689), arts. 6–15.

identifiable human being or legal entity. This poses challenges in respect of AI, where an outcome may be the result of developer who designed the model, the organisation that deployed it, the data upon which it was trained, the user who operated it and the circumstances in which it was used.[3]

The resulting problem may be described as an accountability gap. If responsibility becomes impossible to establish merely because an algorithm was involved, technological complexity can effectively become a defence against liability.[4]

India does not have a single statute governing civil and criminal liability for AI-generated harm. This requires an examination of whether existing provisions, including the Consumer Protection Act, 2019, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, contract law and constitutional principles, are capable of addressing such harm.

The central issue, therefore, is whether these existing provisions are capable of dealing with AI-related harm and, if not, what principles should guide future legislation.

THE AI ACCOUNTABILITY PROBLEM

AI systems differ from conventional products because their behaviour may depend upon training data, model architecture, subsequent updates and the context in which they are deployed.

Consider an AI-powered hiring system that unfairly treats job applicants because the data it was trained on shows past treatment. The final choice might be made automatically. Many people might be connected to the process in some way but the person who built the system the company that bought it the person who handled the data the company that used the results and the people in charge of making sure it’s

---

[3] NITI Aayog, Approach Document for India: Part 1—Principles for Responsible AI, at 23 (2021), NITI Aayog official report.

[4] *Id.* at 23; NITI Aayog, Responsible AI for All: Approach Document for India—Part 1: Principles for Responsible *AI*, at 18–23 (2021).

used properly.[5]

The law needs to tell the difference, between making something controlling it which putting it into action and using it wrong. A person who creates the system shouldn't be blamed for every result it produces. At the same time a company shouldn't be able to say "the computer made the choice" and avoid being responsible.

The appropriate approach is one based upon foreseeability, control, negligence and the capacity to prevent harm.

NEGLIGENCE AND AI-GENERATED HARM

Negligence remains one of the most important legal concepts through which AI-related harm may be addressed.

A negligence claims generally requires the existence of a duty of care, breach of that duty, causation and damage. Although Indian negligence law developed primarily without reference to artificial intelligence, its principles can potentially be applied to AI systems.

The Supreme Court's decision in Jacob Mathew v. State of Punjab is relevant for its discussion of the standard of reasonable care in professional negligence. The broader principle is that liability depends upon whether the relevant actor failed to exercise the level of care reasonably expected in the circumstances.[6]

In an AI context, this could involve asking:

- Was the system adequately tested before deployment?
- Were foreseeable risks identified?
- Was the training data appropriately assessed?
- Were users warned about known limitations?

---

[5] NITI Aayog, Responsible AI for All: Approach Document for India—Part 1: Principles for Responsible AI, at 23 (2021).

[6] See Jacob Mathew v. State of Punjab, (2005) 6 SCC 1, ¶ 48 (India).

- Was adequate human supervision provided?
- Were failures monitored after deployment?

These questions are particularly significant in high-risk fields such as healthcare, financial services and public administration. The EU AI Act, for example, requires risk-management processes for high-risk AI systems and provides for testing, transparency, and human oversight.[7] The involvement of AI should therefore not eliminate the ordinary legal requirement of reasonable care.

INDIAN STATUTORY FRAMEWORK GOVERNING AI LIABILITY

India does not presently have a single comprehensive statute specifically governing liability for artificial intelligence. Instead, AI-related liability is addressed through existing laws depending upon the nature of the harm and the persons involved.

The Consumer Protection Act, 2019 provides an important statutory framework through its product-liability provisions under Sections 82–87. Sections 84–86 address circumstances in which manufacturers, product service providers and product sellers may be held liable for harm caused by defective products or deficient services. These provisions may become relevant to AI-enabled products and services where inadequate design, warnings, testing or reasonable care results in consumer harm.[8]

The Information Technology Act, 2000 is relevant to AI-related cyber conduct. Sections 43 and 43A address specified forms of unauthorized access, damage and failure to maintain reasonable security practices, while Sections 72 and 72A concern confidentiality and disclosure of information. Section 79 provides conditional intermediary safe harbour subject to statutory requirements.[9]

The Digital Personal Data Protection Act, 2023 is particularly significant because AI systems frequently process personal data. Section 8 places obligations upon Data

[7] Regulation (EU) 2024/1689, 2024 O.J. (L 2024/1689), arts. 9–15.

[8] Consumer Protection Act, No. 35 of 2019, §§ 82–87, India Code (2019).

[9] Information Technology Act, No. 21 of 2000, §§ 43, 43A, 72, 72A, 79, India Code (2000).

Fiduciaries, including responsibility for processing undertaken through Data Processors.[10] The Act also provides rights relating to access, correction and erasure of personal data and mechanisms for grievance redressal.[11]

The Bharatiya Nyaya Sanhita, 2023 may apply where AI is deliberately used to facilitate criminal conduct. For example, Section 336 addresses forgery involving false documents or electronic records, subject to the ingredients of the offence being established.[12]

The Bharatiya Sakshya Adhiniyam, 2023 is also important because AI disputes may depend upon electronic and digital evidence, including system records and AI-generated outputs.[13]

Together, these laws provide several routes for addressing AI-related harm. However, their fragmented nature highlights the need for a more coherent framework that allocates responsibility according to control, foreseeability, reasonable care and the capacity to prevent harm.

WHO SHOULD BEAR LIABILITY?

Indian law should avoid a model under which every harmful AI outcome automatically results in liability for the developer. Instead, responsibility should correspond to the actor's role.

- Developers may be responsible where harm results from negligent design, inadequate testing, known vulnerabilities or failure to address foreseeable risks.
- Deployers may bear responsibility where they select an inappropriate system, fail to monitor it or use it in a context presenting risks that should reasonably have been identified.

---

[10] Digital Personal Data Protection Act, No. 22 of 2023, § 8, India Code (2023).

[11] *Id.* §§ 11–13, 13–14.

[12] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 336, India Code (2023).

[13] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, India Code (2023).

- Users may be responsible where they intentionally misuse AI or disregard known limitations.
- Service providers and sellers may fall within the statutory product-liability framework where the requirements of the Consumer Protection Act 2019 are satisfied.[14]

This approach recognises that AI accountability is fundamentally a question of allocation of responsibility across an ecosystem.

Globally, different jurisdictions have begun to grapple with these questions in different ways. The European Union's AI Act (2024) adopts a precautionary approach by imposing a strict liability model for high-risk AI systems. Under this regime, providers of such systems are held accountable regardless of fault whenever harm arises.[15]
The United States, by contrast, has adopted a more fragmented, sector-based approach, where liability rules differ across industries such as healthcare, finance, and autonomous vehicles.[16]
In India, however, the courts have not yet had the opportunity to deal with AI-specific liability cases. When faced with similar issues, Indian courts have so far relied on analogies drawn from existing principles of product liability, negligence under the IT Act, and constitutional jurisprudence such as the K.S Puttaswamy judgment on privacy.[17]

THE NEED FOR A DEDICATED ARTIFICIAL INTELLIGENCE LIABILITY FRAMEWORK

The existing Indian statutes provide several legal tools, but they remain fragmented.

The Consumer Protection Act 2019 addresses product liability and consumer harm. The Information Technology Act addresses various forms of cyber conduct and intermediary responsibility. The Digital Personal Data Protection Act 2023 regulates

[14] Consumer Protection Act, No. 35 of 2019, §§ 84–86, India Code (2019).

[15] Regulation (EU) 2024/1689, 2024 O.J. (L 2024/1689), arts. 6, 8–15.

[16] See generally Nat'l Inst. of Standards & Tech., *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023).

[17] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, 298–99 (India).

digital personal-data processing. The Bharatiya Nyaya Sanhita, 2023 provides criminal offences applicable to certain AI-assisted conduct. The Bharatiya Sakshya Adhiniyam, 2023 addresses electronic evidence.[18]

Together, these laws can address many individual forms of AI-related harm. Yet they do not establish a comprehensive framework for determining responsibility when an AI system independently produces an unexpected harmful outcome.

A future framework could introduce:

1. Risk classification for AI systems;
2. Mandatory risk assessments for high-risk applications;
3. Requirements for testing and monitoring;
4. Preservation of audit trails and system logs;
5. Human oversight in high-impact decisions;
6. Clear disclosure of material AI involvement;
7. Mechanisms to address information asymmetry between victims and technology providers; and
8. Clear allocation of liability according to control, foreseeability and capacity to prevent harm.

Such regulation should complement, rather than unnecessarily duplicate, existing legislation.

WAY FORWARD AND RECOMMENDATIONS

The existing legal framework in India may require further development to address situations in which harm is caused by the design, deployment, or operation of artificial intelligence systems. One possible approach would be to introduce a dedicated legislative framework dealing with AI-related liability. A statutory framework could also provide greater certainty to individuals, developers, businesses, and other stakeholders

[18] Consumer Protection Act, No. 35 of 2019, §§ 82–87; Information Technology Act, No. 21 of 2000, §§ 43, 43A, 72, 72A, 79; Digital Personal Data Protection Act, No. 22 of 2023, § 8; Bharatiya Nyaya Sanhita, No. 45 of 2023, § 336; Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

regarding their respective legal obligations.

AI applications are tested under regulatory supervision before being introduced on a wider scale. Subject to appropriate safeguards, such mechanisms could permit limited regulatory flexibility while ensuring that risks are identified at an early stage. In addition, liability standards may need to vary according to the sector in which an AI system is deployed.

AI-related disputes may also require mechanisms that are faster and less burdensome than conventional litigation. Mediation and arbitration could provide suitable alternatives in appropriate cases, particularly where disputes involve contractual relationships between developers, businesses, users, or other private parties.

The objective of future AI regulation should therefore not be limited to imposing liability after harm has occurred. It should also establish preventive safeguards, clarify responsibilities, and provide effective remedies when harm does occur. A balanced framework would seek to protect individuals and their legal rights without imposing regulatory requirements so burdensome that legitimate technological research and innovation become unnecessarily difficult.

CONCLUSION

The emergence of AI does not make existing law irrelevant. On the contrary Indian law already contains principles that can be applied to AI-related disputes. The Consumer Protection Act 2019 provides an important statutory foundation through its product-liability provisions. The Information Technology Act, 2000 addresses forms of technology-related misconduct. The Digital Personal Data Protection Act, 2023 places responsibility upon Data Fiduciaries for compliance concerning personal-data processing. The Bharatiya Nyaya Sanhita, 2023 provides criminal-law provisions of applying to certain AI-assisted misconduct while the Bharatiya Sakshya Adhiniyam, 2023 provides the evidentiary framework necessary for proving digital conduct.

The principal weakness is therefore not necessarily the absence of law but the absence

of a coherent framework connecting these laws to the distinctive characteristics of AI.

AI should not become a black box in which responsibility disappears whenever an algorithm is involved. At the time liability should not be imposed merely because an AI system produced an undesirable result. The appropriate legal approach should examine who designed the system, who controlled it who deployed it what risks were foreseeable what safeguards were implemented and whether reasonable care was exercised.

The fundamental principle should remain simple: technological autonomy cannot mean legal immunity.