INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE AND LEGAL LIABILITY: EMERGING CHALLENGES IN INDIA

AUTHORED BY - NEELANSH RAO & PRATIKSYA JENA

Abstract

The rapid proliferation of Artificial Intelligence (AI) systems across sectors ranging from healthcare diagnostics and autonomous mobility to judicial decision-support and financial credit-scoring has generated a profound and largely unresolved question of legal liability in India. Existing Indian legislation - principally the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Consumer Protection Act, 2019 - was neither designed nor sufficiently interpreted to address the distinctive attributes of AI: opacity, autonomy, adaptability, and multi-party causal chains.[4] This paper undertakes a systematic doctrinal and comparative analysis of the liability gap confronting Indian jurisprudence. Drawing on frameworks from the European Union's AI Act 2024, the United States' sector-specific regulatory approach, and emerging scholarly discourse, the paper identifies five structural impediments: the identification problem, the causation problem, the attribution problem, the accountability problem, and the remediation problem. The paper proposes a three-tier legislative architecture comprising an AI Liability Act, an AI Safety Authority, and a specialised AI Tribunal. The research concludes that incremental statutory interpretation is insufficient and only purpose-built legislative reform can ensure that technological innovation proceeds with commensurate legal responsibility.

Keywords: *Artificial Intelligence, Legal Liability, India, AI Act, Algorithmic Accountability, Product Liability, Digital Personal Data Protection, Negligence, Strict Liability, AI Governance.*

ISSN: 2582-6433

1. Introduction

India's Artificial Intelligence (AI) economy is projected to contribute approximately USD 967 billion to the national GDP by 2035, positioning the country as one of the most consequential AI markets globally.[1] Yet the velocity of AI deployment has dramatically outpaced the evolution of legal and regulatory frameworks designed to govern the attendant risks. As AI systems increasingly make or materially influence decisions that affect fundamental rights - from bail determinations and loan applications to medical diagnoses and content moderation - the question of who bears legal responsibility when such systems cause harm has become both theoretically significant and practically urgent.

The challenge is not merely one of legislative lacuna but of conceptual architecture. Traditional Indian tort law, modelled substantially on English common law principles of negligence, causation, and foreseeability, presupposes a human actor whose conduct can be evaluated against an objective standard of reasonable care. When an AI system trained on historical data perpetuates discriminatory lending patterns, or when an autonomous diagnostic algorithm misclassifies a malignant tumour, the causal chain between the harm and any identifiable human decision-maker is attenuated, fragmented, or wholly opaque.[6] This "responsibility gap" has been widely identified in global legal scholarship but remains institutionally unaddressed in India.

This paper proceeds in seven substantive sections. Section 2 provides a landscape survey of AI deployment in India. Section 3 analyses the existing legal architecture and its inadequacies. Section 4 examines the five structural problems in AI liability attribution. Section 5 undertakes a comparative study of international frameworks. Section 6 advances a legislative reform proposal tailored to Indian constitutional and socio-economic conditions. Section 7 concludes with reflections on the path forward.

2. The AI Landscape in India: Scale, Sectors, and Stakes

2.1 Sectoral Deployment

India's AI deployment spans both public and private sectors with remarkable breadth. The healthcare sector has witnessed the introduction of AI-powered diagnostic tools, including those employed by the National Digital Health Mission for radiological image analysis. The judiciary has experimented with AI tools for case management and predictive analytics in bail

ISSN: 2582-6433

determinations, raising acute questions of algorithmic fairness and due process.

The financial sector presents perhaps the most consequential deployment. Non-Banking Financial Companies (NBFCs) and FinTech platforms increasingly rely on machine learning credit-scoring models that draw on non-traditional data - social media activity, app usage patterns, and geolocation - to assess creditworthiness.[11] Such systems affect millions of borrowers, yet the Reserve Bank of India has issued only limited guidance on algorithmic accountability in lending.

2.2 Data on AI-Related Incidents in India

The following visualisations illustrate the growing frequency of AI-related legal incidents in India relative to global trends, alongside the distribution of cases across application domains.

Figure 1: Reported AI-Related Legal Incidents (India vs. Global, 2018-2024)

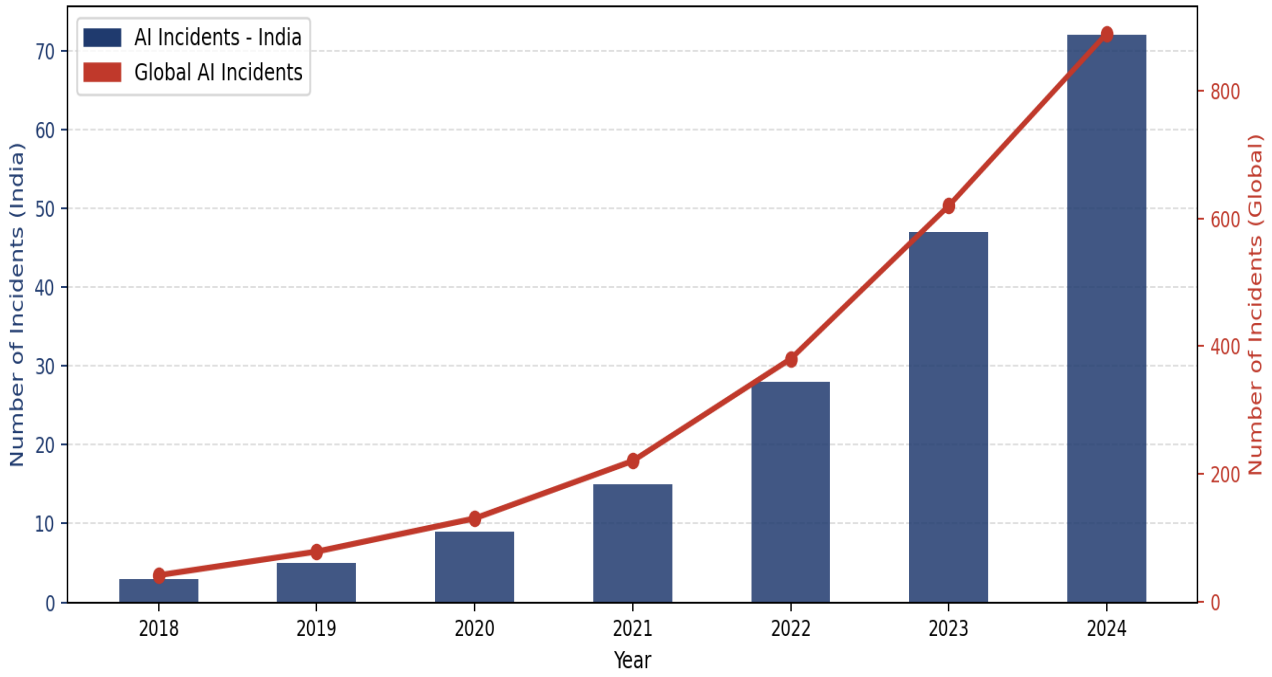

Figure 1: Reported AI-Related Legal Incidents, India vs. Global (2018-2024). Source: AI Incident Database (2024); Authors' compilation.

Figure 1 demonstrates a near-24-fold increase in reportable AI incidents in India between 2018 and 2024, tracking but lagging global trends.[10] The accelerating trajectory from 2021 onwards correlates with the mass adoption of large language models, AI-powered lending platforms, and automated content moderation systems. Importantly, these visible incidents represent only a fraction of total AI harms, as the absence of mandatory incident reporting produces significant under-reporting.

 ISSN: 2582-6433

Figure 2: Distribution of AI Legal Liability Cases by Domain (Global Dataset, 2019-2024)

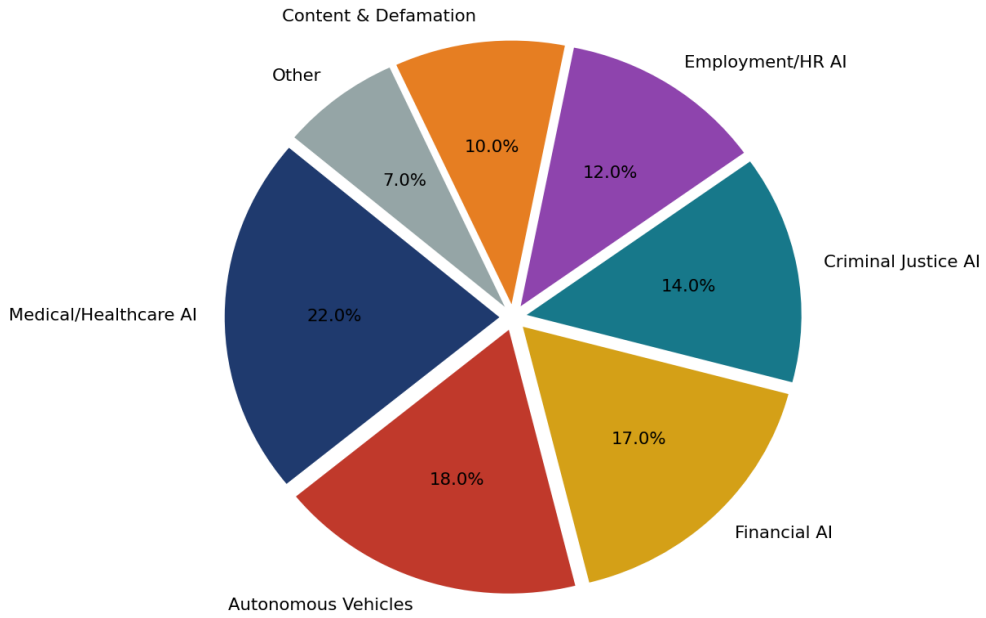

Figure 2: Distribution of AI Legal Liability Cases by Domain (Global Dataset, 2019-2024). Source: Authors' analysis; Stanford AI Index 2024.

Figure 2 reveals that healthcare AI, autonomous vehicles, and financial AI collectively account for approximately 57% of global AI liability cases. These three domains are precisely those in which India is witnessing the most aggressive deployment, signalling that India's courts and regulatory bodies will soon confront an escalating docket of AI-related disputes for which current legal frameworks are manifestly inadequate.

3. The Existing Indian Legal Framework and Its Inadequacies

3.1 Constitutional Foundations

The Constitution of India provides an overarching normative framework within which AI governance must be situated. Article 21 (right to life and personal liberty), Article 14 (equality before law), and Article 19(1)(g) (right to carry on any occupation, trade, or business) collectively create both rights that AI may imperil and freedoms that AI-enabling legislation must not unnecessarily curtail. The Supreme Court in Shreya Singhal v. Union of India established that technological regulation must satisfy the tests of proportionality and reasonableness,[18] a standard directly applicable to AI liability legislation.

ISSN: 2582-6433

3.2 The Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) constitutes the foundational legislation governing digital conduct in India.[5] Section 43A creates civil liability for 'body corporates' that negligently handle sensitive personal data, while Section 72A creates criminal liability for wrongful disclosure of personal information. However, the IT Act was conceived to address human-authored digital offences - hacking, phishing, identity theft - and its drafters did not anticipate scenarios in which autonomous, learning systems produce harmful outputs without direct human instruction. The Act contains no provisions addressing algorithmic decision-making, AI system design obligations, or vicarious liability for autonomous agents.

3.3 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's most contemporary legislative engagement with data-driven technologies.[4] The Act mandates purpose limitation, data minimisation, and consent-based processing. However, it does not address downstream liability arising from AI decisions made using lawfully processed data. An AI system may process personal data entirely in compliance with the DPDP Act and yet produce a discriminatory credit-scoring decision causing substantial individual harm. The DPDP Act addresses the input dimension of AI harm but is silent on the output dimension.

3.4 Consumer Protection Act, 2019

The Consumer Protection Act, 2019 (CPA) provides potentially the most immediate avenue for AI-related redress in India, through its provisions on 'deficiency of service' and 'product liability' under Chapter VI.[13] Section 82 imposes strict liability on product manufacturers for defects, and Section 86 extends liability to product sellers. The challenge lies in the AI context: whether AI software constitutes a 'product' under Section 2(33), whether an AI-driven service failure constitutes a 'defect' under Section 2(10), and how liability is apportioned across a supply chain comprising data providers, model developers, cloud infrastructure operators, and application deployers. Judicial guidance on these questions remains conspicuously absent.

ISSN: 2582-6433

Figure 3: India's Legal Framework - Current vs. Required Adequacy for AI Governance

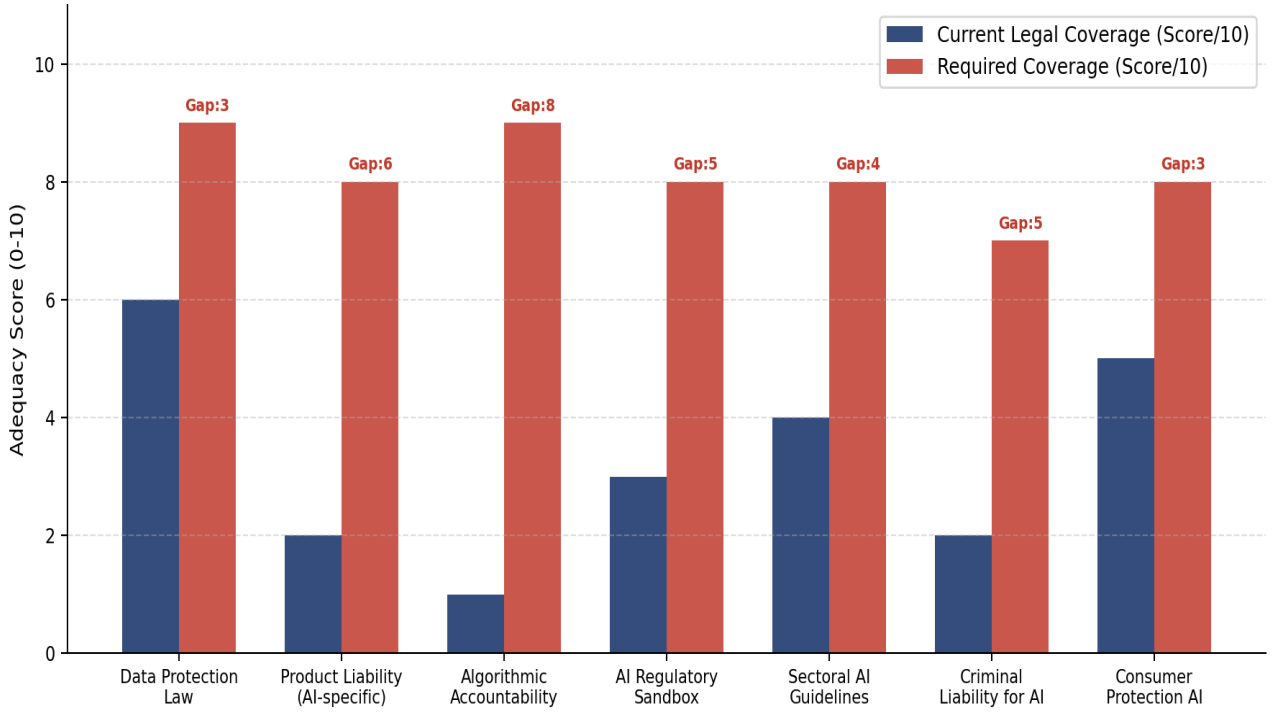

Figure 3: India's Legal Framework - Current vs. Required Adequacy Scores for AI Governance (Authors' Assessment, 2024).

Figure 3 presents the authors' assessment of India's current legal coverage against an expert-benchmarked required standard across seven AI governance dimensions.[20] The most critical gaps appear in algorithmic accountability (gap: 8), product liability specific to AI (gap: 6), and criminal liability for AI-enabled harms (gap: 5). These gaps collectively represent the legislative terrain that any reform proposal must address.

4. Structural Problems in AI Liability Attribution

4.1 The Identification Problem

The first structural problem is identifying the responsible party across a complex, multi-layered AI development and deployment chain. A typical AI system involves: (i) data aggregators who compile training datasets; (ii) foundational model developers who train large-scale models; (iii) fine-tuners who adapt models for specific applications; (iv) integrators who embed models into products; and (v) deployers who offer the final service to end-users.[14] Indian law has not yet developed principles for allocating liability across this chain, creating a systemic incentive for each party to disclaim responsibility.

ISSN: 2582-6433

4.2 The Causation Problem

Establishing causation in AI-related harms requires proof that a specific algorithmic output caused the plaintiff's injury. Deep neural networks present near-intractable opacity - the so-called "black box" problem[19] - making it practically impossible for a plaintiff to reconstruct the internal processing chain that led to a harmful decision. Indian courts applying the "but for" test derived from Donoghue v. Stevenson principles[12] will struggle to apply this counterfactual standard when the model's internal logic is inaccessible even to the model's own developers.

4.3 The Attribution Problem

AI systems trained on historical data may perpetuate and amplify systemic biases without any explicit instruction to discriminate. An AI hiring tool trained predominantly on male-dominated professional histories may systematically disadvantage women candidates, yet no individual human decision-maker may have intended this outcome. Attribution of liability in such cases requires a theory of structural responsibility that Indian tort law, premised on individual fault, is currently ill-equipped to provide.

4.4 The Accountability Problem

The accountability problem concerns institutional mechanisms for ongoing oversight of AI systems post-deployment. Unlike a defective product with a fixed state, an AI system may continue to evolve through learning, potentially drifting from its originally approved parameters.[16] India currently has no mandatory AI system auditing requirements, no obligation to maintain model cards or data sheets, and no regulatory body with technical competence to assess AI safety. NITI Aayog's Responsible AI frameworks[17] remain aspirational guidance without enforcement authority.

4.5 The Remediation Problem

Even where liability is established, the remediation problem asks: what form should redress take? Traditional compensatory damages may be inadequate where AI-mediated harms are diffuse or affect populations rather than identifiable individuals. A biased credit-scoring algorithm may deny thousands of eligible applicants without any single denial being individually actionable. Class action mechanisms under the CPA 2019 provide a partial avenue, but procedural constraints and the novelty of algorithmic harm claims render this an incomplete remedy.

ISSN: 2582-6433

5. Comparative International Frameworks

5.1 The European Union: A Risk-Based Tiered Approach

The European Union's AI Act (Regulation 2024/1689), which entered into force in August 2024, represents the world's first comprehensive, binding AI regulatory framework.[2] The Act adopts a risk-based tiered architecture, classifying AI systems into four categories: unacceptable risk (prohibited), high-risk (subject to ex ante conformity assessment, technical documentation, and post-market monitoring), limited risk (subject to transparency obligations), and minimal risk (unregulated). Critically, the Act imposes strict liability on providers of high-risk AI systems for damages caused by AI outputs, dramatically reducing the evidentiary burden on plaintiffs.

5.2 The United States: Sectoral Fragmentation

The United States has adopted a fundamentally different approach, relying on existing sector-specific regulatory agencies - the Food and Drug Administration for medical AI, the Federal Trade Commission for consumer-facing AI, and the National Highway Traffic Safety Administration for autonomous vehicles - supplemented by the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (October 2023). This approach preserves flexibility but produces regulatory gaps and inconsistencies. No federal AI-specific liability statute exists, leaving plaintiffs dependent on general products liability, negligence, and consumer protection doctrines of variable adequacy.

5.3 China: Provider-Centric Strict Liability

China's Interim Measures for the Management of Generative Artificial Intelligence Services (2023) impose primary liability on 'providers' of generative AI services, defined broadly to encompass model developers and application deployers. The strict liability model eliminates the plaintiff's burden to establish negligence, instead requiring the provider to demonstrate that it took all feasible precautions to prevent the harm. This approach prioritises victim compensation but may disincentivise AI innovation if insufficiently calibrated.

ISSN: 2582-6433

5.4 Comparative Framework Analysis

Figure 4: Comparative International AI Liability Frameworks (2024)

Jurisdiction	Primary Legislation	Liability Model	Strict Liability?	AI-Specific Law?
European Union	AI Act 2024 + Product Liability Directive	Risk-based tiered	Yes (High-risk)	Yes
United States	Sector-specific (FDA, FTC, NHTSA)	Negligence/Product	Partial	No (Federal)
United Kingdom	AI Safety Framework (2023)	Common Law + Guidance	Under review	No
China	Generative AI Regulation 2023	Provider-liability	Yes	Yes (Partial)
Singapore	Model AI Governance Framework	Voluntary + Guidance	No	No
India	DPDP Act 2023 + IT Act 2000	Negligence (implicit)	No	No

Figure 4: Comparative International AI Liability Frameworks (2024). Source: Authors' compilation from primary legislation and secondary sources.

Figure 4 crystallises the key dimensions of divergence across six major jurisdictions. India stands as the only major AI-deploying economy that has neither enacted AI-specific legislation nor extended strict liability principles to AI-caused harms.[3] This positions India at significant comparative disadvantage both in terms of investor confidence (as legal uncertainty increases transactional risk) and user protection (as victims of AI harm lack adequate redress). The EU model, while regulatory in character, offers the most sophisticated template for a jurisdiction of comparable scale and diversity, though significant adaptation to India's constitutional framework and developmental priorities is necessary.

6. Towards an Indian AI Liability Framework: A Reform Proposal

6.1 Design Principles

Any legislative framework for AI liability in India must be anchored in four design principles derived from both constitutional mandates and comparative best practice:

* Proportionality: Regulatory obligations must be calibrated to the risk profile of the AI application, avoiding disproportionate compliance burdens on low-risk or beneficial systems.
* Technology Neutrality: Legislation must be framed in terms of functional outcomes and harms rather than specific technical architectures, ensuring durability across rapid technological change.
* Access to Justice: Procedural mechanisms must be designed to overcome the asymmetric information and resource disparities between AI-deploying corporations and affected individuals.

ISSN: 2582-6433

* Innovation Facilitation: The framework must not create regulatory conditions so adverse as to divert AI investment to less regulated jurisdictions, undermining India's development objectives.

6.2 Proposed Three-Tier Architecture

Tier 1: AI Liability Act

The centrepiece of the proposed reform is a standalone AI Liability Act modelled broadly on the EU AI Act but adapted to Indian legal traditions. Key provisions would include:

* A risk classification system designating "high-risk AI systems" in sectors including healthcare, financial services, criminal justice, employment, and critical infrastructure.
* Mandatory conformity assessments for high-risk systems prior to deployment, involving technical auditing by accredited third-party bodies.
* Reversed burden of proof: where a plaintiff demonstrates that an AI system caused harm, the defendant bears the burden of proving technical compliance and that the harm was unforeseeable.
* A minimum liability insurance requirement for high-risk AI deployers, creating an assured compensation fund for victims.
* A "right to explanation" for individuals adversely affected by automated decisions, operationalising the transparency principle already nascent in the DPDP Act.

Tier 2: AI Safety Authority of India (ASAI)

The second tier comprises a statutory AI Safety Authority of India (ASAI), established with technical, legal, and domain expertise.[8] ASAI's mandate would encompass: pre-market technical assessment of high-risk AI systems; post-deployment monitoring and incident reporting obligations; sector-specific guidance in coordination with existing regulators (RBI, SEBI, MCI, IRDAI); and international engagement with the EU AI Office and global standard-setting bodies. ASAI would be empowered to order product withdrawals, impose administrative penalties, and publish mandatory incident reports.

Tier 3: Specialised AI Tribunal

The third tier is a specialised AI Tribunal with jurisdiction over civil liability claims arising from AI-related harms. The Tribunal would feature: simplified pleading rules eliminating the need for plaintiffs to specify the precise technical mechanism of harm; court-appointed technical experts to bridge evidentiary asymmetry; class action provisions enabling

 ISSN: 2582-6433

representative claims for population-level algorithmic harms; and expedited procedures to ensure that the pace of judicial resolution is commensurate with the pace of technological harm. Appeals would lie to the High Court on questions of law.

6.3 Proposed Liability Attribution Model

Figure 5 presents the authors' proposed liability attribution model, which operationalises the legal framework at the level of individual harm events.

Figure 5: Proposed AI Liability Attribution Framework for India

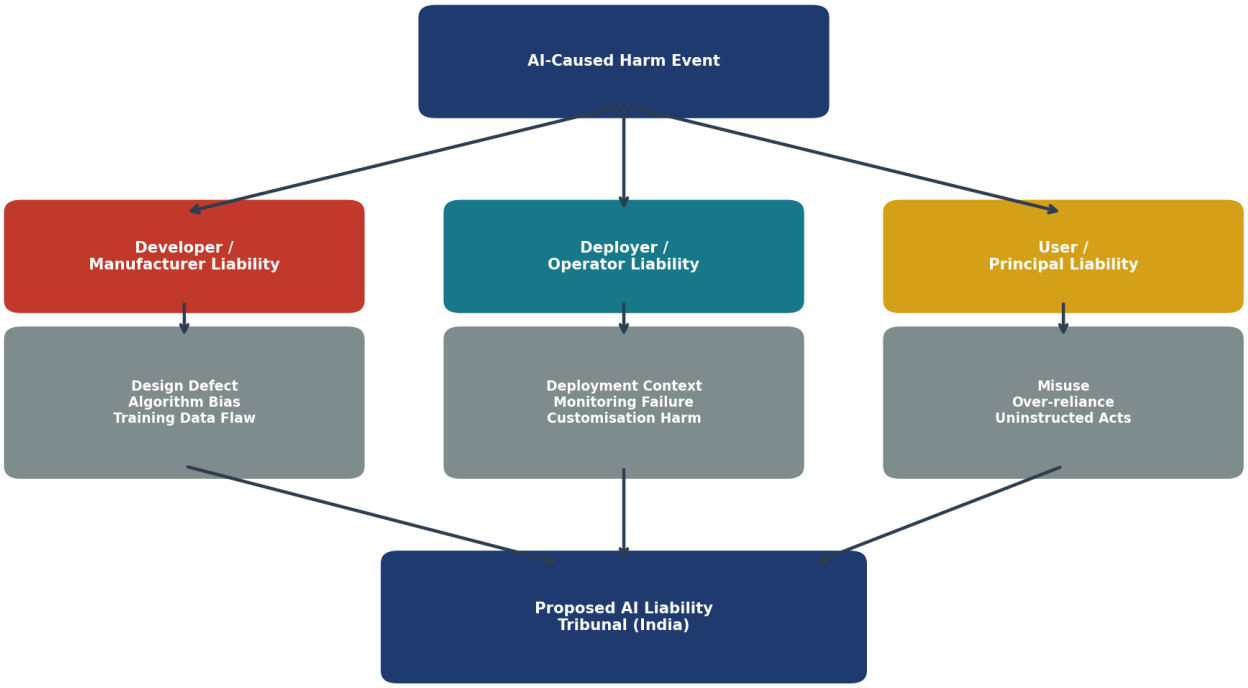

Figure 5: Proposed AI Liability Attribution Framework for India. Source: Authors' original framework (2024).

The attribution model in Figure 5 proceeds from a harm event through three parallel liability channels: developer/manufacturer liability (for design defects, algorithmic bias, and training data flaws); deployer/operator liability (for contextual misapplication, monitoring failures, and unauthorised customisation); and user/principal liability (for foreseeable misuse or over-reliance).[9] All three channels converge at the proposed AI Tribunal, which determines appropriate apportionment of liability through structured contributory fault analysis. This model accommodates the multi-party causal chains characteristic of AI systems while preserving the doctrinal coherence of Indian tort law.

ISSN: 2582-6433

6.4 Constitutional Compatibility

The proposed framework must satisfy constitutional scrutiny under Articles 14 and 19. The risk-classification approach satisfies Article 14's equality requirement by ensuring that like AI systems are treated alike, irrespective of the commercial size of the deployer.[7] The right to explanation provision engages Article 21's liberty guarantee, grounding the procedural entitlement in substantive constitutional rights. The mandatory insurance requirement constitutes a reasonable restriction on the right to carry on business under Article 19(1)(g), proportionate to the legitimate state interest in protecting citizens from AI harm. The legislative competence of Parliament to enact the AI Liability Act is well-established under Entry 97 of List I (residuary) and Entries 42 and 43 of List III (concurrent) of the Seventh Schedule.

7. Conclusion

This paper has demonstrated that India confronts a structural legal liability gap in the governance of artificial intelligence that is both theoretically significant and practically consequential. Existing legislative instruments - the IT Act, DPDP Act, Consumer Protection Act, and the general law of torts - provide fragmented, inadequate, and conceptually ill-suited tools for addressing the distinctive features of AI-caused harm: opacity, autonomy, multi-party causal chains, and population-level impact.

The comparative analysis demonstrates that leading jurisdictions have responded to this challenge through purposive legislative reform: the EU through its comprehensive, risk-based AI Act; China through provider-centric strict liability; and the United States through intensified sectoral regulatory engagement. India's current reliance on interpretive stretching of pre-digital legislation is unsustainable as AI deployment accelerates across sectors affecting hundreds of millions of citizens.[2]

The three-tier reform architecture proposed in this paper - comprising an AI Liability Act, an AI Safety Authority of India, and a specialised AI Tribunal - offers a constitutionally grounded, innovation-sensitive, and victim-protective framework for Indian AI governance. The framework is designed to be technology-neutral, scalable to future AI developments, and compatible with India's federal constitutional structure.

Ultimately, the legal challenge posed by artificial intelligence is not merely one of adaptation

ISSN: 2582-6433

but of institutional imagination. India has the opportunity to develop an AI liability framework that reflects its own constitutional values, developmental priorities, and social realities, rather than importing frameworks designed for different legal traditions. The time for that institutional imagination is now, before the accumulation of unredressed AI harms forecloses the space for principled legislative design.

References

A. Primary Sources: Legislation

a. Constitution of India, 1950.
b. Information Technology Act, 2000 (No. 21 of 2000), Government of India.
c. Information Technology (Amendment) Act, 2008, Government of India.
d. Consumer Protection Act, 2019 (No. 35 of 2019), Government of India.
e. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Government of India.
f. Regulation (EU) 2024/1689 of the European Parliament and of the Council (AI Act), Official Journal of the European Union, L 2024/1689.
g. China, Interim Measures for the Management of Generative Artificial Intelligence Services, Cyberspace Administration of China, 2023.

B. Primary Sources: Case Law

h. M.C. Mehta v. Union of India, AIR 1987 SC 1086 (Supreme Court of India).
i. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).
j. Bangalore Electricity Supply Company Limited v. Hennur Properties (P) Ltd., (2022) 6 SCC 401.
k. Donoghue v. Stevenson [1932] AC 562 (House of Lords).
l. Bolam v. Friern Hospital Management Committee [1957] 1 WLR 582 (Queen's Bench Division).

C. Secondary Sources: Books and Monographs

m. Floridi, L. et al., The Ethics of Artificial Intelligence: Principles and Frameworks (Oxford University Press, 2022).
n. Pasquale, F., The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, 2015).

ISSN: 2582-6433

o. Calo, R., Frischmann, B., & Strandburg, K. (eds.), Governing Privacy and the Internet (Cambridge University Press, 2019).
p. Balganesh, S., Copyright, Creativity, Commerce: The Making of the Indian Copyright Act (Oxford University Press, 2018).

D. Secondary Sources: Journal Articles

q. Calo, R., "Robotics and the Lessons of Cyberlaw" (2015) 103 California Law Review 513.
r. Floridi, L. et al., "An Ethical Framework for a Good AI Society" (2018) 28 Minds and Machines 689.
s. Gersen, J.E. & Vermeule, A., "Thin Rationality Review" (2007) 114 Michigan Law Review 1355.
t. Venkatesan, S., "Artificial Intelligence and the Question of Legal Personhood in India" (2022) 34 National Law School of India Review 112.
u. Balganesh, S., "The Constraint of Legal Doctrine" (2012) 160 University of Pennsylvania Law Review 1843.

E. Government Reports and Policy Documents

v. NITI Aayog, "National Strategy for Artificial Intelligence" (2018). Available at: https://niti.gov.in
w. NITI Aayog, "Responsible AI for All" (2021). Available at: https://niti.gov.in
x. Reserve Bank of India, "Report of the Working Group on Digital Lending" (2021). Available at: https://rbi.org.in
y. MeitY, "India AI Mission Framework" (2024). Available at: https://meity.gov.in
z. Standing Committee on Finance, "Report on Expert Committee on Data Protection Framework for India" (2022).
aa. AI Incident Database, "Incidents Involving India" (Responsible AI Collaborative, 2024). Available at: https://incidentdatabase.ai