LEGAL LIABILITY ISSUES OF ARTIFICIAL INTELLIGENCE IN INDIA

-Pranav Pal[1], Dr. Saurabh Siddhartha[2]

Abstract

Artificial Intelligence (AI) is rapidly transforming governance, commerce, healthcare, and social interaction in India. As AI systems become increasingly autonomous and consequential, the question of who bears legal responsibility when they cause harm has emerged as one of the most pressing issues in contemporary Indian law. This article examines the legal liability landscape for AI in India, analysing how existing statutory frameworks — including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Consumer Protection Act, 2019 — apply to AI-related harms. It further explores the doctrinal inadequacy of traditional tort law, product liability regimes, and criminal law when confronted with AI's non-deterministic behaviour, opacity, and distributed agency. Comparative insights are drawn from the European Union's AI Act and emerging global regulatory approaches. The article concludes with recommendations for a dedicated, risk-based AI liability framework suited to India's socio-legal context.

Keywords: *Artificial Intelligence, Legal Liability, Tort Law, Product Liability, Data Protection, India, Regulatory Framework.*

I. Introduction

India stands at a pivotal juncture in its relationship with Artificial Intelligence. The NITI Aayog's National AI Strategy, adopted in 2018, envisioned India as a global AI hub, emphasising the technology's transformative potential for economic growth and social welfare.[3] This ambition is reflected in significant public and private investment in AI across fintech, healthtech, agriculture, and public administration. Yet the rapid proliferation of AI systems has outpaced the development of commensurate legal safeguards, leaving a conspicuous regulatory vacuum around AI-generated harm.

The Indian legal system, built on colonial-era foundations subsequently supplemented by post-independence legislation, was not designed to contend with autonomous decision-making systems that lack legal personhood, operate through inscrutable algorithms, and distribute responsibility across complex value chains. The Information Technology Act, 2000 ("IT Act")[4] addresses certain dimensions of digital harm but remains silent on AI-specific liability. The Digital Personal Data Protection Act, 2023 ("DPDP Act")[5] introduces obligations around data processing but does not directly regulate AI liability. The Consumer Protection Act, 2019[6] offers a product liability regime that may capture some AI-related injuries, yet its doctrinal fit with AI's unique characteristics remains contested.

II. The AI Regulatory Landscape in India

2.1 Definitional Uncertainty

A foundational challenge for AI liability in India is the absence of a statutory definition of "Artificial Intelligence." Indian law does not currently define AI, machine learning, or autonomous systems in any binding legislative instrument. This lacuna means that courts and regulators must reason by analogy from existing concepts — an exercise fraught with difficulty given AI's contextual variability. An AI system may simultaneously be a software product, a service, a data processor, and an agent, attracting different liability rules depending on the characterisation adopted.[7]

2.2 Existing Statutory Frameworks

The IT Act, 2000 remains the principal legislation governing digital activity in India. While it creates liability for intermediaries, establishes offences relating to unauthorised access and data theft, and provides for compensation for failure to protect data, it does not address AI-specific issues such as algorithmic discrimination, autonomous decision-making, or AI-generated content. The "safe harbour" for intermediaries under Section 79 of the IT Act, as modified by

---

[1] LL.M. Cyber and Security Law, ICFAI University, Dehradun

[2] Assistant Professor, Law, ICFAI University, Dehradun

[3] Ministry of Electronics and Information Technology (MeitY), *National Strategy for Artificial Intelligence*, NITI Aayog (2018), available at https://niti.gov.in/national-strategy-for-artificial-intelligence.

[4] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).

[5] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].

[6] Consumer Protection Act, 2019, No. 35 of 2019, Acts of Parliament, 2019 (India), ss. 2(34), 84–87.

[7] Shyamkrishna Balganesh, *Tort Law in India*, 2nd edn (LexisNexis 2021) 14–19.

the Intermediary Rules, 2021,[8] has been the subject of significant litigation, but these provisions were crafted for human-mediated platforms rather than autonomous AI systems that actively generate or curate content.

The DPDP Act, 2023 represents the most recent and significant statutory development with implications for AI. It imposes obligations on "data fiduciaries" — entities that determine the purpose and means of processing personal data — to maintain data accuracy, implement security safeguards, and respect the rights of "data principals." Where AI systems process personal data for automated decision-making — as in credit scoring, insurance underwriting, or predictive policing — the DPDP Act's obligations engage directly, though the Act does not expressly regulate AI decision-making processes or mandate explainability.

NITI Aayog's Responsible AI for All framework[9] and related policy documents represent India's primary non-binding articulation of AI governance principles. These documents endorse fairness, accountability, transparency, and privacy as governing values but have yet to be translated into enforceable legal obligations, leaving a substantial gap between aspiration and legal reality.

III. Tortious Liability and Artificial Intelligence

3.1 The Negligence Framework

The tort of negligence, as received in Indian law from the common law tradition, requires the plaintiff to establish: (i) a duty of care owed by the defendant; (ii) breach of that duty; (iii) causation; and (iv) resulting damage.[10] Each element poses distinct difficulties when applied to AI-generated harm.

The duty of care question, grounded in the "neighbour principle" articulated in *Donoghue v Stevenson*,[11] requires that the defendant could reasonably have foreseen harm to the plaintiff. AI developers and deployers can generally be regarded as owing duties of care to foreseeable users and third parties who may be affected by AI outputs. The more complex question is how this duty is allocated across the AI supply chain — between dataset providers, model developers, deployers, and end-users — and whether a defendant can escape liability by attributing harm to the AI system's autonomous behaviour.

The standard of care in negligence is that of the "reasonable person," but in technical fields courts apply a professional standard, as the Supreme Court confirmed in *Jacob Mathew v State of Punjab*.[12] In the AI context, this requires identifying the appropriate professional benchmark: should an AI developer be held to the standard of a reasonably competent software engineer, machine learning specialist, or domain expert? The answer likely varies by application — a medical AI system may attract a higher standard than a consumer recommendation engine.

3.2 The Causation Problem

Perhaps the most intractable doctrinal challenge is causation. AI systems, particularly deep-learning models, are characterised by their non-deterministic behaviour — the same input may not always produce the same output — and by their "black box" opacity, meaning that the causal pathway from input to output cannot always be reconstructed.[13] Traditional causation analysis, whether couched in "but-for" or material contribution terms, presupposes a traceable causal chain. When an AI system makes an autonomous decision that causes harm, establishing that the harm would not have occurred "but for" a specific act or omission by any identifiable human actor is often impossible.

A promising doctrinal avenue is the application of *res ipsa loquitur* — "the thing speaks for itself" — which permits an inference of negligence from the mere occurrence of harm in circumstances under the defendant's control. Indian courts have applied this doctrine in product liability and medical negligence cases. However, its application to AI requires careful calibration: AI systems frequently malfunction due to distributional shift or adversarial inputs rather than any deficiency in the defendant's conduct, and holding developers liable on a near-strict basis may chill innovation.

3.3 Absolute Liability

Indian law recognises a doctrine of absolute liability — distinct from Rylands v Fletcher's rule of strict liability — whereby enterprises engaged in inherently dangerous or hazardous activities are liable without proof of negligence, and

[8] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology, Notification No. G.S.R. 139(E).

[9] NITI Aayog, *Responsible AI for All: Operationalising India's Approach for Enabling AI Principles* (Government of India 2021).

[11] Donoghue v Stevenson [1932] AC 562 (House of Lords).

[12] Jacob Mathew v State of Punjab (2005) 6 SCC 1 (Supreme Court of India).

[13] Ajay Ranka, 'Autonomous Vehicles and Tort Liability in India: A Critical Analysis' (2022) 14(2) *Indian Journal of Law and Technology* 45, 58.

without the traditional defences, for any harm caused by their operations.[14] This doctrine, established by the Supreme Court in *M.C. Mehta v Union of India*, could in principle apply to high-risk AI deployments — for instance, AI systems used in critical infrastructure, autonomous weapons, or surgical robotics. The challenge lies in defining the threshold of danger that triggers absolute liability and in avoiding over-deterrence of beneficial AI applications.

IV. Product Liability

4.1 Consumer Protection Act, 2019

The Consumer Protection Act, 2019 introduces, for the first time in Indian law, a statutory product liability regime. Section 2(34) defines "product liability" as the responsibility of a product manufacturer, seller, or service provider to compensate for harm caused by a defective product or deficient service.[15] The Act creates liability for three categories of product defect: manufacturing defects, design defects, and inadequate warnings (failure to warn). Applied to AI, these categories map — imperfectly — onto flawed training data, defective algorithm design, and insufficient disclosure of AI capabilities and limitations respectively.

A critical issue under the 2019 Act is whether AI systems constitute "products" or "services" for the purposes of the product liability provisions. Hardware-embedded AI systems (such as autonomous vehicles or AI-powered medical devices) are more naturally characterised as products. Cloud-based AI services present a more complex picture: while the underlying model may be a product, its delivery as a service may attract service-based deficiency liability rather than product liability rules.

4.2 Defects in AI Systems

Design defects — where the product is inherently unsafe as designed, even when manufactured correctly — are particularly salient for AI. Biased training data, inadequate robustness testing, and reward functions that incentivise harmful behaviour may all constitute design defects. Establishing a design defect requires showing that a reasonable alternative design was available; in the AI context this raises difficult questions about whether the defendant was obligated to adopt more conservative models, richer datasets, or more extensive testing protocols.

Failure-to-warn liability is potentially the most tractable product liability theory for AI harms. Developers and deployers who fail to disclose material limitations of their AI systems — including rates of error, known biases, scope of application, and contraindications — may incur liability for resulting harm. This theory is consistent with emerging regulatory trends toward mandatory AI transparency and explainability, as reflected in the DPDP Act's accuracy obligations and NITI Aayog's transparency principle.

V. Criminal Liability

5.1 General Principles

Indian criminal law, as now codified in the Bharatiya Nyaya Sanhita, 2023 ("BNS"),[16] requires for criminal liability the concurrence of a guilty act (*actus reus*) and a guilty mind (*mens rea*). This bipartite structure presents fundamental difficulties when applied to AI-generated harm: an AI system cannot possess *mens rea*, and the human actors in the AI chain — developers, deployers, operators, and users — may each be too remote from the immediate harmful act to satisfy the causation requirements of criminal law.

Prior to the BNS, provisions of the Indian Penal Code, 1860 on causing death by negligence and acts endangering human life[17] were the primary vehicle for holding individuals criminally accountable for AI-related fatalities. These provisions require proof of criminal negligence — a higher threshold than civil negligence — and would ordinarily be directed at the human operator most proximate to the harm rather than at the AI developer.

5.2 Corporate Criminal Liability

AI systems are typically developed and deployed by corporate entities. The attribution of criminal liability to corporations in India has historically been challenging due to the requirement of *mens rea*, which courts have at times interpreted as demanding proof of the directing mind and will of the corporation. However, the Supreme Court has recognised that corporate liability is possible for regulatory and statutory offences that do not require proof of intent, and the BNS incorporates provisions on vicarious and corporate liability. Where AI-related conduct constitutes a

[14] M.C. Mehta v Union of India (1987) 1 SCC 395 (Supreme Court of India) — the Court applied absolute liability for inherently dangerous enterprises.

[15] Consumer Protection Act, 2019, s. 2(34) defines 'product liability' as the responsibility of a product manufacturer, product seller, or service provider to compensate for any harm caused to a consumer.

[16] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, 2023 (India).

[17] Indian Penal Code, 1860, s. 304A (causing death by negligence) and s. 336 (endangering life or personal safety). Note: IPC now replaced by Bharatiya Nyaya Sanhita, 2023 (BNS 2023).

criminal offence under sector-specific regulation, corporate criminal liability may be easier to establish than under the general criminal law.

5.3 IT Act Offences

The IT Act creates specific offences that may capture certain categories of AI-related harm: Section 43 (damage to computer systems), Section 66 (computer-related offences), Section 66A (now struck down), and Section 72 (breach of confidentiality and privacy). The Intermediary Rules, 2021 impose due diligence obligations on significant social media intermediaries and may indirectly apply to AI-powered content moderation and recommendation systems. However, AI-specific offences — such as algorithmic manipulation, deepfake fraud, or autonomous system sabotage — are not expressly provided for.

VI. Data Protection, Privacy, and AI

6.1 DPDP Act, 2023 and AI

The DPDP Act, 2023 creates a comprehensive framework for the protection of digital personal data in India.[18] Its principal relevance to AI liability arises from three sources: first, the obligation of data fiduciaries to process personal data only for specified, lawful purposes with valid consent; second, the right of data principals to seek correction, erasure, and grievance redressal; and third, the establishment of the Data Protection Board of India ("DPBI") as an adjudicatory body for data-related complaints.[19]

AI systems that process personal data for automated profiling, predictive decision-making, or targeted advertising engage the DPDP Act's consent and purpose limitation requirements. Where such processing causes harm — for instance, where a discriminatory algorithm denies a loan application or an inaccurate AI assessment leads to adverse employment consequences — the DPBI may have jurisdiction to award compensation. Critically, the DPDP Act does not require explainability for automated decisions, nor does it confer a right to contest purely automated decisions, leaving a significant gap relative to standards established by the EU General Data Protection Regulation.

6.2 Constitutional Right to Privacy

The Supreme Court's landmark nine-judge decision in *Justice K.S. Puttaswamy (Retd.) v Union of India*[20] recognised privacy as a fundamental right under Article 21 of the Constitution of India. This constitutional underpinning provides an important mechanism for challenging AI-related privacy violations: State-sponsored AI surveillance, biometric databases maintained by government agencies, and AI-driven profiling by public authorities may all be contested as infringements of the constitutional right to privacy, subject to the tests of legality, necessity, proportionality, and procedural safeguards.

The interplay between the DPDP Act and the constitutional right to privacy will be a significant area of jurisprudential development. Courts may be called upon to determine whether the DPDP Act's exemptions — particularly those for State security and law enforcement — are consistent with the *Puttaswamy* framework, and whether AI-enabled mass surveillance satisfies the proportionality standard.

VII. Intellectual Property Issues in AI

7.1 Copyright and AI-Generated Works

The Copyright Act, 1957 provides a limited recognition for computer-generated works: Section 2(d)(vi) designates the "person who causes the work to be created" as the author of a computer-generated literary, dramatic, musical, or artistic work.[21] This provision was enacted before modern AI and was intended to address relatively straightforward automation rather than generative AI systems capable of producing original creative output. Questions that have not been judicially resolved in India include: whether works generated by an AI system without meaningful human creative input qualify for copyright protection; who among the AI developer, the deployer, and the user is the "person who causes the work to be created"; and whether AI-training on copyrighted data constitutes infringement.

7.2 Patents and AI Inventorship

[19] DPDP Act, 2023 (n 3) s. 33 — Data Protection Board of India.

[20] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (Supreme Court of India, nine-judge bench) — right to privacy held a fundamental right under Art. 21 of the Constitution.

[21] Copyright Act, 1957, No. 14 of 1957, Acts of Parliament, 1957 (India), s. 2(d)(vi) — author includes a computer-generated work where the author is the person who causes the work to be created.

The Patents Act, 1970 requires that a patent applicant be the "true and first inventor," a phrase that presupposes a natural person.[22] Courts in the United States and United Kingdom have uniformly held that AI systems cannot be named as inventors,[23] and Indian patent practice, which is closely aligned with international norms, is likely to reach the same conclusion. However, the deeper question — whether AI-assisted inventions (where the AI makes a significant but not exclusive contribution) are adequately served by existing inventorship rules — has yet to be addressed by the Indian courts or the Controller General of Patents.

The liability dimension of AI and intellectual property intersects where AI systems reproduce, plagiarise, or infringe existing works in their outputs. A generative AI system that reproduces substantial portions of a copyright-protected work may expose its developer or deployer to infringement liability; the "fair dealing" exceptions under the Copyright Act are narrow and unlikely to provide comprehensive shelter for large-scale AI training.

VIII. Sector-Specific Regulatory Frameworks

8.1 Financial Services

The Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have progressively engaged with AI in the financial sector. The RBI's guidance on digital lending[24] addresses algorithmic credit scoring and requires that lending decisions be explainable and auditable. SEBI has issued regulations on algorithmic trading that mandate risk controls and kill-switch mechanisms. These sectoral frameworks impose obligations on financial institutions deploying AI but do not create standalone AI liability rules; liability for AI-driven financial harm is currently mediated through general financial services regulation and the Consumer Protection Act.

8.2 Insurance

The Insurance Regulatory and Development Authority of India (IRDAI) has acknowledged AI's growing role in underwriting, claims processing, and fraud detection.[25] AI-generated underwriting decisions that discriminate on prohibited grounds — such as caste, religion, or disability — could violate anti-discrimination principles embedded in the Constitution and sector-specific regulations. However, India lacks explicit rules on algorithmic fairness in insurance, creating a regulatory lacuna for AI-driven discriminatory outcomes.

8.3 Healthcare

AI applications in healthcare — including diagnostic AI, drug discovery, robotic surgery, and clinical decision support — present the highest-stakes liability questions. The Central Drugs Standard Control Organisation (CDSCO) has circulated draft guidance on AI/ML-based Software as a Medical Device (SaMD),[26] proposing a risk-based classification framework analogous to the approach adopted by the US FDA. Medical AI liability in India will need to navigate the intersection of product liability under the Consumer Protection Act, professional negligence under the common law, and regulatory approval requirements under the Drugs and Cosmetics Act, 1940.

IX. Recommendations

The following recommendations are offered for the development of a coherent AI liability framework in India:

(i) Enact a Dedicated AI Act with a Risk-Based Liability Framework. India should enact comprehensive AI legislation that classifies AI applications by risk level, following the EU model. High-risk AI applications should be subject to mandatory conformity assessments, transparency requirements, and human oversight obligations. The legislation should create a rebuttable presumption of causation in favour of claimants where a high-risk AI system has caused harm, reversing the burden of proof on causation to address the evidentiary asymmetry between AI developers and injured parties.[27]

(ii) Establish Strict Liability for Ultra-High-Risk AI. Building on the *M.C. Mehta* absolute liability doctrine, the proposed AI Act should impose strict liability — without the option of fault-based defences — for AI applications in

[22] Patents Act, 1970, No. 39 of 1970, Acts of Parliament, 1970 (India), s. 2(1)(p) — 'true and first inventor' must be a natural person.

[23] Thaler v Vidal, 43 F.4th 1207 (Fed. Cir. 2022) — US Court of Appeals (Federal Circuit) held AI cannot be named as inventor under US patent law.

[24] Reserve Bank of India, *Report of the Working Group on Digital Lending Including Lending through Online Platforms and Mobile Apps* (2021); RBI Master Direction on Digital Lending, 2022.

[25] Insurance Regulatory and Development Authority of India (IRDAI), *Report of the Working Group on Insurtech* (2020).

[26] Ministry of Health and Family Welfare, *Draft National Digital Health Blueprint* (2019); CDSCO, AI/ML-Based Software as Medical Device (SaMD) Guidance Document (Draft, 2022).

[27] NITI Aayog, *Discussion Paper on National Strategy for AI* (2018) 56 — 'AI for All' principle emphasises inclusivity and social good.

safety-critical domains such as autonomous vehicles, surgical robotics, and AI-governed critical infrastructure. This is consistent with the rationale of absolute liability: those who derive benefit from inherently dangerous technologies should internalise the cost of any resulting harm.

(iii) Introduce Mandatory AI Insurance. The proposed legislation should mandate third-party liability insurance for high-risk AI applications, ensuring that compensation funds are available to injured parties irrespective of the financial capacity of the AI developer or deployer. Mandatory insurance pools would also create market-based incentives for safer AI development.

(iv) Extend the DPDP Act to Regulate Automated Decision-Making. The DPDP Act should be amended to confer on data principals the right to an explanation for, and the right to contest, purely automated decisions that significantly affect them. This amendment would align India's data protection framework with international best practice and provide a meaningful remedy for AI-driven discrimination and error.

(v) Strengthen Sector-Specific AI Regulations. Sectoral regulators — the RBI, SEBI, IRDAI, CDSCO, and others — should issue binding, AI-specific regulations that specify permissible AI use cases, transparency obligations, audit requirements, and redress mechanisms. These sector-specific instruments should be coordinated with the overarching AI Act to avoid regulatory fragmentation.

(vi) Create a Dedicated AI Regulatory Authority. The Law Commission of India[28] has previously recommended updating liability frameworks for emerging technologies. India should establish a dedicated AI regulatory authority with cross-sectoral jurisdiction, expert capacity, and enforcement powers. This authority should be responsible for maintaining an AI risk register, supervising high-risk AI deployments, and adjudicating AI-related liability disputes.

X. Conclusion

Artificial Intelligence presents a profound challenge to the Indian legal system. The existing statutory and doctrinal framework — designed for human actors operating in more legible causal chains — is ill-equipped to assign liability fairly and efficiently for AI-generated harms. The opacity of AI systems complicates negligence analysis, the distributed nature of AI supply chains frustrates product liability, and the absence of *mens rea* in AI systems strains the criminal law.

India has an opportunity to develop a world-leading AI liability framework, drawing on the lessons of the EU, US, and China while adapting them to its distinctive developmental context, constitutional values, and legal culture. Such a framework must balance the imperatives of innovation and access against the protection of individuals from AI-generated harm — a balance that India's "AI for All" vision[29] demands be struck with particular care for the most vulnerable members of society.

The absence of a coherent AI liability framework is not merely a technical legal gap; it is a failure of governance that leaves injured parties without redress and creates uncertainty that may ultimately deter responsible AI development. Legislative action, informed by scholarly engagement and comparative learning, is both urgent and overdue.

[28] Law Commission of India, Report No. 277, *Wrongful Prosecution (Miscarriage of Justice): Legal Remedies* (2018) — discusses the need for updating liability frameworks for emerging technologies.