The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 7 | July 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Legal liablity for AI- Driven Decision: Who's Responsible In India?

Harshita Saharavat

LL.M, HNB Garhwal University (A Central university), Srinagar, Uttrakhand

Email; harshitasherawat26@gmail.com

DOI : https://doi.org/10.5281/zenodo.16880254

ARTICLE DETAILS

Research Paper

Accepted: 31-07-2025

Published: 10-08-2025

Keywords:

Artificial Intelligence liablity, AI Regulation In india, Legal Responsibility, Algorithimic Accountablity.

ABSTRACT

In India, the growth of artificial intelligence (AI) in industries such as healthcare, banking, law enforcement, and governance has raised significant legal issues about accountability and liability. As AI systems begin to make or influence decisions that were previously made by people, Indian law remains unprepared to confront the implications of harm caused by autonomous or algorithm-driven acts. This study investigates the essential question of who should be held legally accountable when AI systems break, give biased results, or cause unintended harm in the Indian setting. Using doctrinal legal research and comparative analysis, the study explores existing Indian statutes—including the Information Technology Act of 2000, the Indian Penal Code of 1860, the Consumer Protection Act of 2019, and tort law principles—to determine their application to AI-related injury. The paper concludes that the current legal framework is fragmented, lacks clarity in allocating accountability across AI stakeholders, and fails to account for the autonomous and opaque nature of modern AI systems. Additionally, India lacks a specialized regulatory framework to control the usage and repercussions of AI. Drawing on worldwide developments such as the European Union's AI Act and global liability models, the paper advocates for a multi-tiered liability system, sector-specific regulation, and the implementation of strict liability for high-risk AI applications in India. The findings highlight the urgent need for

a comprehensive legal framework that combines technological innovation, rights-based responsibility, and legal certainty.

1. Introduction

1.1 Rise of Artificial Intelligence and Its Expanding Role in Decision-Making

Artificial intelligence (AI) has swiftly progressed from a support tool to a core decision-making mechanism across numerous industries. In India, the spread of AI technology has altered governance, commerce, and public services through programs such as Digital India and NITI Aayog's AI plan. AI systems are now being used for diagnostic tools in healthcare, algorithmic credit assessments in finance, facial recognition and predictive policing in law enforcement, and automated recruitment screening in human resources. These technologies are increasingly making or influencing decisions that directly impact individual rights, public safety, and access to critical services.

1.2 Nature of AI-Driven Decision-Making: Autonomous, Opaque, and Data-Driven.

Modern AI, unlike old automated systems, relies on autonomous, complicated, and data-intensive machine learning models. These systems frequently expand beyond their original programming, producing results using self-trained algorithms based on large datasets. The inherent opacity—also known as the "black box" problem—makes it impossible for consumers, developers, and regulators to trace or explain how a decision was reached. This lack of transparency is exacerbated by the absence of direct human monitoring in many high-volume or real-time decision-making scenarios, which raises legal and ethical concerns when harm or discrimination occurs.

1.3 Global Concern Over Accountability and Liability

The international legal community has expressed serious worries about the lack of accountability when AI systems make harmful or incorrect decisions. Traditional liability frameworks are based on ideas of human purpose, foreseeability, and negligence, which may not apply to non-human, algorithmic actors. Legal theorists such as Matthias (2004) have noted the emergence of a "responsibility gap" in AI systems that behave unpredictably, while Pagallo (2013) has proposed for a distributed liability model across AI's design and operational lifecycle. In response, the European Union introduced the AI Act and the AI Liability Directive, which seek to establish legal norms and accountability procedures for high-risk AI systems. However, such systematic replies are almost nonexistent in India.

1.4 The Indian Legal Context and Research Gap

Despite the fast deployment of AI systems across industries, India lacks a specific legal framework for addressing responsibility in AI-driven decisions. Current laws, such as the Information Technology Act of 2000, the Indian Penal Code of 1860, the Consumer Protection Act of 2019, and tort law, were not designed with AI in mind and offer limited remedy for those affected by automated or algorithmic choices. While Indian study has focused on data protection and ethical AI governance, there is a significant void in literature and legislation about legal culpability for AI-caused harm. This leaves Indian courts and regulatory authorities unprepared to assign blame when AI systems have unexpected repercussions.

Research Objectives

1. To evaluate the current Indian legal framework governing AI-related liability.
2. To find legal and philosophical gaps in determining liability for AI-caused harm.
3. To establish a comprehensive, constitutionally sound liability framework for artificial intelligence in India.

Research Question

1. How may culpability be apportioned in India when an artificial intelligence system causes injury without direct human intervention?
2. How effective are existing Indian legal frameworks—such as the Information Technology Act, IPC, and Consumer Protection Act—in mitigating AI-related harms?
3. How may Indian tort and contract law principles be construed or revised to account for the complexity of AI autonomy and algorithmic decision-making?
4. How might legal approaches to AI liability in other jurisdictions (such as the EU or the United States) influence the development of an Indian model for responsibility allocation?
5. How should responsibility be split among developers, deployers, consumers, and governmental authorities when AI technologies are employed in sensitive industries such as healthcare or policing in India?

Literature Review

Matthias, A. (2004). “The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata.”

Matthias explains the "responsibility gap" that occurs when machine learning systems behave in ways that their founders did not intend. He contends that classic legal notions such as purpose and foreseeability fail to apply to non-human decision-makers. This issue is particularly pertinent in India, where laws are still based on the assumption of human action and foreseeability, leaving gaps in determining accountability when AI commits harm autonomously.

2. Pagallo, U. (2013). “The Laws of Robots: Crimes, Contracts, and Torts.”

Pagallo investigates the legal treatment of robots and AI under civil and criminal law. He investigates the application of product responsibility and tort law to intelligent computers and addresses the difficulties in defining agency and personhood. His work implies that liability should be spread, which has consequences for India, where no AI-specific legislation exist and obligations are legally murky.

Although international researchers such as Matthias and Pagallo have tackled AI culpability using notions such as the "responsibility gap" and modified legal doctrines, their research has been focused on established Western jurisdictions with emerging AI-specific policies. In contrast, India's legal structure, which is based on pre-digital legislation, has not sufficiently addressed the intricacies of AI-related harm, particularly in terms of responsibility in autonomous and opaque decision-making. Although Indian academia has looked into AI ethics and data protection, there has been no doctrinal study of culpability across the AI lifespan. This paper fills that gap by analyzing the constraints of Indian laws and proposing a contextual responsibility framework tailored to India's socio-legal circumstances.

Research Methodology

The paper applies a doctrinal legal research technique, based on a critical examination of legislative provisions (e.g., IT Act, IPC, Consumer Protection Act, and Contract Act), judicial decisions, academic literature, and legal theory. A comparative legal analysis is also used to get insights from global models such as the European Union's AI Act and US tort law techniques. To analyze the practical obstacles in culpability attribution, hypothetical and real-world use examples are included, such as facial recognition failures or AI-based credit denials.

2-Understanding AI-Driven Decision-Making

2.1 Definition and Types of AI-Driven Decisions

Artificial intelligence (AI)-driven decision-making is the process by which computer systems, particularly those that use machine learning (ML), deep learning, or neural networks, make or influence

decisions that previously required human judgment From straightforward rule-based outcomes to intricate autonomous actions, these judgments can take many forms. Three categories of AI judgments can be distinguished:

Assisted Decision-Making: AI delivers data-driven insights or recommendations, while a human maintains final control (for example, medical diagnosing tools).

1. Automated Decision-Making: The system makes decisions using pre-defined rules with little or no human intervention (for example, loan approval automatically).
2. Autonomous Decision-Making: Advanced systems make their own decisions and evolve over time using unsupervised or reinforcement learning.

These categories differ not just in their level of autonomy, but also in their legal ramifications, particularly in terms of foreseeability, intent, and control, all of which are crucial in determining culpability.

2.3 Use Cases in Indian Context

Artificial intelligence-driven decision-making has already made inroads into numerous major areas in India, sometimes without proper regulatory or ethical oversight:

1. Lending and Credit Scoring: Fintech companies and digital lenders employ artificial intelligence to assess creditworthiness based on alternative data such as social media activity or mobile usage trends. While efficient, these solutions risk prejudice, lack transparency, and provide little recourse in the event of service refusal.
2. Healthcare: AI applications including as diagnostic imaging, therapy prediction, and hospital triage are currently being tested in Indian public and private hospitals. However, errors in diagnosis or triage caused by faulty training data or unsupervised AI could result in catastrophic harm with no obvious blame attribution.The Black Box Problem and Algorithmic Opacity
3. Facial Recognition and Law Enforcement: Government programs such as the National Automated Facial Recognition System (AFRS) and state police departments are increasingly using artificial intelligence for surveillance and identification. These systems raise concerns about mistaken identification, privacy invasion, and racial or caste bias—all without adequate safeguards or accountability measures.

These examples demonstrate that, while AI promises efficiency and scale, its implementation in India poses a danger of harm in the absence of effective processes to assign blame and ensure redress. The absence of algorithmic openness, paired with India's social and legal intricacies, highlights the urgent need for a contextual responsibility framework.

3 -The Concept of Legal Liability in the Context of AI

3.1 Traditional Concepts of Legal Liability

Legal liability is commonly defined as the status of being legally accountable for anything, particularly for acts or omissions that cause injury. Traditional legal doctrine divides responsibility into the following categories:

1. Civil liability- arises from a breach of contractual agreements or duties under civil law. This encompasses situations in which one party fails to fulfill a legal obligation, resulting in loss or injury to another (for example, service breakdown under a software contract).
2. Criminal Liability- Assigned when a person or corporation does an act that is considered a criminal under penal statutes. Establishing mens rea (criminal intent) and actus reus (wrongful deed) in AI environments can be problematic.
3. Tort Liability- A subset of civil liability, tort law addresses harm or injury caused by carelessness, nuisance, or strict liability. Tort principles such as duty of care, causation, and foreseeability are critical in determining culpability and compensation.
4. Statutory liability- arises from breaches of requirements established by specific statutes, such as the Information Technology Act of 2000 or the Consumer Protection Act of 2019. These may hold organizations or people liable for losses such as data breaches, poor services, or unfair business practices.

Traditionally, culpability implies a human actor capable of purpose, negligence, or knowledge of harm—criteria that AI systems do not meet directly.

3.2 Challenges in Assigning Liability to AI Systems

AI complicates the established frameworks in numerous ways:

Autonomy and Lack of Intent: AI systems, particularly those based on machine learning, make decisions without explicit human instructions or predicted reasoning. Because AI lacks consciousness and legal personality, it cannot be held responsible in the traditional sense.

1. Opacity and Explainability: Because many AI algorithms are "black-box" in nature, even developers may not completely comprehend how a decision was reached. This makes it difficult to show causation, foreseeability, or negligence—all important tort law elements.
2. Distributed Responsibility: AI systems involve several actors, including developers, data scientists, vendors, platform providers, and end users. Determining who is to blame when harm happens becomes difficult, especially when responsibility is spread across borders or institutions.
3. Lack of Precedents and Regulatory Clarity: There is no case law or statutory guidance relevant to AI in Indian law. Existing legal principles were not intended to handle the harm produced by autonomous agents working at scale.

These elements contribute to a "responsibility gap" in which harm exists but no legally culpable actor fits into established legal categories.

3.3 Global Views on AI Accountability.

Legal systems around the world are experimenting with legislation and policies to address the issue of AI liability:

1. European Union-The proposed AI Liability Directive and AI Act seek to impose severe liability on high-risk AI applications. Developers and deployers may face liability regardless of guilt, particularly if AI causes personal injury or property damage.
2. The United States has primarily followed a sectoral and tort-based strategy, with cases interpreted using existing product liability and negligence doctrines. However, courts are wary and uneven due to the novelty of AI damages.
3. Singapore and Japan- have proposed frameworks for shared or distributed responsibility, recognizing the ecosystem nature of AI systems. These strategies strive to strike a balance between innovation with accountability.
4. UNESCO and the OECD- International organizations have adopted nonbinding guidelines on AI ethics and human accountability, emphasizing openness, justice, and traceability as legal requirements.

In contrast, India lacks a clear position or policy framework regarding AI liability. While the DPDP Act of 2023 addresses automated decision-making in terms of data protection, there is currently no complete law establishing legal liability for algorithmic harm.

4. Indian Legal Framework and AI

4.1 Overview of Relevant Indian Laws

Despite the rapid adoption of AI technologies across sectors in India, the country's legal framework remains fragmented and not specifically tailored to address the challenges posed by AI-driven decision-making. Existing laws must be interpreted and extended to cover emerging scenarios, often with significant ambiguity.

4.1.1 Information Technology Act of 2000.

The IT Act is India's primary legislation covering digital activities, cybercrime, and data security. While it governs intermediaries and cybercrimes, it does not address AI liability, algorithmic harm, or automated decision-making. Sections 43A and 72A hold firms liable for data breaches, however they do not apply to losses caused by autonomous AI choices. The Act's focus remains primarily on human-controlled systems.

4.1.2 Consumer Protection Act (2019)

This Act protects customers from unfair commercial practices, defective products, and poor service. Under this law, AI-based platforms or automated service providers may be held accountable for providing incorrect services. However, it is unclear how accountability would be ascribed when harm is caused by autonomous decision-making or algorithmic bias. especially in e-commerce, fintech, or telemedicine.

4.1.3 Indian Contract Act (1872)

AI systems frequently use smart contracts or algorithmically mediated agreements. However, the Act assumes legal personality, volition, and consent, all of which AI systems lack by definition. This raises concerns regarding enforceability, contract creation, and culpability when an AI agent enters or breaches a contract on behalf of a human or company.

4.1.4 Indian Penal Code (1860)

Criminal responsibility under the IPC is based on mens rea (criminal intent) and actus reus (criminal act). Assigning mens rea to an AI system is a conceptual difficulty. For example, if a facial recognition technology falsely implicates a person, resulting in arrest or damage, the problem is identifying whether any human actor had the necessary intent or negligence to support criminal culpability.

4.2 Judicial precedents and regulatory gaps.

Indian courts have yet to produce significant jurisprudence on AI liability. There are a few relevant precedents in data protection, algorithmic profiling, and surveillance (for example, Justice K.S. Puttaswamy v. Union of India), but they are largely indirect. There is no authoritative ruling that directly addresses the legal liability for AI-related harm.

Furthermore, regulatory authorities such as the RBI, SEBI, and NITI Aayog have produced position papers on safe AI use, but none of them have legislative authority or provide a binding legal framework. The Digital Personal Data Protection (DPDP) Act of 2023 acknowledges automated decision-making under consent rules, but does not specify liability or remedy methods.

4.3 Challenges in Applying Existing Laws to AI Systems.

1. Lack of Legal Personhood: Indian laws require a liable entity to be a person—natural or juristic. AI systems currently do not qualify, creating a gap when no direct human actor can be identified.
2. Attribution of Fault: In autonomous decision-making, tracing the source of harm—whether to the developer, deployer, user, or data provider—is technically and legally difficult.
3. Opacity and Explainability: Most Indian laws assume a human actor can explain or justify actions. AI systems, particularly deep learning models, often lack this capacity, making legal standards like "reasonable foreseeability" or "due diligence" hard to apply.
4. No Risk Classification or Registration: Unlike the EU, India lacks a tiered risk framework or registry for high-risk AI systems. This makes it difficult to pre-emptively regulate or hold actors accountable.
5. Cross-sectoral Confusion: Multiple sector-specific regulators (RBI, IRDAI, TRAI) may be involved in overseeing AI deployment, yet there is no harmonized liability standard across these regimes.

5 **Comparative Legal Approaches to AI Liability**.

As countries face the unique issues of governing artificial intelligence, several jurisdictions have developed distinct legal methodologies for assigning liability in AI-driven decisions. A comparison of the European Union and the United States provides valuable lessons for India as it develops its AI governance framework.

5.1 European Union: Comprehensive and Risk-Based Regulation

5.1.1 EU Artificial Intelligence Act

The European Commission proposed the Artificial Intelligence Act in 2021, which was implemented in 2024. It is the world's first horizontal legislative framework for AI. It categorizes AI systems into four danger levels: unacceptable, high risk, limited risk, and minimum risk. High-risk AI (such as in healthcare, employment, or law enforcement) must meet stringent requirements for openness, data quality, human monitoring, and documentation. While the AI Act does not define liability, it does set regulatory preconditions that influence how liability is determined under other EU legislation.

5.1.2 General Data Protection Regulation (GDPR)

The GDPR, enforced since 2018, regulates the processing of personal data by AI systems and introduces rights against automated decision-making (Article 22). It gives individuals the right to explanation, contestation, and human intervention when subjected to decisions made solely by automated means, especially those affecting legal rights or significant outcomes.

5.1.3 Product Liability Directive

The revised Product Liability Directive (2024) modernizes the EU's strict liability regime to cover AI systems as products, even when software is offered as a service. It removes the burden of proving fault when an AI product causes damage, holding developers or providers strictly liable. This is crucial in cases where causal links are hard to establish due to algorithmic opacity.

5.2 United States: Sectoral and Tort-Based Framework.

Unlike the EU's comprehensive model, the United States takes a fragmented, sector-specific approach based mainly on tort law and judicial interpretation.

5.2.1 Tort and Product Liability.

AI-related injuries are typically addressed using standard tort principles such as negligence, strict responsibility, and failure to warn. Plaintiffs must show duty, breach, causation, and injury. However, courts have struggled to apply these criteria to artificial intelligence, notably in cases involving self-driving cars, algorithmic discrimination, and medical diagnostic technologies.

5.2.2 Sectorial Regulation

The FDA (for AI in healthcare), FTC (for algorithmic transparency), and NHTSA (for self-driving cars) provide guidelines or non-binding rules. However, there is currently no federal legislation governing AI

liability. The Blueprint for an AI Bill of Rights (2022) provides ethical recommendations but lacks enforceability.

5.3 Lessons for India.

India may learn valuable lessons from both the EU and US approaches:

Domain Lessons for India.

Risk-Based Regulation.Adopt a tiered classification of AI systems based on their potential for damage (EU model).

1. Strict liability provisions.Establish statutory liability for high-risk or autonomous AI deployments.
2. Explainability StandardsMandate algorithmic transparency and human oversight in crucial sectors.
3. The Rights Framework protects individual rights against automated choices, comparable to GDPR.
4. Interim Tort AdaptationWhile formal AI laws are being developed, employ judicial interpretations of tort and contract law.
5. Unified Policy Approach: Create a centralized AI regulatory authority to prevent regulatory fragmentation.

India must strike a balance between innovation and responsibility, avoiding both overregulation and underregulation. Drawing on international experience, solutions will be tailored to local institutional and constitution context would be essential.

6 Who Should Be Held Responsible? Identifying Possible Actors in AI Liability

As artificial intelligence systems gain clout in vital areas such as healthcare, banking, policing, and employment, identifying who is legally liable when such systems cause harm becomes a critical legal and ethical concern. Several probable actors may be considered liable under Indian law:

6.1 Developers and Programmers

Software engineers, data scientists, and designers are accountable for:

1-Creating algorithms

2-Choosing training data,

3-Designing risk mitigating features.

If harm results from design defects, skewed datasets, or insufficient safety standards, developers may be held accountable under product liability, carelessness, or defective design principles. In India, such liabilities may arise under

1. The Consumer Protection Act of 2019
2. The Information Technology Act of 2000 (for intermediate and software responsibility)
3. Tort law (negligence and failing to warn).

Challenge: Developers frequently complain about a lack of predictability caused by AI's independent learning.

6.2 Deployers and Operators

Entities or persons who install or run AI systems—such as banks employing credit-scoring algorithms or law enforcement using facial recognition—have authority over:

1-Where and how AI is applied,

2-The operational environment

3-Human oversight.

They may be held liable under vicarious liability principles, particularly if harm results from poor implementation, a lack of transparency, or a failure to monitor system activity. This concept is most suited to India's existing contract and agency legislation (Indian Contract Act of 1872) and public law principles of governmental accountability.

6.3 End User or Client

End-users, such as doctors utilizing AI diagnosis tools or HR professionals using automated hiring software, may incur liability if they:

1. Fail to check AI outputs.
2. Rely on decisions without exercising human judgment.

However, their culpability should be restricted to negligence or misuse rather than defects in the system itself.

6.4 The AI System (Legal Personhood Debate)

Some have proposed creating autonomous AI "electronic personhood"—similar to corporate legal status—in order to hold AI directly answerable. However, this remains highly controversial and legally unviable in India, because:

Artificial intelligence lacks awareness, volition, or moral agency.

India's existing definition of "person" under constitutional and statute law (limited to natural or juristic persons)

Practical enforcement concerns (AI cannot hold assets, pay damages, or be punished).

Courts in India have been hesitant to extend legal personhood to non-human agents beyond symbolic exclusions (such as temples and rivers).

6.5 Shared and Hybrid Liability Models.

Given the scattered nature of AI development and deployment, a hybrid liability approach may be most suited. This may involve:

Developers for flawed design or bias.

Deployers for lack of supervision,

Users for negligent reliance.

Statutory caps or safe harbors may be available for good-faith actors who adhere to due diligence processes.

This multi-tiered duty would more accurately reflect the realities of AI ecosystems and be consistent with India's mixed legal tradition, which balances civil, tort, and statutory culpability.

Under India's current legal framework, AI systems cannot be held accountable. Instead, accountability must be assigned to human and corporate Human and corporate actors are ranked according to their level of control, knowledge, and intent. A doctrinal and legislative evolution is required to define and codify these obligations across industries.

7 Recommendations in the Indian context

Given the increasing deployment of AI systems across industries, as well as the current legal ambiguity surrounding responsibility for AI-driven judgments, India urgently demands a proactive, rights-based, and technically sound legislative framework. The ideas below try to fill the current legal and regulatory deficiencies.

7.1 Enact AI-specific legislation

India must go beyond fragmented statutory interpretations and pass comprehensive AI legislation that:

Clearly describes AI systems and categorises risk levels.

Establishes legal culpability standards based on control, intent, and foreseeability.

Balances innovation with constitutional guarantees such the right to equality, privacy, and due process.

Such legislation should align with existing laws (IT Act, Consumer Protection Act, IPC) and include clear liability provisions for developers, deployers, and users.

7.2 Create a centralized regulatory authority for AI governance.

A separate AI regulatory entity should be established, comparable to the European Union's AI Office or sectoral regulators such as SEBI or TRAI. Functions should include:

1-Developing and upgrading risk-based standards

2-Overseeing compliance and certification mechanisms.

3-Investigating harms and enforcing fines.

4-Working with sector-specific regulators (e.g., in health, finance, and law enforcement).

This authority must have legal, technological, and ethical knowledge while remaining independent and transparent.

7.3 Mandatory Auditing for High-Risk AI Systems

AI systems deployed in high-risk domains—such as healthcare diagnostics, predictive policing, credit scoring, and hiring—should undergo:

1-Third-party algorithmic audits can reveal bias or discrimination.

2-Impact assessments to ensure data privacy and fairness,

3-System upgrades mistake rates, and decision rationales are all reported on a regular basis.

Such audits may be mandated by law, with civil or criminal consequences for noncompliance.

7.4 Introducing Liability Insurance for AI-Based Services

India should adopt a compulsory AI liability insurance policy, similar to how doctors and attorneys have professional indemnity insurance.

1-To compensate for damages caused by computational errors, bias, or malfunction,

2-To ensure that victims of AI-related injury receive timely compensation,

3-To motivate companies to keep AI systems safe and explainable.

This would also cut litigation costs and explain financial risk allocation.

1. Implement Guiding Principles: Transparency, Accountability, and Fairness.Any legal and regulatory reaction to AI should be based on the following principles
2. Transparency: Make sure that AI decisions are explainable to those affected.
3. Accountability: Assign unambiguous legal responsibilities to human and business actors throughout the AI lifespan.
4. Fairness and Non-Discrimination: Prevent algorithmic harms that propagate societal biases, caste discrimination, or economic disadvantage.

These ideas can be included into laws, public procurement regulations, and sectoral standards.

A future-ready AI liability framework for India must be multi-layered, cross-sectoral, and based on constitutional values. Without defined norms for accountability, AI systems may jeopardize legal certainty, justice, and public trust. The proposed proposals seek an equal balance between responsible innovation and legal accountability.

8 Conclusion.

This study critically explored the issue of legal culpability for AI-driven choices in India. It emphasized the growing reliance on AI systems in critical sectors such as healthcare, finance, policing, and human

resources, and revealed that existing Indian legal frameworks—including the IT Act, Consumer Protection Act, IPC, and Contract Law—are insufficient to address the challenges posed by autonomous, opaque, and data-driven decision-making. The review of doctrinal limits, comparative foreign models, and legal personhood issues demonstrates that Indian law lacks unambiguous procedures for assigning blame when AI systems cause harm.

Key findings highlight the lack of AI-specific rules, ambiguous accountability chains, and the limited applicability of classic responsibility doctrines such as negligence, vicarious culpability, and strict liability. Globally, jurisdictions such as the EU and the United States are actively creating liability regimes through legal instruments such as the EU AI Act and sectoral tort frameworks, providing valuable insights into India's future path.

The study's consequences are far-reaching: legal systems must adapt to protect fundamental rights, technology must be guided by enforced ethical standards, and governance methods must strike a balance between innovation and responsibility. India must rapidly adopt AI-specific legislation, establish an independent regulatory authority, require audits of high-risk systems, and implement fairness and transparency principles across industries.

Future research should look into legal interpretations of AI-related harms in India, sector-specific liability case studies, and the socio-technical effects of AI deployment on vulnerable groups. Legislative reform is required not only to reduce the accountability gap, but also to create a trustworthy and rights-compliant AI ecosystem.

References

- Baxi, U. (2023). Law, technology, and constitutionalism in the Global South. Oxford University Press.
- Calo, R. (2015). Robotics and the lessons of cyberlaw. California Law Review, 103(3), 513–563. https://doi.org/10.2139/ssrn.2402972https://doi.org/10.2139/ssrn.2402972
- Chopra, S., & White, L. F. (2011). A legal theory for autonomous artificial agents. University of Michigan Press.
- Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin’s Press.

- European Parliament. (2017). Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.htmlhttps://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html
- Ghosh, S. (2022). Regulatory sandboxes and safe harbours for AI in India. Vidhi Centre for Legal Policy Working Paper. https://vidhilegalpolicy.inhttps://vidhilegalpolicy.inhttps://doi.org/10.1525/nclr.2016.19.3.412
- Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? Self-driving cars and criminal liability. New Criminal Law Review, 19(3), 412–436. https://doi.org/10.1525/nclr.2016.19.3.412
- Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.
- Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- Kumar, A. (2023). Shared liability in complex tech environments: An Indian perspective. NUJS Law Review, 16(1), 101–120. https://nujslawreview.orghttps://nujslawreview.org
- Mehta, P. (2023). Contractual oversight and liability in automated systems. NLSIU Review of Public Law, 7(2), 89–105.
- Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2). https://doi.org/10.1177/2053951716679679https://doi.org/10.1177/2053951716679679
- Mohd. Salim v. State of Uttarakhand, 2017 SCC OnLine Utt 367 (India).
- NITI Aayog. (2021). Responsible AI for All: Part 1 – Principles for Responsible AI. Government of India. https://niti.gov.in
- Pagallo, U. (2013). The laws of robots: Crimes, contracts, and torts. Springer.
- Singh, R. (2020). Negligence and AI in Indian tort law. Indian Journal of Law and Technology, 16(1), 45–61. https://ijlt.in
- Solaiman, S. M. (2017). Legal personality of robots, corporations, and animals: A comparative analysis. Artificial AIntelligence and Law, 25(3), 269–291https://doi.org/10.1007/s10506-017-9212-0