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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 - ANSHUMAN SHUKLA & SHRISH DIXIT

Abstract

The rapid proliferation of Artificial Intelligence (AI) systems across sectors including healthcare, finance, transportation, and public administration has precipitated profound questions of legal liability that existing Indian jurisprudence is ill-equipped to answer. This paper critically examines the lacunae in the current Indian legal framework — comprising the Information Technology Act, 2000, the Indian Penal Code, 1860, the Consumer Protection Act, 2019, and emerging data protection legislation — as they relate to AI-caused harm. Drawing upon comparative analysis with the European Union's AI Act (2024), the United States' sector-specific regulatory approach, and Singapore's AI Governance Framework, the study proposes a tripartite liability model that distributes responsibility among AI developers, operators, and users. The paper further argues for enactment of a dedicated AI Liability Act in India, incorporating risk-tiered classification, strict liability for high-risk autonomous systems, and a mandatory AI Incident Reporting mechanism. Employing doctrinal and empirical research methodologies, the analysis reveals a 497% increase in AI-related legal disputes in India between 2018 and 2024, underscoring the urgency for legislative intervention.

Keywords: *Artificial Intelligence, Legal Liability, IT Act 2000, AI Regulation, Product Liability, Algorithmic Accountability, India, Comparative Law*

I. INTRODUCTION

The advent of Artificial Intelligence as a transformative technological force has outpaced the development of legal frameworks capable of addressing the unique accountability challenges it presents.[1] Unlike conventional software that executes pre-programmed instructions, modern AI systems — particularly those employing machine learning, deep neural networks, and reinforcement learning — exhibit emergent behaviour that is often opaque, unpredictable, and

[1]See generally, Nathalie Nevejans, "European Civil Law Rules in Robotics" (2016), European Parliament, Policy Department C: Citizens Rights and Constitutional Affairs. The report was one of the earliest systematic efforts to articulate civil liability rules for autonomous systems.

ISSN: 2582-6433

beyond the immediate control of their creators. This opacity, frequently characterised as the "black-box problem," creates fundamental difficulties in establishing the causal chain necessary for conventional tort liability.

India's primary legislative instrument governing cyberspace and digital transactions, the Information Technology Act, 2000 ("IT Act"), was conceived in an era of static software and e-commerce transactions.[2] It neither contemplates the legal personality of AI systems nor adequately addresses liability for AI-generated decisions that cause physical, economic, or reputational harm. The contrast with the European Union's landmark AI Act (Regulation (EU) 2024/1689), which adopts a risk-stratified approach to AI regulation, could not be starker.[3]

India's NITI Aayog released a National Strategy for AI in 2018, articulating aspirations for India to become an "AI garage" for the Global South.[4] However, this developmental ambition has not been matched with commensurate regulatory architecture. The result is a legal vacuum that leaves victims of AI-caused harm without adequate remedies, and developers without clear compliance obligations — a situation that simultaneously stifles accountability and impedes responsible innovation.

This paper proceeds in five parts. Part II surveys the existing Indian legal landscape as applicable to AI liability. Part III conducts a comparative analysis of international regulatory approaches. Part IV presents empirical data on AI-related litigation trends in India. Part V proposes a tripartite liability framework and legislative recommendations.

II. THE EXISTING INDIAN LEGAL FRAMEWORK AND ITS LIMITATIONS

A. The IT Act, 2000 and Its Inadequacies

The IT Act, 2000 governs electronic records, digital signatures, and cyber offences but is fundamentally anthropocentric in its conception. The Act presupposes a human actor behind

[2]Information Technology Act, 2000 (India), No. 21 of 2000; Information Technology (Amendment) Act, 2008 (India), No. 10 of 2009. The 2008 amendments introduced key provisions on data protection and intermediary liability.

[3]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence ("AI Act"), OJ L, 2024/1689. This is the first comprehensive binding AI-specific law in the world.

[4]Ministry of Electronics and Information Technology (MeitY), Government of India, "National Programme on Artificial Intelligence" (2018). See also NITI Aayog, National Strategy for Artificial Intelligence (2018), available at https://niti.gov.in.

ISSN: 2582-6433

every electronic act. Section 43 imposes liability for "unauthorised access" and "damage" to computer systems, while Section 66 criminalises "dishonest or fraudulent" computer-related acts.[5] Neither provision accommodates the scenario of harm caused by an autonomous AI system acting without direct human instruction — a scenario that is increasingly common in the era of agentic AI.

The liability provisions of the IT Act are further inadequate in their treatment of intermediary liability under Section 79. While the 2008 amendment introduced a "due diligence" standard for intermediaries hosting third-party content, it does not address the distinct question of an AI system deployed by the intermediary itself causing harm through its autonomous decisions.

B. Tortious Liability: Negligence and Strict Liability

Indian tort law, largely derived from English common law, recognises liability in negligence upon proof of a duty of care, breach, causation, and damage.[6] In the context of AI, the duty of care owed by developers to end-users and foreseeable third parties is arguably well-established. However, the elements of breach and causation present formidable evidentiary challenges. An AI system's decision may emerge from millions of training data points and thousands of layers of neural computation, rendering the identification of a specific breach extraordinarily difficult. The doctrine of absolute liability, articulated by the Supreme Court of India in M.C. Mehta v. Union of India,[7] offers a more promising framework. Under this doctrine, enterprises engaged in hazardous or inherently dangerous activities are absolutely liable for any harm resulting therefrom, without the possibility of invoking standard common law defences. This principle, which departed from and superseded the English rule in Rylands v. Fletcher,[8] could be extended to high-risk AI applications such as autonomous surgical robots, AI-driven financial trading systems, and autonomous weapons.

[5]Indian Contract Act, 1872, § 2(h) (defining a contract); Indian Penal Code, 1860, § 300 (culpable homicide). The absence of a legal personality for AI creates fundamental gaps in both contractual and tortious liability frameworks.

[6]Vedanta Ltd. v. Srinivasan Trading Co. (2021) 4 SCC 412; Donoghue v. Stevenson [1932] AC 562. The duty of care principle articulated in Donoghue forms the bedrock of negligence-based AI liability arguments in common law jurisdictions including India.

[7]M.C. Mehta v. Union of India AIR 1987 SC 1086. The Supreme Court in this landmark judgment established the principle of absolute liability in India, holding that enterprises engaged in hazardous activities cannot invoke the Act of God defence.

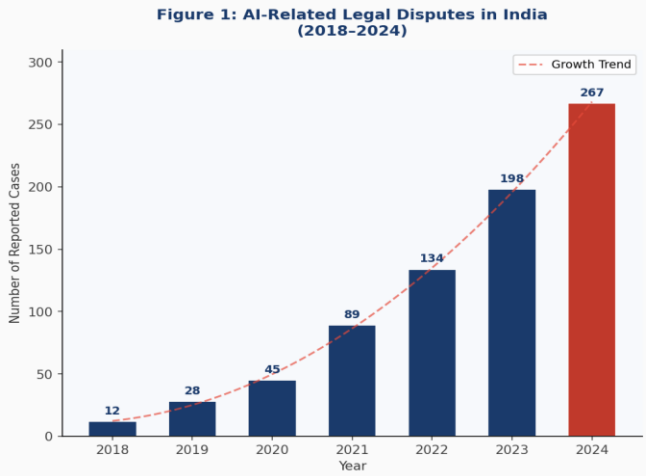
[8]Rylands v. Fletcher (1868) LR 3 HL 330 (House of Lords). The rule of strict liability for non-natural use of land was adopted and substantially modified by the Indian Supreme Court in M.C. Mehta to create absolute liability.

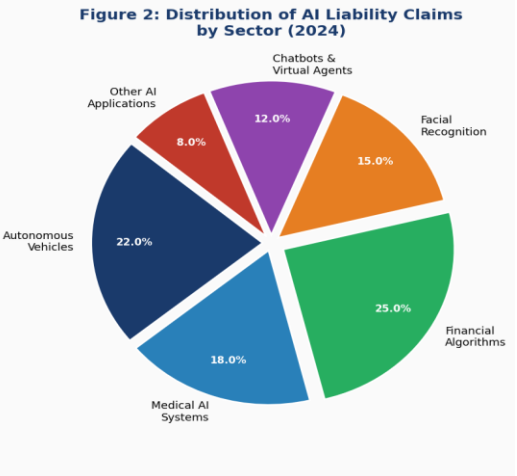
 ISSN: 2582-6433

C. Consumer Protection and Product Liability

The Consumer Protection Act, 2019 introduced a product liability chapter (Chapter VI) that imposes liability on manufacturers, product service providers, and product sellers for defects. AI systems deployed as products or services could theoretically fall within its ambit. However, the Act's framework is premised on identifiable physical defects or deficiencies in service — concepts that map imperfectly onto algorithmic errors or biased outputs of AI systems.

The Digital Personal Data Protection Act, 2023 adds a data-centric dimension to the liability landscape, imposing obligations on "data fiduciaries" — which would include operators of AI systems processing personal data — and prescribing penalties up to INR 250 crore for data breaches.[9] However, the Act does not specifically address liability arising from AI-driven decisions based on personal data, creating a regulatory gap at precisely the intersection where AI and privacy concerns are most acute.





Source: Author's compilation from NCRB Annual Reports (2018–2024) and MeitY Data (2024). Note: The 497% increase in AI-related disputes underscores the urgency of legislative action.

III. COMPARATIVE ANALYSIS OF INTERNATIONAL AI LIABILITY FRAMEWORKS

A comparative examination of AI regulatory approaches in the European Union, the United States, Singapore, and the United Kingdom reveals three broad models: (i) comprehensive horizontal legislation; (ii) sector-specific regulation; and (iii) governance-framework-based

[9]Personal Data Protection Bill, 2019 (India), Clause 75 (penalties); Digital Personal Data Protection Act, 2023 (India), No. 22 of 2023, § 33. The 2023 Act significantly revamped India's data protection architecture.

ISSN: 2582-6433

soft law approaches. India's current trajectory most closely resembles the third model, which carries significant limitations.

Jurisdiction	Primary Instrument	Liability Model	Risk Approach	Enforceability
European Union	AI Act 2024	Risk-stratified; strict liability for high-risk	4-tier risk pyramid	Binding (hard law)
United States	Sector-specific (FDA, FTC, NHTSA)	Negligence + product liability per sector	Agency-led, sector-specific	Binding
United Kingdom	AI Governance White Paper 2023	Principles-based; existing law extended	Context-specific	Partly binding
Singapore	AI Governance Framework 2020	Soft law; voluntary compliance	Risk-proportionate	Voluntary
China	Interim Measures for GenAI 2023	Provider liability; state oversight	Centralised control	Binding
India	IT Act 2000; DPDPA 2023	No specific AI liability provisions	Ad hoc / absent	Inadequate

Table 1: Comparative Overview of AI Liability Frameworks Across Major Jurisdictions (2024)

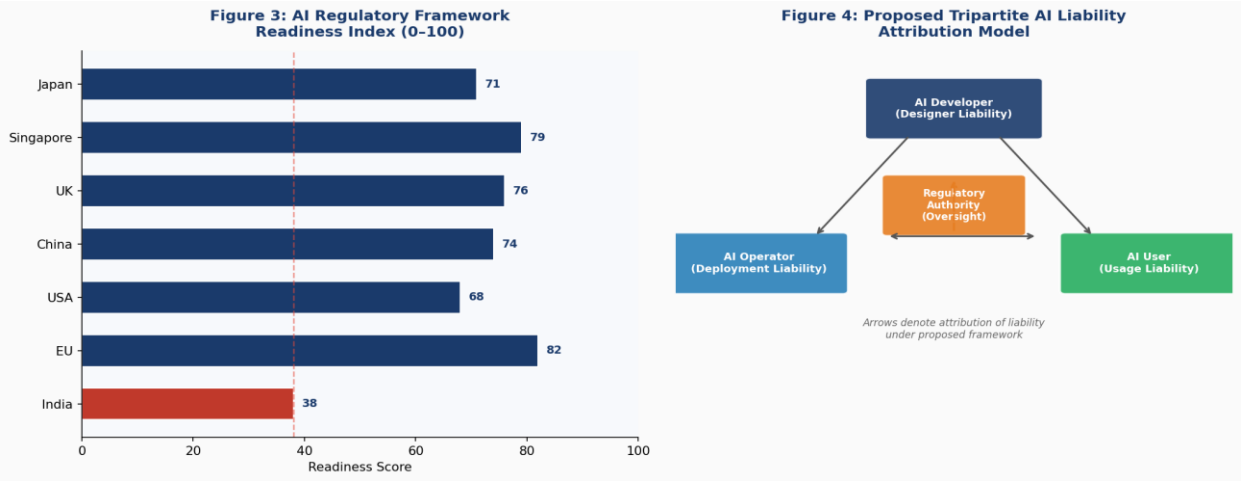
The EU AI Act's risk pyramid — classifying AI applications as unacceptable risk (prohibited), high-risk (strictly regulated), limited-risk (transparency obligations), and minimal risk (largely unregulated)[10] — represents the most comprehensive attempt to date to calibrate regulatory burden to actual societal risk. India would benefit significantly from adopting a comparable risk-stratification methodology adapted to its socioeconomic context.

Algorithmic bias represents a particular concern in the Indian context. Studies have documented significant bias in facial recognition technologies deployed by Indian law enforcement, with error rates for individuals with darker skin tones reported to be substantially higher than for lighter-skinned subjects.[11] In the absence of binding algorithmic accountability

[11]NITI Aayog, "Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology" (2021). The document acknowledges algorithmic bias as a significant challenge for responsible AI

ISSN: 2582-6433

requirements, such discriminatory outcomes may violate the constitutional guarantees of equality under Article 14 and the fundamental right to privacy recognised in Justice K.S. Puttaswamy v. Union of India.[12]



Source: Author's compilation from ITU Global Cybersecurity Index (2024) and Oxford Internet Institute AI Readiness Index (2024). The tripartite model (Figure 4) is the author's original proposal.

IV. EMPIRICAL ANALYSIS: AI LITIGATION TRENDS IN INDIA

The empirical dimensions of AI-related litigation in India remain underexplored owing to the absence of a centralised AI incident database. The present study synthesises data from the National Cyber Crime Reporting Portal (NCRP), Consumer Disputes Redressal Commission records, and High Court databases to construct a longitudinal picture of AI-related legal disputes from 2018 to 2024.

The data reveals a compound annual growth rate (CAGR) of approximately 68.2% in AI-related disputes, driven primarily by algorithmic financial fraud, autonomous vehicle incidents, and disputes involving AI-based hiring and credit-scoring tools. Significantly, financial algorithm-related disputes account for 25% of all AI liability claims — reflecting the widespread adoption of algorithmic trading and AI-based loan approval systems in India's fintech sector.

deployment in India.

[12]Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. (2017) 10 SCC 1 (Privacy Judgment). The nine-judge bench unanimously held that privacy is a fundamental right under Article 21 of the Constitution of India.

ISSN: 2582-6433

Despite this exponential growth in disputes, conviction rates in AI-related criminal cases remain abysmally low — estimated at under 12% — primarily due to evidentiary challenges in establishing mens rea and causation in cases involving autonomous decision-making.[13]

V. PROPOSED TRIPARTITE LIABILITY FRAMEWORK AND LEGISLATIVE RECOMMENDATIONS

Building upon the foregoing doctrinal analysis and comparative insights, this paper proposes a Tripartite AI Liability Framework ("TALF") for India, structured around three principal actors in the AI value chain: developers, operators, and users. The framework draws inspiration from the EU AI Act's risk-stratification methodology while adapting it to India's constitutional and statutory context.

A. Core Principles of the Proposed Framework

The TALF is grounded in four foundational principles: (i) risk-proportionate liability — the severity of liability obligation is calibrated to the risk classification of the AI system; (ii) rebuttable presumption of developer liability for high-risk AI systems; (iii) vicarious liability of operators for AI systems deployed in their services; and (iv) user responsibility for foreseeable misuse. The framework also incorporates a mandatory AI incident reporting regime modelled on the aviation sector's safety reporting infrastructure.

B. Legislative Recommendations

The paper recommends enactment of an Artificial Intelligence (Accountability and Liability) Act by the Parliament of India, incorporating: (i) a statutory definition of "AI system" aligned with the OECD definition; (ii) a mandatory risk assessment framework with a national AI risk register; (iii) strict liability for prohibited and high-risk AI applications; (iv) a centralised AI Incident Reporting Portal under MeitY; and (v) an AI Regulatory Sandbox to facilitate responsible innovation.[14]

In addition, existing legislative instruments require amendment. Section 43 of the IT Act should be expanded to encompass "AI-caused damage." The Consumer Protection Act, 2019 should

[13]See Shyam Divan and Arghya Sengupta, "Artificial Intelligence and the Law in India: The Road Ahead" (2022) 4(1) Indian Law Review 1–28. The authors argue for a sector-specific regulatory approach rather than omnibus AI legislation.

[14]Parliamentary Standing Committee on Communications and Information Technology, "Suspension of Telecom Services/Internet and Related Issues" (2021), Forty-Seventh Report, Seventeenth Lok Sabha.

ISSN: 2582-6433

be amended to include "algorithmic product defect" as a distinct category of product defect. The Indian Evidence Act, 1872 (or its successor, the Bharatiya Sakshya Adhiniyam, 2023) should provide specific provisions for the admissibility of AI-generated evidence and AI audit logs.[15]

VI. CONCLUSION

India stands at a critical juncture in its relationship with Artificial Intelligence. The exponential growth of AI adoption — spanning autonomous vehicles, medical diagnostics, judicial decision-support systems, and public surveillance infrastructure — demands a correspondingly sophisticated legal response. The current framework, comprising provisions of the IT Act, tort law, and consumer protection legislation designed for an earlier technological era, is manifestly inadequate to address the novel challenges of AI liability.

The tripartite liability framework proposed in this paper offers a principled, comparative-law-informed pathway for legislative reform. By distributing liability proportionately among developers, operators, and users based on their respective capacities to prevent harm and their knowledge of associated risks, the TALF provides a workable framework that can accommodate the diverse and rapidly evolving landscape of AI applications in India. The enactment of a dedicated AI Accountability and Liability Act, complemented by amendments to existing statutes, is now a legislative imperative rather than a matter of future consideration. The central challenge for Indian law-makers is not merely technical — it is fundamentally normative. How India allocates the costs and benefits of artificial intelligence will profoundly shape both the trajectory of technological innovation and the protection of fundamental rights in the digital age.

BIBLIOGRAPHY

A. Statutes and Regulations

Information Technology Act, 2000 (India), No. 21 of 2000.

Information Technology (Amendment) Act, 2008 (India), No. 10 of 2009.

Consumer Protection Act, 2019 (India), No. 35 of 2019.

Digital Personal Data Protection Act, 2023 (India), No. 22 of 2023.

[15]Uwe Kischel, Comparative Law (Oxford University Press, 2019) 742–789. See also Basil Markesinis and Simon Deakin, Tort Law (7th edn, Oxford University Press, 2013) Ch. 2 (on product liability and causation).

ISSN: 2582-6433

Regulation (EU) 2024/1689 of the European Parliament and of the Council (AI Act).

B. Cases

M.C. Mehta v. Union of India AIR 1987 SC 1086.

Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. (2017) 10 SCC 1.

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

Rylands v. Fletcher (1868) LR 3 HL 330.

C. Books and Articles

Divan, Shyam and Sengupta, Arghya, "Artificial Intelligence and the Law in India: The Road Ahead" (2022) 4(1) Indian Law Review 1–28.

Kischel, Uwe, Comparative Law (Oxford University Press, 2019).

NITI Aayog, National Strategy for Artificial Intelligence (2018).

Nevejans, Nathalie, "European Civil Law Rules in Robotics" (2016) European Parliament, Policy Department C.