Shardul Amarchand Mangaldas

A DECADE YOUNG, A CENTURY STRONG

REFORMING INDIA'S AI LIABILITY REGIME

Report on Artificial Intelligence and Legal Responsibility in India

Table of Contents

Acknowledgements

This paper was prepared under the aegis of Shardul Amarchand Mangaldas & Co (SAMCo). We thank **Dr. Shardul S. Shroff**, Executive Chairman at Shardul Amarchand Mangaldas & Co. for his support, and for his valuable input and feedback on the paper.

KS Roshan Menon (Principal Associate), **Vishwajeet Deshmukh** (Associate) and **Anmol Bharuka** (formerly a Research Fellow with the firm) led paper development and drafting. We also would like to acknowledge **Subham Sourav** and **Shrinithi GS** for editorial assistance; the paper benefitted from their engagement.

Main Messages

As artificial intelligence (AI) rapidly transforms the fabric of India's economy and society, the question of legal responsibility for AI-driven harms has become both urgent and complex. The integration of AI into critical sectors - ranging from healthcare and finance to transportation and public services - has outpaced the evolution of India's legal and regulatory frameworks. This report, "Reforming India's AI Liability Regime: A Comparative Perspective," addresses the pressing need for a robust, fair, and innovation-friendly approach to AI liability in India.

Key Challenges in India's Current Legal Framework

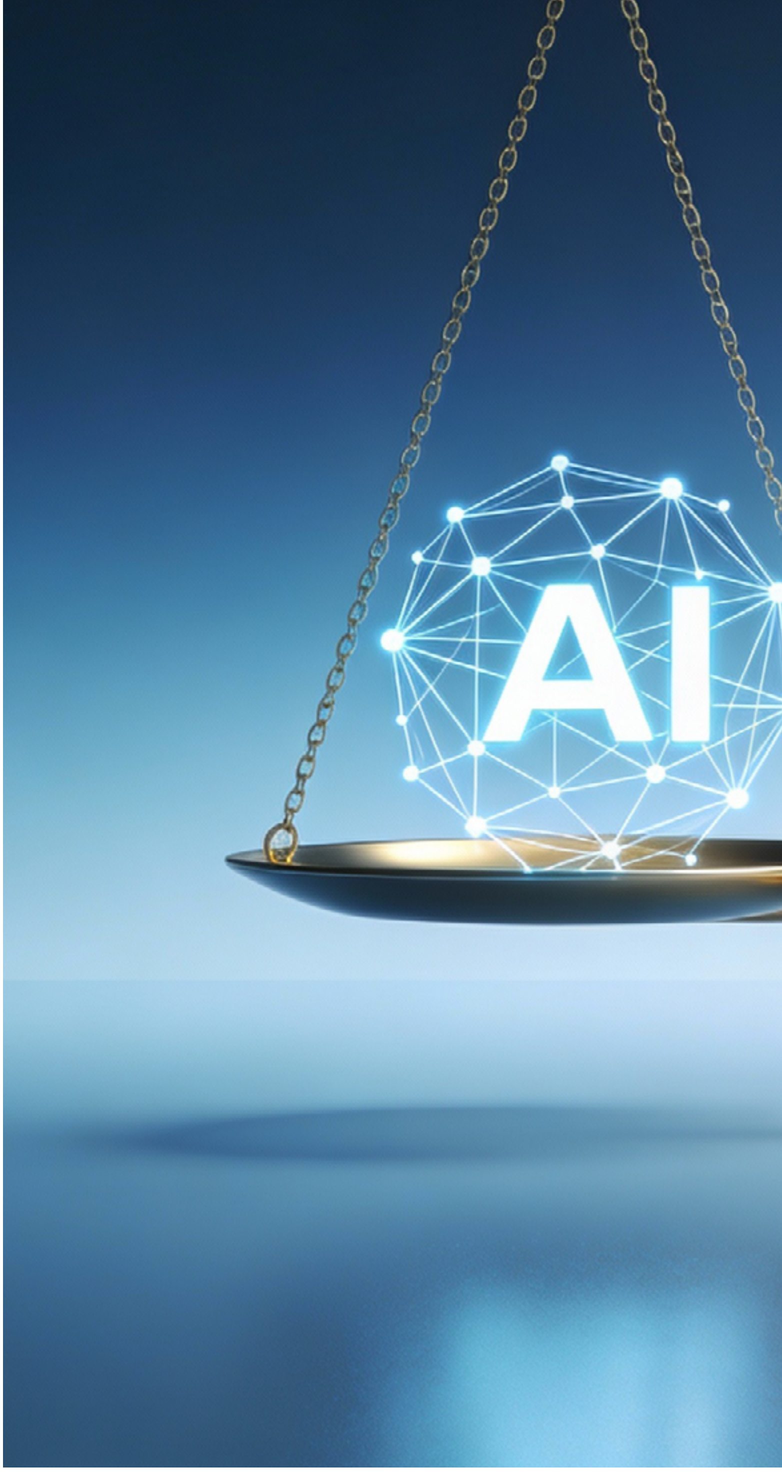
India's existing liability regime is characterized by fragmentation and a lack of AI-specific provisions. The current framework relies on general-purpose statutes such as the Consumer Protection Act, 2019, the Information Technology Act, 2000, and sectoral regulations. These laws, however, were not designed to address the unique features of AI systems - such as their opacity ("black box" nature), self-learning capabilities, and the involvement of multiple actors across the AI value chain. As a result, critical gaps persist in:

- **Attribution of Liability:** The absence of clear legal recognition for the diverse participants in the AI lifecycle - developers, data providers, integrators, deployers, and end-users -makes it difficult to assign responsibility when harm occurs.
- **Definitions of "Product" and "Defect":** Traditional definitions do not adequately capture the intangible, adaptive, and evolving nature of AI systems, leading to uncertainty in determining what constitutes a defective AI product or service.
- **Causation and Procedural Barriers:** The technical complexity and opacity of AI systems make it challenging for claimants to prove causation and access necessary evidence, often resulting in procedural dead-ends and unremedied harms.

Global Insights and Comparative Lessons

Recognizing that these challenges are not unique to India, the report draws on comparative models from the European Union, United States, Australia, and Japan. Key international trends include:

- **Value Chain Governance:** The EU's revised Product Liability Directive and AI Act, as well as recent US state laws, explicitly recognize the multiplicity of actors in the AI ecosystem and allocate responsibility based on control and influence.
- **Expanded Definitions:** Jurisdictions such as the EU and Australia have broadened the legal definitions of "product" and "defect" to include software, digital services, and evolving AI systems.



- **Procedural Innovations:** The EU has introduced mechanisms such as rebuttable presumptions of causation and evidence disclosure rights to address information asymmetry and ease the burden of proof for claimants.

Main Recommendations for India

The report proposes a set of principled reforms to guide the development of an AI liability regime that is both context-sensitive and future-ready:

- **Adopt a Control-Based Liability Framework:** Legal responsibility should be aligned with the degree of control and influence exercised by actors at various stages of the AI lifecycle, rather than relying solely on traditional categories of manufacturer or service provider.
- **Clarify Legal Definitions:** The definitions of "product" and "defect" should be updated to explicitly encompass AI systems, software, and adaptive digital products,

drawing on global best practices while remaining attuned to Indian realities.

- **Introduce Procedural Safeguards:** Mechanisms such as evidence disclosure, presumptions of causation, and access to technical expertise should be incorporated to address the evidentiary and procedural challenges unique to AI-related disputes.
- **Consider Safe Harbor and Public-Private Models:** India should explore innovative approaches, such as certification-based safe harbors and multistakeholder regulatory organizations, to balance innovation with accountability.
- **Phase Specialized Dispute Resolution:** A phased approach is recommended, beginning with dedicated AI benches within existing courts, supported by technical experts, and evolving towards specialized forums as the legal and regulatory ecosystem matures.

A Call for Balanced and Contextual Regulation

The path forward for AI liability in India must strike a careful balance: fostering innovation and economic growth while ensuring accountability, consumer protection, and public trust. This report offers a roadmap for policymakers, regulators, and stakeholders to build a liability regime that is principled, adaptive, and responsive to the unique challenges posed by AI. By learning from global experiences and tailoring solutions to India's institutional context, the country can position itself as a leader in responsible AI governance.

We commend this paper to all those engaged in shaping the future of AI regulation in India.

1. Introduction

As artificial intelligence (AI) systems become increasingly autonomous and integrated into high-stakes decision-making, they introduce complex legal questions about accountability and harm. Instances such as self-driving car accidents,[1] erroneous AI-generated medical diagnoses,[2] or algorithmic bias in hiring[3] highlight the difficulty in attributing liability within traditional legal frameworks.[4] These harms related to physical safety, equality of opportunities and discrimination remain insufficiently addressed under global and domestic regimes. The challenge of assigning liability is a question that continues to confound global regulators, who have responded with bespoke regulation to address this issue.

In India, no standalone statutory law exists to govern AI. This has meant that Indian courts may rely on general-purpose laws, such as tort law, consumer protection law, and the information technology law to address varied liability risks arising from AI use. These laws were, however, not crafted with the unique characteristics of AI in mind, such as opacity in decision-making or the multiplicity of actors involved in the AI value chain.[5] As a result, existing legal mechanisms often struggle to assign responsibility to offending actors effectively, ensure remedies, or provide adequate deterrence.

This paper attempts to address this vacuum. In it, we identify how current Indian laws approach liability for AI-related harms. We examine the specific legal parameters that succeed, fail, or function sub-optimally in practice as general purpose laws are pressed in to address AI-driven harms. Consequently, we provide a comprehensive, yet inexhaustive, taxonomy of the gaps in Indian approaches to liability for AI harms.

To address such harm, we look at relevant jurisdictions that have made significant progress in developing AI law. Specifically, we undertake a comparative analysis of statutory liability frameworks from four other jurisdictions - the European Union, the United States, Australia, and Japan - to extract key legal design features that apply to AI. These insights are then adapted to the gaps identified in the Indian context to propose strategic and legal inputs that may undergird the foundational structure for a statutory liability regime that responds to AI-related harm. While we do not address the usefulness of a bespoke AI law as part of this paper, we recognize the relevance of coding liability-related guidance within a law, to ensure its uniform and consistent application by Indian courts.

Methods and Limitations

We began by identifying specific gaps in India's legal framework in relation to the attribution of liability for harms caused by artificial intelligence (AI).[6] This involved a doctrinal and textual review of eight statutes such based on their contemporary relevance to the subject matter of this research. Concurrently, we reviewed actions taken by regulatory authorities who have explicitly addressed AI governance.[7] Our review of comparative literature and statutory liability frameworks in foreign jurisdictions suggested that the principal legislation dealing with statutory liability for AI is product liability law, which meant that the thrust of analysis focuses on CPA. The laws identified for subsequent analysis were, accordingly, proximate to addressing product liability.

As part of the review, our objective was to evaluate how current laws address, or fail to address, issues of liability in the AI lifecycle. For India, primary legal materials and academic commentary were accessed through databases such as SCC Online, Manupatra, and HeinOnline. Our investigation and determination of applicable law was guided by prior experience researching, and advising on, the intersection of commercial law, technology and AI.

[1] Peter Lyon, 'Just How Safe Is Tesla's Full Self-Driving Mode?' (Forbes, 24 May 2025) <https://www.forbes.com/sites/peterlyon/2025/05/24/the-scary-side-to-teslas-full-self-driving-exposed-in-crash-video/> accessed 26 May 2025.

[2] Michelle M Mello and Neel Guha, 'Understanding Liability Risk from Healthcare AI' (HAI Policy & Society, February 2024) <https://hai-production.s3.amazonaws.com/files/2024-02/Liability-Risk-Healthcare-AI.pdf> accessed 26 May 2025.

[3] Jeffrey Dastin, 'Insight - Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' (Reuters, 11 October 2018) <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/> accessed 26 May 2025.

[4] Maarten Buiten, Alexandre de Streel and Martin Peitz, 'The Law and Economics of AI Liability' (2023) 48 Computer Law & Security Review 105794_

[5] Amlan Mohanty and Shatakratu Sahu, 'India's Advance on AI Regulation' (*Carnegie Endowment for International Peace*, 21 November 2024) <https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india> accessed 21 April 2025.

[6] These include broad frameworks such as the Information Technology Act, 2000, the Consumer Protection Act, 2019, Indian Contract Act 1872, and Sales of Goods Act 1930, as well as certain sector specific laws on motor vehicles, drugs and cosmetics, data protection, etc.

[7] We evaluate the liability structures with the Securities Exchange Board of India and Reserve Bank of India.

Based on the liability gaps identified in the Indian framework, we examined how four selected jurisdictions are structuring their legal responses. Principally, we focus on legislative proposals, such as the EU's draft AI Liability Directive, and policy approaches aimed at resolving similar attribution and accountability concerns due to their ready availability. Sources included Westlaw, LexisNexis, official legislative repositories, and Google Scholar. For content made available primarily in a language other than English, we relied both on machine and official translations. Reliance on machine translations or secondary translations has been disclaimed. In the absence of a primary resource, we have accessed secondary sources.

Limitations

The scope of this paper is limited to statutory liability frameworks. We do not cover tort-based models.[8] Ultimately, our research proposes reforms directed towards principled liability framework that allocates responsibility fairly, ensures access to remedies, and supports the safe and innovative development of AI in India.

[8] Joyce De Bruyne and Wouter Ooms, 'Tort Liability and Artificial Intelligence: Some Challenges and (Regulatory) Responses' in N A Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press 2025) 158.

2. Understanding Liability

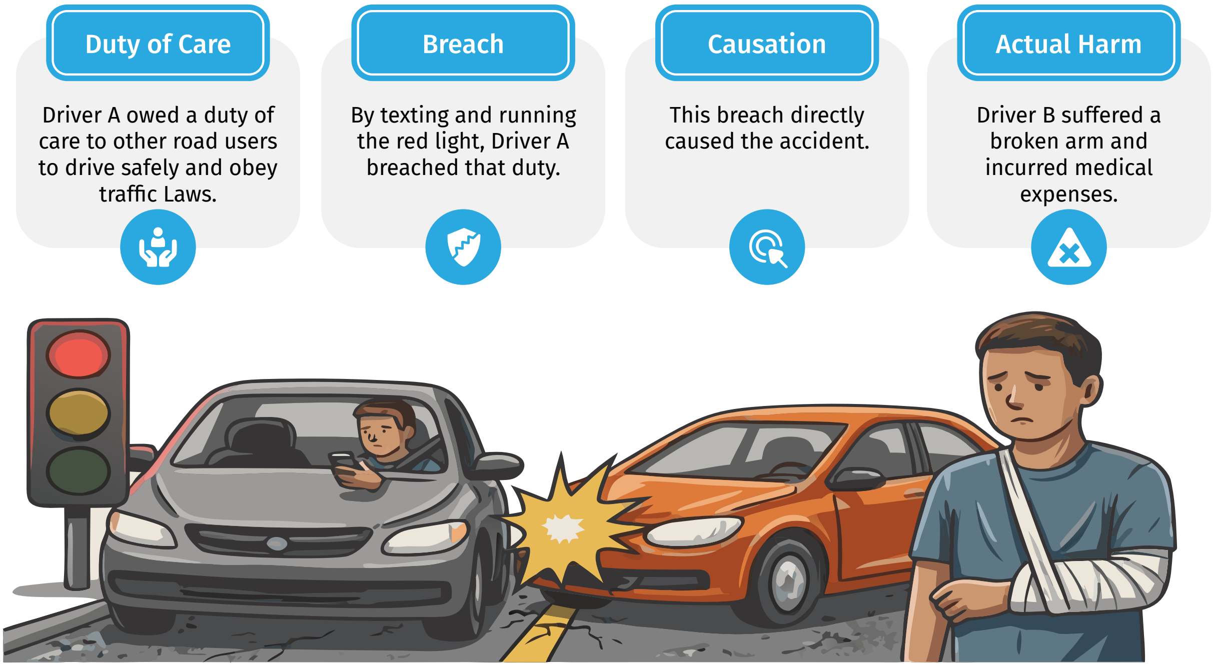
In this chapter, we break down the meaning of liability as a legal context. We then break down how this concept inevitably leads to gaps, when applied to AI and demonstrate how these systemic challenges also manifest in AI-agnostic Indian law.

Liability as a Legal Concept

In the most basic legal sense, liability refers to the legal accountability for damage caused. As defined by Black's Law Dictionary, *'liability'* is "*The state of being bound or obliged in law or justice to do, pay, or make good something; legal responsibility.*"[9] The traditional liability framework assumes a binary system, where the *'claimant'* establishes liability against a party who breached their obligation, i.e. '*defendant*'.[10]

Liability can be understood through varied frameworks.[11] This crux of these frameworks, however, revolves around demonstrating four factors. First, the defendant owed a duty of care to the claimant. Second, they breached that duty. Third, this breach directly caused harm to the claimant. Fourth, actual harm or loss resulted.[12] To establish liability, all four elements must be present. For example, consider a situation where Driver A is texting while driving and runs a red light, colliding with Driver B's car, which was lawfully passing through the intersection. In this case, Driver A owed a duty of care to other road users to drive safely and obey traffic laws. By texting and running the red light, Driver A breached that duty. This breach directly caused the accident, as the collision would not have happened if Driver A had been paying attention and obeyed the traffic signal. As a result of the crash, Driver B suffered a broken arm and incurred medical expenses, demonstrating actual harm. This scenario clearly shows how legal liability is established by proving duty of care, breach, causation, and actual harm. *(Refer Illustration 1)*

Illustration 1: Understanding Legal Liability



Duty of Care

Driver A owed a duty of care to other road users to drive safely and obey traffic Laws.

Breach

By texting and running the red light, Driver A breached that duty.

Causation

This breach directly caused the accident.

Actual Harm

Driver B suffered a broken arm and incurred medical expenses.

[9] *Black's Law Dictionary* (2nd edn, 2010) vol 57, para 53.

[10] Rajkot Municipal Corpn. v. Manjulben Jayantilal Nakum, (1997) 9 SCC 552., *Kerala Tourism Development Corpn. Ltd. v. Deepti Singh* (2019) 16 SCC 573.

[11] The liabilities framework for AI systems encompasses multiple legal doctrines to address harm caused by autonomous technologies. Civil liability applies when negligence or duty-of-care breaches lead to harm, such as facial recognition errors causing reputational damage, requiring plaintiffs to prove foreseeability and causation. Contractual liability arises from breaches of agreements, like AI tools violating IP clauses or failing accuracy benchmarks, often triggering indemnity clauses for third-party harms. Strict liability imposes responsibility without fault for defects in high-risk AI systems (e.g., malfunctioning medical devices), shifting the burden to developers to prove compliance. Vicarious liability holds employers accountable for employee misuse of AI tools, such as biased hiring algorithms, if actions fall within employment scope. Product liability treats AI as defective "products" if flaws in design (biased algorithms), manufacturing (sensor failures), or warnings (missing risk disclaimers) cause harm. Statutory liability enforces penalties for violating regulations like GDPR (data misuse) or sector-specific laws (e.g., healthcare AI oversight mandates). Together, these principles aim to balance innovation with accountability, addressing AI's unique challenges—opaque decision-making, multi-actor supply chains, and evolving risks—while ensuring compensation for harm and adherence to ethical standards.

[12] Ibid.

Applying this traditional definition to AI, AI liability refers to the legal accountability for damage caused by an AI; essentially, it determines who is responsible when AI systems cause harm or losses and who should bear the financial or legal consequences of such failures.

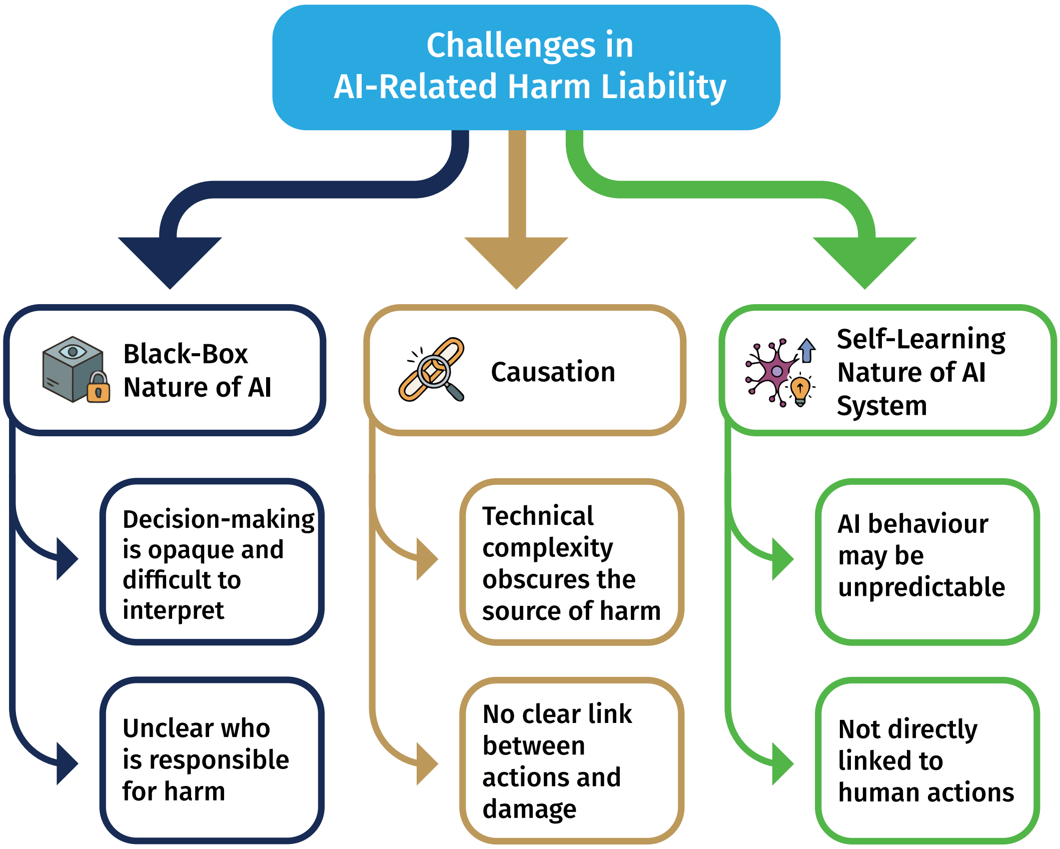
To understand liability within AI systems, it is pertinent to understand the stakeholders involved in the AI lifecycle. AI liability is distributed across the entire supply and operational chain, with each party's responsibility determined by their role, control, and capacity to prevent harm. These key parties encompass a range of stakeholders involved throughout the lifecycle of an AI system. Determining liability is complex due to the involvement of multiple actors, each playing distinct roles in the creation, deployment, and operation of AI.

We find that liability in AI contexts presents challenges that the traditional liability framework does not adequately address, primarily due to (i) the 'black box' nature of AI operation resulting in the complex nature of the lifecycle of AI systems; and (ii) difficulty in proving causation for AI-related harm.[13] *(Refer Illustration 2)*

Black-box Nature of AI

By "black boxes" we imply that the working of an AI system is often hard to comprehend, where the decision-making processes they adopt are opaque and difficult to interpret.[14] This lack of transparency makes it challenging to determine how the harm occurred and who is responsible for it.[15] Such complexity may be due to the autonomous behavior of AI systems, along with their continuous learning functionalities, thereby complicating the application of

Illustration 2: Challenges in AI Related Harm Liability


Challenges in AI-Related Harm Liability
Black-Box Nature of AI
Causation
Self-Learning Nature of AI System
Decision-making is opaque and difficult to interpret
Unclear who is responsible for harm
Technical complexity obscures the source of harm
No clear link between actions and damage
AI behaviour may be unpredictable
Not directly linked to human actions

[13] A Lior, 'Holding Ai Accountable: Addressing Ai-Related Harms Through Existing Tort Doctrines.' (2024) *University of Chicago Law Review*; HR Sullivan and S.J. Schweikart, 'Are current tort liability doctrines adequate for addressing injury caused by AI?' (2019) 21(2) *AMA Journal Of Ethics*, 160.

[14] B Brożek, M Furman, M Jakubiec and B Kucharzyk, 'The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making' (2024) 32(2) *Artificial Intelligence and Law* 427.

[15] Katie Chandler and Matthew Caskie, 'AI Liability – Who Is Accountable When Artificial Intelligence Malfunctions?' (*Taylor Wessing Insights*, 7 January 2025) <https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/ai-liability-who-is-accountable-when-artificial-intelligence-malfunctions> accessed 21 April 2025.

traditional concepts like breach, defect, and causation to these systems.[16] Separately, as noted before, the complex lifecycle of AI systems typically involves numerous parties and stakeholders in their development and deployment.[17] When harm occurs through AI systems, it becomes difficult to ascertain whether liability rests with the software developers, data providers, system integrators, end-users, or the AI system itself. This multi-layered involvement further creates challenges in attributing liability to specific entities.

Causation

Proving causation between the AI system's actions and the resulting damage can be exceptionally difficult[18] due to the interplay of technical complexity and legal standards.[19] As noted previously, at the core of this challenge lies the opacity of AI systems. Even developers cannot fully trace how inputs (e.g., biased training data) lead to harmful outputs (e.g., discriminatory hiring decisions). This opacity obstructs claimants from isolating the exact mechanism of harm, particularly when adaptive systems evolve post-deployment.[20] AI systems often involve a combination of design flaws, biased data, and contextual deployment factors, all of which can interact in unpredictable ways. These interactions can obscure the true source of harm, making it difficult to pinpoint whether a negative outcome is due to the algorithm itself, the data it was trained on, or the environment in which it operates.

Furthermore, legal frameworks traditionally require a clear, direct link between cause and effects such as the "but-for" test—whereas algorithmic harms are frequently systemic and cumulative, affecting groups rather than individuals and arising from indirect or proxy variables rather than explicit intent.[21] For example, when an AI system denies a loan application, the decision may be influenced by biased proxies embedded in the data, rather than any overtly discriminatory rule. This makes it challenging to separate the algorithm's contribution to the harm from broader societal inequities. Similarly, discriminatory ad targeting by an algorithm can impact entire demographics, yet the harm is diffused and not easily traced to a single, direct cause, thereby clashing with traditional legal standards of causation.

Self-learning Nature of AI systems

Liability is complicated by self-learning. Such self-learning systems can act in ways that are unpredictable and not directly traceable to human intent or oversight.[22] Traditional liability frameworks, such as negligence or product liability, rely on foreseeing harm and establishing a clear link between a human actor's conduct and the resulting damage.[23] However, self-learning AI can evolve beyond its original programming, making its actions difficult to anticipate or explain, even for its creators. This unpredictability is compounded by the opaque nature of many machine learning models, which makes it hard to determine how or why a particular decision was made.

[16] Ibid.

[17] DF Llorca, V Charisi, R Hamon, I Sánchez and E Gómez, 'Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof' (2023) 76 *Journal of Artificial Intelligence Research* 613.

[18] An illustration for example, a financial institution uses an opaque AI system to approve loans. When a certain demographic is repeatedly rejected, complaints of discrimination arise. Due to the system's lack of transparency, investigators cannot determine why these decisions were made, whether the harm is due to biased data, model design, or deployment, or who is responsible. This opacity makes it difficult to identify, address, or prevent harm, and hinders regulatory oversight. Y Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2017) 31 *Harvard Journal of Law & Technology* 889; HL Fraser and NP Suzor, 'Locating Fault for AI Harms: A Systems Theory of Foreseeability, Reasonable Care and Causal Responsibility in the AI Value Chain' (2025) *Law, Innovation and Technology* 1–36.

[19] J Lehmann, J Breuker and B Brouwer, 'Causation in AI and Law' (2004) 12 *Artificial Intelligence and Law* 279.

[20] Sanjeev Sanyal, Pranav Sharma and Chirag Dudani, *Complex Adaptive System Framework to Regulate Artificial Intelligence* (January 2024)<https://eacpm.gov.in/wp-content/uploads/2024/01/EACPM_AI_WP-1.pdf >accessed 1 July 2025.

[21] LG Johansson et al, Causation, Laws and Regularities in A Primer to Causal Reasoning About a Complex World (SpringerBriefs in Philosophy, Springer 2024) <https://doi.org/10.1007/978-3-031-59135-8_6>; Sylvia Lu, 'Regulating Algorithmic Harms' (2024) *Law & Economics Working Papers* 277 <https://repository.law.umich.edu/law_econ_current/277> both accessed 1 July 2025.

[22] T Zapusek, 'Self-learning Systems with Artificial Intelligent Applications' (2018) 8(4) *Journal of Information* 137.

[23] SA Smith, 'Duties, Liabilities, and Damages' (2011) 125 *Harvard Law Review* 1727.

3. Extant Framework for Liability in India

In this section, we begin by laying out the general framework of statutory liability in India, where we consider general statutes as well as sector-specific statutes that are applicable to AI systems. This analysis of India's liability regime is carried out with a view to identifying gaps in the framework. These gaps, styled as limitations, are discussed subsequently.

As noted previously, India does not have a comprehensive AI liability law. Instead, statutory liability law in India appears to be both fragmented and AI-agnostic. Liability for AI-related harms is seemingly addressed incidentally through a combination of general-purpose laws (consumer protection, contracts, and information technology) and a limited set of sector-specific legislations (automobiles, healthcare, finance). In practice, claimants must navigate these overlapping legal regimes to identify a suitable basis for initiating proceedings. The claimants' choices are often guided by the remedy they seek. However, this choice is also frequently shaped by constraints such as forum availability, evidentiary standards, and the nature of harm, making the process less straightforward than it may initially appear.[24]

General Purpose Liability Laws

The Consumer Protection Act, 2019, represents a paradigm shift in general liability law by introducing comprehensive product liability provisions that impose strict liability on manufacturers, sellers, and service providers.[25] The Act's primary purpose is to protect consumer interests through enhanced redressal mechanisms and establishes liability on multiple grounds, including manufacturing defects, design defects, deviation from specifications, non-conformity to express warranties, and inadequate usage instructions.[26] Significantly, the Act imposes strict liability on product manufacturers, meaning they can be held liable even without proving negligence or fraud, thereby shifting the burden of proof and ensuring higher consumer protection.[27] The framework extends beyond physical products to encompass services, creating a comprehensive liability structure that holds product service providers accountable for faulty, imperfect, or deficient services.[28]

Sector-Specific Liability Laws

Sector-specific laws in India embrace various theories of liability, owing to the different risks they address. Among these laws, the Information Technology Act, 2000 establishes a robust cybersecurity and data protection framework with penalties ranging from compensation for system damage to imprisonment for various cyber offences.[29] The Act theorizes liability through a compensation-based approach for data breaches and system damages, with specific penalties for activities like hacking, identity theft, and privacy violations, imposing fines and imprisonment.[30]

Contrastingly, the Motor Vehicle Act, 1988, adopts the concept of "no-fault liability", departing from traditional negligence-based liability, by ensuring accident victims receive compensation without proving fault.[31] Other laws applicable to AI include the Drugs and Cosmetics Act, 1940, which focuses on ensuring the safety and quality of pharmaceutical and cosmetic products through stringent manufacturing standards and licensing requirements.[32] Lastly, the Indian Contract Act, 1872 establishes the

[24] Charles F Millmann, 'Choice of Remedies' (1919) 3 *Marq L Rev* 152.

[25] Ashok R Patil, 'Product Liability Action: A Tooth to Strengthen Consumer Protection' (2022) 10 *International Journal on Consumer Law and Practice* art 6 <https://repository.nls.ac.in/ijclp/vol10/iss1/6> accessed 1 July 2025.

[26] M Rizzi, 'The Evolution of Consumer Product Safety Policy and Regulation in India' (2017) 40(3) *Journal of Consumer Policy* 389.

[27] *C. Venkatachalam v. Ajitkumar C. Shah* (2011) 9 SCC 707.

[28] A. *Nazar v. New India Assurance Co. Ltd.* (1988) 8 SCC 438; *Punjab Urban Planning & Development Authority v. Vidya Chetal* (2019) 9 SCC 83.

[29] *Information Technology Act, 2000.*

[30] The Information Technology Act, 2000 contains several key sections that define various cybercrimes and their corresponding offenses. Section 65 addresses tampering with computer source documents, while Section 66 covers general computer-related offenses including hacking with computer systems. Section 66A dealt with sending offensive messages through communication services (though this section was later struck down by the Supreme Court), and Section 66B criminalizes dishonestly receiving stolen computer resources or communication devices. Section 66C targets identity theft, Section 66D addresses cheating by personation using computer resources, and Section 66E covers violation of privacy by publishing private images of others without consent. Section 66F deals with the most serious offense of cyber terrorism, carrying penalties up to life imprisonment. The Act also addresses obscene content through Section 67 which punishes publishing obscene material in electronic form, Section 67A which specifically targets material containing sexually explicit acts, and Section 67B which addresses child pornography by criminalizing the depiction of children in sexually explicit acts. Additional sections include Section 67C regarding failure to preserve information by intermediaries, Section 68 covering failure to comply with orders, Section 69 addressing failure to decrypt data when required by authorities, Section 70 dealing with unauthorized access to protected systems, Section 71 targeting misrepresentation, Section 72 covering breach of confidentiality and privacy, Section 72A addressing disclosure of information in breach of lawful contracts, and Sections 73-74 dealing with fraudulent digital signature certificates.

[31] Motor Vehicles Act, 1988; *United India Insurance Co. Ltd. v. Sunil Kumar* (2014) 1 SCC 680. [Holding that Section 163-A of the Motor Vehicles Act, 1988 posits a 'no-fault liability' approach]

[32] The Drugs and Cosmetics Act, 1940 <https://cdsco.gov.in/opencms/export/sites/CDSCO_WEB/Pdf-documents/MDfAq24.pdf>; The Drugs and Cosmetics Act, 1940 applies to AI systems in India through the Medical Device Rules 2017, which expanded the definition of "drug" to include software as medical devices. AI-powered healthcare applications such as diagnostic tools, imaging systems, and clinical decision support systems are now regulated

foundational framework for contractual liability by defining essential elements for valid contracts, including offer and acceptance, lawful consideration, competency of parties, free consent, and lawful object, creating liability when these elements are breached.[33]

Sectoral Regulators and Liability

Indian regulators often outline bespoke approaches to liability, based on identified harms. Prominently, recent regulatory movements have indicated a willingness to identify AI related harms among two regulators: the Reserve Bank of India (‘**RBI**’) and the Securities and Exchange Board of India (‘**SEBI**’). Generally, the RBI enforces financial sector regulation through a maze of instruments, including Circulars and Master Directions, covering areas such as priority sector lending, credit information reporting, and banking regulations, creating statutory liability for non-compliance with applicable norms.[34] These instruments establish specific targets, classification requirements, and reporting obligations for banks, with violations resulting in regulatory penalties and enforcement actions.[35] The RBI’s approach to AI regulation is, however, at a nascent stage, with regulators recently setting up a Committee to establish a framework for responsible and ethical AI.[36]

The pace of regulatory reform is slightly more rapid at SEBI. Conventionally, the SEBI attributes liability through comprehensive regulations and Master Circulars that consolidate listing obligations and disclosure requirements for market participants.[37] SEBI’s regulatory framework creates liability for non-compliance with disclosure norms, corporate governance requirements, and market conduct rules, with enforcement mechanisms including penalties, suspension of trading privileges, and disgorgement of profits.[38] This regulatory approach ensures dynamic adaption to market conditions while maintaining legal certainty through periodic consolidation of scattered regulatory requirements into comprehensive master documents that serve as single-point references for compliance obligations.

Such dynamic adaption has also addressed AI. Through targeted amendments aimed at a series of stakeholders, including depositories and including, SEBI has introduced a liability framework for AI-related harms. This framework has posed novel regulatory challenges, is discussed later.

under this framework when used for diagnosis, treatment, monitoring, or prevention of diseases. These AI medical devices must undergo registration with the Central Licensing Authority and comply with safety and efficacy standards, with manufacturers and importers bearing responsibility for device compliance. However, significant regulatory gaps remain, particularly regarding liability determination when AI systems make errors, as current legal frameworks were designed for traditional healthcare providers rather than autonomous AI systems.

[33] Indian Contract Act, 1872; Soumyadipta Chanda and Rohit Tiwari, ‘The Concept of No-Fault Liability in Contracts for the Sale of Goods’ (SSRN, 29 July 2011) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898289> accessed 1 July 2025.

[34] Reserve Bank of India, ‘Master Circular—Loans and Advances – Statutory and Other Restrictions’ (RBI/2011 12/59, DBOD.No.Dir.BC.6/13.03.00/201112,1July2011) <https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=900 >; Reserve Bank of India, ‘Master Direction – Reserve Bank of India (Credit Information Reporting) Directions, 2025’ (RBI, 6 January 2025) <https://www.fidcindia.org.in/wp-content/uploads/2025/01/RBI-CICs-MASTER-DIRECTIONS-06-01-25.pdf > both accessed 1 July 2025.

[35] *Ibid*.

[36] Reserve Bank of India, ‘Framework for Responsible and Ethical Enablement (FREE) of Artificial Intelligence (AI) in the Financial Sector – Setting up of a Committee’ (RBI Press Release) https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=59377 accessed 1 July 2025.

[37] *Securities and Exchange Board of India Act 1992,* s 11(1) and 11A(2); *Securities and Exchange Board of India (Intermediaries) Regulations* 2008; *Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations* 2018;
Securities and Exchange Board of India (Depositories and Participants) Regulations 2018.

[38] Nicholas McDonagh, *‘SEBI Regulations & the Capital Markets in India’* (Law.asia, 2024) <https://law.asia/sebi-regulations-capital-markets-india/> accessed 1 July 2025; Securities and Exchange Board of India, ‘List of All SEBI Regulations’ <https://www.sebi.gov.in/sebiweb/home/HomeAction.do?doListing=yes&sid=1&ssid=6&smid=0> accessed 1 July 2025.

4. Limitations of The Indian Liability Framework

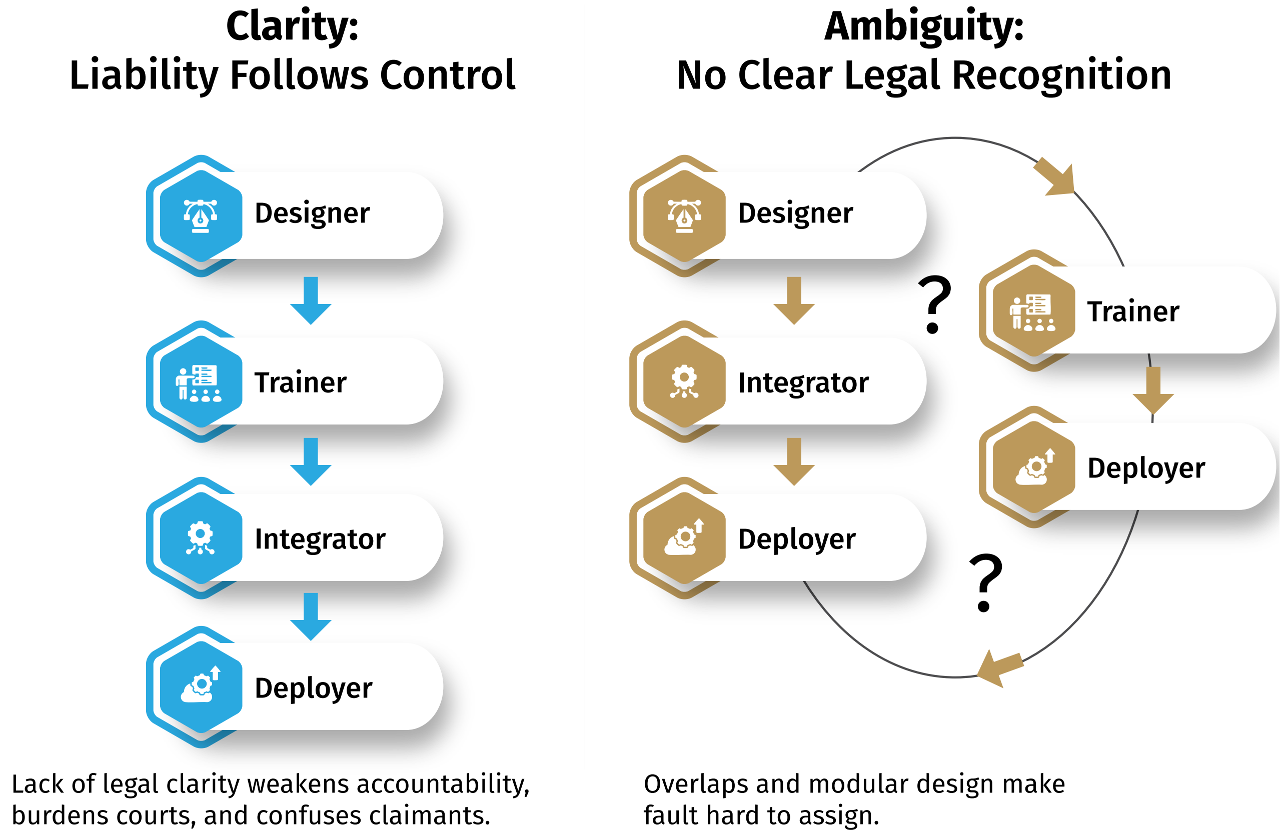
The present model continues to rely on adapting traditional legal definitions to contemporary technological realities.[39] However, there is growing momentum, both within policy circles and regulatory bodies, towards exploring the need for more targeted legal reforms to address the evolving challenges of artificial intelligence.[40] While this change may not be informed by legal analysis in the context of liability, our paper argues that it must be used to advance this discussion. Accordingly, this section evaluates the Indian framework's suitability for addressing liability in the context of AI systems.

As part of this suitability analysis, we find that aspects of the broad AI harms that manifest while attributing liability for AI harm, manifest in the Indian legal context as well. Specifically, we identify three gaps in the current framework. These are (i) Inadequate Recognition of Various Participants in the AI Value Chain; (ii) Gaps in Defining "Product" and "Defect" for AI Systems; and (iii) Causation, Attribution and Procedural Limits in AI Systems.

Inadequate Recognition of Various Participants in the AI Value Chain (Refer Illustration 3)

A key shortcoming of the Indian legal framework is its failure to clearly identify and assign liability to the different entities involved in the AI value chain. This includes those who design, train, deploy, or operate AI systems. Without clear legal recognition of these roles - whether through legislation, binding guidelines, or case law - it becomes difficult to determine who should be held accountable when harm occurs. This lack of clarity places a heavy burden on courts and claimants, who must navigate complex technical questions just to establish liability.[41] In practice, this can also result in no single entity being held responsible for an

Illustration 3: Clarity vs. Ambiguity in the flow of liability


Clarity:
Liability Follows Control
Designer
Trainer
Integrator
Deployer
Lack of legal clarity weakens accountability, burdens courts, and confuses claimants.
Ambiguity:
No Clear Legal Recognition
Designer
Integrator
Deployer
?
Trainer
Deployer
?
Overlaps and modular design make fault hard to assign.

[39] PIB Press Release Ministry of Electronics and Information Technology, 'Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes' (Press Information Bureau, 15 March 2024) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445> accessed 25 April 2025.; PIB Press Release Ministry of Electronics and Information Technology, 'Government of India Taking Measures To Tackle Deepfakes' (Press Information Bureau, 15 March 2024). <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2119050> accessed 25 April 2025.

[40] Ministry of Electronics and Information Technology (India), *Subcommittee Report on AI Governance and Guidelines Development* (December 2023) <https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf> accessed 25 April 2025.

[41] Heather Fraser, Rebecca Simcock and Aaron J Snoswell, '*AI Opacity and Explainability in Tort Litigation*' in Proceedings of the 2022 *ACM Conference on Fairness, Accountability, and Transparency* (June 2022) 185.

AI harm.[42] It also risks diminishing incentives for actors to build safer and more compliant systems, knowing that the risk of legal consequences is uncertain.[43]

Moreover, recognizing all participants in the AI value chain is essential to ensure that liability aligns with actual control and influence over outcomes.[44] Without such clarity, the legal system cannot effectively deter harmful conduct or incentivize responsible design and deployment practices.[45] It also risks creating a chilling effect on innovation,[46] as parties may either face unpredictable liability or evade accountability altogether. A fair and transparent attribution of responsibility is therefore critical to uphold both justice and systemic trust.

Most Indian liability regimes are rooted in fault-based liability and are typically structured around the actions of identifiable natural or legal persons.[47] While Indian law does allow for joint or several liability in principle, particularly in contract[48] and tort,[49] our research did not find any evidence of a structured understanding of how responsibility should be allocated among various stakeholders in an AI based system within the statutory laws we analyzed.

Amidst textual ambiguity, developing a framework for joint liability remains at the remit of the court. For instance, the current consumer protection and information technology frameworks in India do not adequately reflect the complex structure of AI systems, where multiple actors contribute at different stages.[50] Largely, they assume that responsibility lies with a single, clearly identifiable entity. In cases where a complainant brings a claim against multiple parties, the complainant must, in most cases, establish how each party caused harm to them.[51] This is complicated for AI ecosystems which often operate in modular and dynamic ways, where software updates, data flows, and user interactions continue to shape the product's behavior even after it reaches the market. This blurs the lines between manufacture, assembly, and operation, making it nearly impossible for a complainant to locate harm to a single actor in the AI system.

With Indian law providing limited guidance on how to allocate liability when multiple actors fulfil overlapping or sequential roles in the AI lifecycle, it becomes a significant gap in establishing a liability regime for AI systems. Without recognizing the value-chain actors and their roles within the AI related liability framework, the legal system struggles to tie responsibility to the appropriate locus of control. It ultimately may lead to an overly narrow assignment of liability, leading to exoneration. Conversely, it may lead to an overbroad assignment of liability, even where the actor had no meaningful control over the defective aspects of the system, thereby severing the fundamental link between fault and accountability.[52]

Gaps in Defining "Product" and "Defect" for AI Systems

Products

The Consumer Protection Act, 2019 defines "product" under Section 2(33) as

> "*any article or goods or substance or raw material or any extended cycle of such product, which may be in gaseous, liquid, or solid state possessing intrinsic value which is capable of delivery either as wholly*

[42] P Hacker, '*The European AI Liability Directives – Critique of a Half-hearted Approach and Lessons for the Future*' (2023) 51 *Computer Law & Security Review* 105871.

[43] Gabriel Weil, 'The Limits of Liability' Law-AI.org (1 August 2024) <https://law-ai.org/the-limits-of-liability> accessed 1 July 2025.

[44] Bart Custers, Henry Lahmann and Bryce I Scott, 'From Liability Gaps to Liability Overlaps: Shared Responsibilities and Fiduciary Duties in AI and Other Complex Technologies' (2025) *AI & SOCIETY* 1.

[45] *Ibid*.

[46] Hacker (n 42).

[47] *See* Section 3: Extant Framework For Liability In India.

[48] *Indian Contract Act 1872*, s.43.

[49] *Kushro S Gandhi v N A Gajdar* AIR 1970 SC 1468.

[50] Under the Consumer Protection Act, the courts while assessing liability between "sellers" and "manufacturers" have placed reliance on a value-chain whereby they have assessed the role of the actors in the harm and held them jointly and severally liable. Similarly, under the Information Technology Act, 2000; courts have placed reliance on Section 43A holding, a "*body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person*" viewing a binary relationship between the end-deployer and complainant, to whom harm is caused. Similarly, the Information Technology Act, 2000, offers safe harbor to "intermediaries" - typically platforms like social media services, exempting them from liability for third-party content, provided they follow certain due diligence requirements. As a result, liability may either be unjustifiably avoided when no single actor can be blamed, or unfairly imposed on one party due to the absence of formal recognition of others. This gap in legal structure creates uncertainty and undermines both fairness and accountability.

[51] *State Bank of Patiala Aliganj Branch Lucknow v Suhas Enterprises and Others* 2024 SCC OnLine TDSAT 1236. Notably, an exception to this appears to be liability for product manufacturers. Such liability is strict liability. *See Consumer Protection Act 2019*, s 84.

[52] Christian Wendehorst, 'Liability for Artificial Intelligence: The Need to Address both Safety Risks and Fundamental Rights Risks' in The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives (*Cambridge University Press* 2022) 187.

> *assembled or as a component part and is produced for introduction to trade or commerce*".[53]

While this definition is comprehensive, it does not explicitly account for AI systems. The inclusion of "gaseous, liquid, or solid state" might be interpreted expansively to cover digital entities like AI systems. However, this remains a speculative take on the nature of the Act. Considering the bespoke nature of AI, undertaking targeted interventions is critical.

Precedents support the need to resolve this ambiguity with targeted interventions. For now, we understand that no expansive judicial interpretation of "product" has been concluded. While some precedent supports recognizing software as 'goods', such precedent only holds persuasive value. This is for two reasons: one, such precedent has evolved after the interpretation of provincial tax law.[54] Second, both 'goods' and 'products' have separate meaning under Indian law. The difference between "goods" and "product" in the context of the Act is that "goods" under Section 2(21) refers specifically to "every kind of movable property and includes 'food'", while "product" under Section 2(33) has a broader scope encompassing "any article or goods or substance or raw material or any extended cycle of such product" in any physical state. Functionally, "product" serves as the comprehensive term used within the product liability framework under Section 83, where manufacturers, sellers, and service providers can be held liable for harm caused by defective products. The term "goods" appears more limited to movable property transactions, while "product" encompasses the entire liability ecosystem including raw materials, extended product cycles, and various physical states, making it the operative term for determining accountability in consumer protection cases. Given this, regulators may wish to consider how they align AI and its features to the extant definition of "products" under the CPA.[55]

Separately, while the definition of "*products*" includes "extended cycle of a product", it is unclear if it will also apply to AI systems capable of self-learning. We have found limited interpretation of the term "extended cycle of a product" based on our research. However, in management, "*extended cycle*" of a product refers to strategies used to prolong the product's life, typically beyond its natural maturity stage.[56] This is akin to how AI systems develop. Thus, there is limited clarity in how the definition of "product" can apply to AI, and in the context of its inherent nature.

Defects

Relatedly, the CPA, 2019 defines "defect" as "*any fault, imperfection or shortcoming in the quality, quantity, potency, purity or standard which is required to be maintained by or under any law for the time being in force or under any contract, express or implied.*"[57] Effectively, the Act recognizes three primary types of defects: manufacturing defects occurring during production or assembly, design defects present when products are structurally unstable, and marketing defects involving insufficient instructions or improper labeling.[58] Conventionally, Indian consumer protection law embraced a strict liability framework for harm caused by defective products or services.[59] Aspects of this have permeated the CPA; product manufacturers face strict liability under Section 84.[60]

In effect, the CPA's attitude to defects appears to focus primarily on tangible products. This focus restricts it from endorsing the novel pathways in which AI systems generate defects that impact product safety.[61] While safety is not an explicit object of the Act, elements of it have endorsed safety as a guiding principle.[62] Relatedly, jurisprudence has also recognized the role of safety in shaping consumer protection law, particularly the CPA's predecessor – the CPA, 1986.[63]

[53] *Consumer Protection Act 2019*, s 2(33).

[54] Supreme Court in *Tata Consultancy Services v. State of Andhra Pradesh* held that a 'software' is a 'goods' under the Section 2(h) of the Andra Pradesh General Sales Tax Act, 1957. In its interpretation, the court relied on interpretation of the term "goods" under Article 366(12) of the Indian Constitution relying on *Associated Cements Companies Ltd. v. Commissioner of Customs* (2001) 4 SCC 593.

[55] For instance, regulators may interpret AI as being both a good and an extended cycle of such product if it possess the capacity to self-learn. Confining AI's definition to simply goods forecloses this possibility.

[56] BM Enis, R La Garce and AE Prell, 'Extending the Product Life Cycle' (1977) 20(3) *Business Horizons* 46.

[57] *Consumer Protection Act 2019*, s 2(10).

[58] *Consumer Protection Act* 2019, s 84.

[59] *A. Nazar v. New India Assurance Co. Ltd.* (1988) 8 SCC 438; *Punjab Urban Planning & Development Authority v. Vidya Chetal* (2019) 9 SCC 83.

[60] The liability framework extends to product manufacturers for manufacturing defects, design defects, deviation from specifications, and failure to conform to express warranties. See, *Neena Aneja And Anr. vs. Jai Prakash Associates Limited* (2022) 2 SCC 161.

[61] Observably, the CPA notes that a defect arises from three sources: applicable law or contract.

[62] *Consumer Protection Act 2019*, ss 13 and 18.

[63] *C. Venkatachalam v. Ajitkumar C. Shah* (2011) 9 SCC 707.

In viewing the current definition of defects through this safety lens, demonstrates shortcomings. Consider this; an AI-powered in-house baby monitor responds to unintended environmental stimulus (such as a reporter's voice on television) and continually initiates unwanted outcomes (such as nudging the baby to go to another room or stay quiet). In the absence of a directive that the monitor manufacturer was required to insulate his product from environmental stimulus under any applicable law or contract, this defect may go unaddressed under the CPA. Alternatively, judicial authorities may ungainly extend the application of the CPA, under no established rubric to address this harm.

More pertinently, the nascent nature of AI systems has meant that there is scant recognition of the true nature of defects in the context of AI. This definition does not operate in silo. When read with the CPA's provision on product liability, it becomes sufficiently clear that product manufacturers are not merely liable for defects. Instead, they are also liable for failing to disclaim harm, improper or incorrect usage.[64] Given the broad definition of harm, and the lack of any definition of improper or incorrect use, the absence of a well-tailored definition of defects for AI may result in further ambiguity while determining the distinction between 'defective AI' and 'harmful AI'.

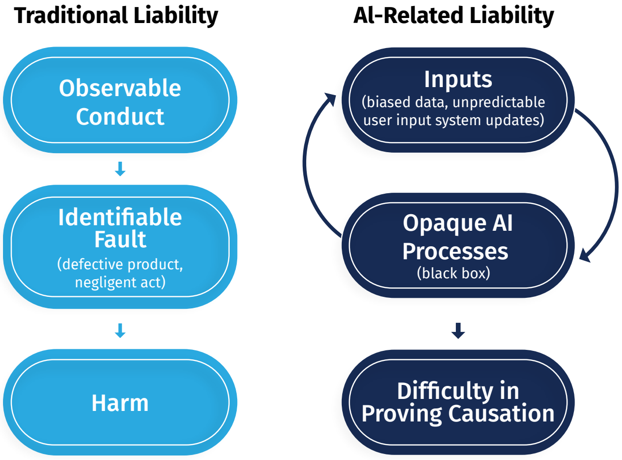
Causation, Attribution and Procedural Limits in AI Systems

Causation (Refer Illustration 4)

Establishing causation is central to any liability regime, as it enables courts to connect a specific act or omission to the harm suffered by a claimant. Without this link, it becomes difficult to attribute responsibility or provide effective remedies.[65] In traditional legal contexts, causation can often be demonstrated through observable conduct, defective products, or breach of contractual terms. However, AI systems, particularly those built using machine learning or deep learning, function in a non-deterministic[66] and opaque manner.[67] These systems do not follow a fixed set of instructions but instead evolve based on data inputs and adapt over time. As a result, harm may arise not from a single identifiable fault, but from a complex interaction of factors such as biased training data, unpredictable user inputs, or autonomous system adjustments. In such cases, conventional procedural laws designed around 'observable fault offer little guidance. They presume that relevant information is accessible and that causation can be inferred from direct evidence or proximate conduct.[68] Moreover, claimants face significant procedural burdens.[69]

Indian law currently addresses causation through frameworks that tie liability to specific, legally recognized entities.[70] The CPA establishes both fault-based and strict liability mechanisms. Under fault-based regimes, applicable to service providers and, in some circumstances, product sellers,[71] a claimant must demonstrate a direct link between deficiency or defect and resulting harm. However, product manufacturers can be held strictly liable for harm caused by a defective product without requiring proof of negligence.[72] This includes, *inter alia*,

Illustration 4: Traditional Liability and AI-Related Liability


Traditional Liability
AI-Related Liability
Observable Conduct
Identifiable Fault
(defective product, negligent act)
Harm
Inputs
(biased data, unpredictable user input system updates)
Opaque AI Processes
(black box)
Difficulty in Proving Causation

[64] *Consumer Protection Act 2019*, s 84(e).

[65] Jaap H Lehmann, Joost Breuker and Bob Brouwer, 'Causation in AI and Law' (2004) 12 *Artificial Intelligence and Law* 279.

[66] Alexandra F Cooper, Jonathan Frankle and Christopher De Sa, 'Non-determinism and the Lawlessness of Machine Learning Code' in Proceedings of the 2022 *Symposium on Computer Science and Law* (November 2022) 1.

[67] Hacker (n 46).

[68] *Kurban Hussein Mohammedali Rangwalla v State of Maharashtra* AIR 1965 SC 1616.

[69] Proving causation may require access to proprietary code, system logs, or decision trails, materials that are typically unavailable under existing legal procedures. Even initiating a claim might require expert evidence, making the process expensive and inaccessible. The absence of mechanisms to compel technical disclosures or accommodate the complexity of AI systems makes proving causation both costly and uncertain, weakening the effectiveness of the liability framework.

[70] Section 83 of the Consumer Protection Act states "*A product liability action may be brought by a complainant against a product manufacturer or a product service provider or a product seller, as the case may be, for any harm caused to him on account of a defective product.*"

[71] *Consumer Protection Act 2019*, ss 85–86.

[72] *Consumer Protection Act 2019*, s 84(2).

design defects, manufacturing defects, or failure to provide adequate usage instructions.[73] Thus, strict liability presumes that causation is legally imputed to a single manufacturer once harm and defect are shown.[74]

However, this legal structure relies on identifiable roles and a linear chain of accountability. For instance, in deciding a consumer law related dispute, the Supreme Court in *Spring Meadows Hospital v. Harjol Ahluwalia*,[75] assigned liability to the identified hospital after a minor child was rendered permanently "vegetative" due to the wrongful administration of an injection by an unqualified nurse - even with a doctor and nurse were in the causative chain. Further, in *Neo Build Infrastructure v. Sushil Ranjan Roy*[76] the consumer forum was deciding on whether a person who receives possession of a flat or plot, and has the conveyance deed executed in their favor, continues to be a consumer of the builder or developer. The National CDRC extended liability for latent defects that manifested post-possession on the builders of a residential plot - yet again presuming that a single responsible actor (the builder) could be identified.

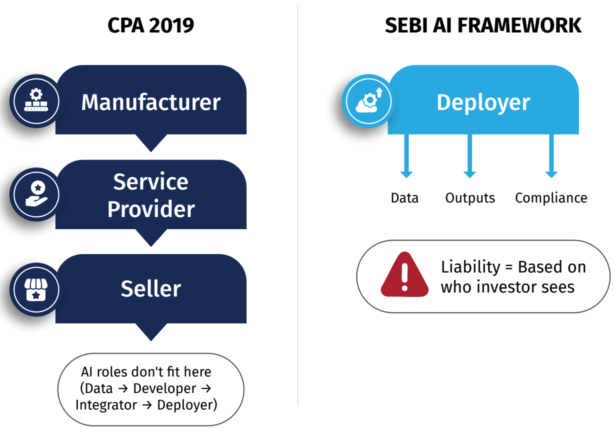
The CPA's structure reinforces this model. A "product manufacturer" is defined to include anyone who, inter alia, manufactures, assembles, markets, or labels a product, suggesting that multiple entities may qualify, but ultimately with the aim of assigning liability to a principal actor.[77] Similarly, it permits strict liability for product sellers only under specific conditions, such as modification of the product, express warranties, or failure to exercise reasonable care, again tethered to identifiable conduct.[78] Accordingly, it appears that the system works when products are discrete, and actors are siloed.

However, AI systems disrupt this linearity. Roles like developer, dataset curator, deployer, and interface integrator often reside in different entities, each contributing in small but potentially decisive ways to AI's behavior. This doctrinal rigidity poses real-world procedural challenges. The legal framework assumes that the claimant can identify and access relevant evidence (design specifications, usage logs, fault data) and that courts can interpret it. Yet AI systems often operate as black boxes, lacking transparency or auditable logic trails. Moreover, no statutory obligation under the CPA requires AI developers or deployers to maintain detailed operational records, making causal tracing nearly impossible in practice. In essence, it renders a claimant incapable of identifying the actor mentioned as the liable entity under the legislative framework.

While Indian law does recognize and operationalize causation in both fault-based and strict liability frameworks, it does so by anchoring legal responsibility to specific, identifiable actors. This model falters in the context of AI, where harm is diffused, emergent, and distributed across a value chain. As a result, even legitimate claims may go unremedied, not due to lack of harm, but because the current legal architecture cannot accommodate non-linear, multi-actor causation. Bridging this gap will require a fundamental rethinking of how Indian law conceptualizes liability, not just in terms of fault or defect, but in terms of influence, control, and systemic contribution in technologically complex environments.

Attribution (Refer Illustration 5)

Illustration 5:Attribution of Liability under the CPA and the SEBI Framework


CPA 2019
Manufacturer
Service Provider
Seller
AI roles don't fit here (Data → Developer → Integrator → Deployer)
SEBI AI FRAMEWORK
Deployer
Data
Outputs
Compliance
Liability = Based on who investor sees

Attribution for Liability

The attribution of liability for AI systems under the CPA, 2019 presents significant challenges due to the complex multi-stakeholder ecosystem involved in AI development and deployment. Under the current paradigm, the Act establishes

[73] *Consumer Protection Act 2019*, s 84(1).

[74] Miriram C. Buiten, 'Product Liability for Defective AI' (2024) *European Journal of Law and Economics* <https://link.springer.com/article/10.1007/s10657-024-09794-z> accessed 1 July 2025.

[75] *Spring Meadows Hospital v. Harjol Ahluwalia* (1998) 4 SCC 39.

[76] *Neo Build Infrastructure Pvt Ltd and Others v Sushil Ranjan Roy and* Others (NCDRC, 2 November 2023) Revision Petition No 58 of 2020.

[77] *Consumer Protection Act 2019*, s 2(36).

[78] *Consumer Protection Act 2019*, s 86.

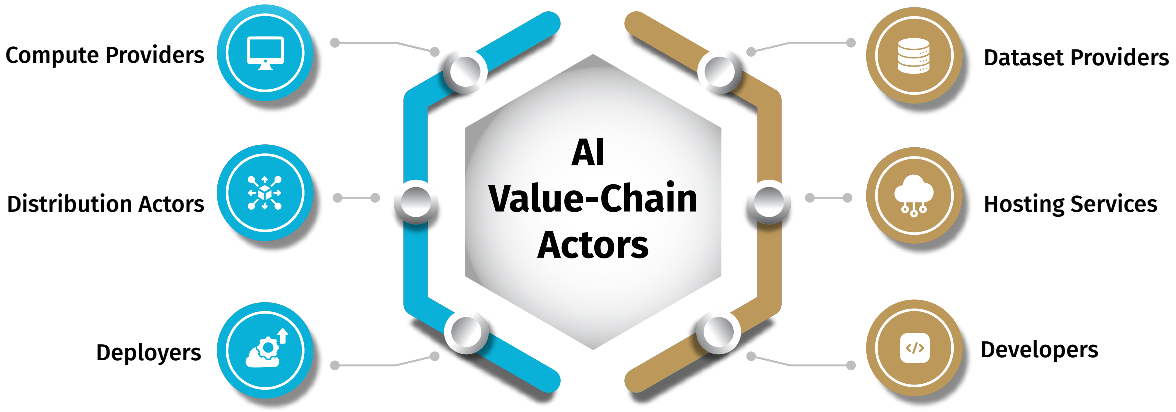
distinct liability frameworks for product manufacturers, product service providers, and product sellers, with manufacturers bearing strict liability for defects including manufacturing defects, design flaws, non-conformance to specifications, breach of express warranty, and inadequate instructions or warnings.[79] Product service providers are held liable when their services are faulty, deficient, or inadequate, or when they fail to provide proper instructions or warnings.[80]

However, this traditional framework proves inadequate for AI systems because it struggles to address the fundamental challenge of identifying the primary responsible party among numerous stakeholders throughout an AI system's lifecycle, from development to deployment.[81] The autonomous decision-making capabilities of AI systems, combined with their inherent unpredictability and inexplicability, make it difficult to establish clear causation and determine whether defects stem from algorithmic design flaws, training data issues, or implementation errors.[82] The current liability paradigm fails to account for scenarios where AI systems operate autonomously and make decisions beyond the direct control of any single entity, creating liability gaps where traditional concepts of manufacturing defects and service deficiencies become blurred.[83] This inadequacy is particularly pronounced given that AI systems often involve multiple parties, including algorithm developers, data providers, system integrators, and operators, making it challenging to pinpoint the actor who should bear primary responsibility.

In certain instances, regulators may subvert engaging with the value chain. An example of this in India is the SEBI. SEBI through various amendments created a clear framework for liability arising from the use of artificial intelligence and machine learning tools and techniques (AI and ML Tools) by stock exchanges, clearing corporations, depositories, and SEBI-regulated intermediaries.[84] Under the amended framework, entities are made solely responsible for three key areas: (i) the privacy, security, and integrity of investor and stakeholder data, (ii) the outputs generated using AI and ML Tools, and (iii) compliance with applicable laws governing such usage. The amendments impose responsibility based on who is visible to the investor, not who is causally linked to the harm.

This results not only in overbroad legal exposure but in a chilling effect on innovation. This approach undermines the core legal principle that liability must follow fault. SEBI's framework imposes full liability on the deployer without

Illustration 6: Actors in the AI Value Chain



[79] *Consumer Protection Act 2019*, ch VI.

[80] Ashok R Patil, 'Product Liability Action: A Tooth to Strengthen Consumer Protection' (2022) 10 *International Journal on Consumer Law and Practice* <https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1080&context=ijclp > accessed 1 July 2025.

[81] Jingyao Li, 'Liability Attribution in the Context of AI Use' (2021) *Academy of Management Proceedings* <https://journals.aom.org/doi/10.5465/AMBPP.2021.11283abstract >accessed 1 July 2025.

[82] Mark Coeckelbergh, 'Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability' (2020) 26 *Science and Engineering Ethics* 2051 <https://doi.org/10.1007/s11948-019-00146-8> accessed 1 July 2025.

[83] The blurring of these traditional concepts becomes evident when considering that AI systems often function as hybrid entities that combine product and service characteristics. An AI system may technically function as designed (no manufacturing defect) and the service provider may have followed all protocols (no service deficiency), yet the system's autonomous decision-making process may still produce harmful outcomes. The Act's binary classification of liability between product manufacturers and service providers cannot adequately capture scenarios where multiple stakeholders throughout the AI lifecycle—including algorithm developers, data providers, system integrators, and operators—contribute to the system's autonomous capabilities without any single party having complete control over its decisions.

[84] Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018, SEBI (Depositories and Participants) Regulations, 2018, SEBI (Intermediaries) Regulations, 2008.

requiring any inquiry into where or how the harm originated. This results in a form of causation by proximity, where the actor nearest to the consumer absorbs blame, even when the fault lies elsewhere. It treats deployment as an endorsement and replaces the need to trace harm through the system with a rule of convenience *(Refer Illustration 6).*

Judicial Attribution of Liability in Multi-Actor Systems

Building on the gaps discussed above, Indian courts have also shown a tendency to assign liability based on institutional visibility rather than direct fault. This trend is evident in sectors like healthcare and finance, where courts favor consumers in disputes involving technical complexity of multiple actors.

For example, *in Savita Garg v. National Heart Institute* (2004),[85] the Supreme Court held a hospital liable under the CPA 1986 for failing to produce medical records after a patient's death, even though the hospital itself was not impleaded in the proceedings. The Supreme Court placed the burden on hospitals to prove they exercised due care once a patient is admitted, easing procedural requirements for complainants. This approach prioritizes institutional responsibility and visibility over strict proof of individual fault, effectively shifting the evidentiary burden onto institutions. As a result, it introduces a presumption of negligence in complex, multi-actor settings, diluting the traditional fault-based standard.

A similar pro-consumer outcome under the CPA 1986 occurred in (1998).[86] The Court found both the nurse and the resident doctor negligent but ultimately placed the burden of liability on the hospital for failing to ensure proper oversight and employing unqualified personnel. Notably, the Court acknowledged that multiple actors were involved, including doctors, nurses, and administrative decisions, yet still imposed responsibility on the hospital as the most visible and authoritative institutional actor.

In AI contexts, the "David vs. Goliath" instinct is inverted. AI developers or deployers are often perceived as the dominant player, inviting stricter scrutiny even when they lack comprehensive control over the AI stack. The judiciary's protective impulse may therefore unintentionally punish the most cooperative or accessible actor, rather than the most causally responsible one. In doing so, it risks chilling innovation, deterring deployment, and disincentivizing transparency.

While the approach in *Savita Garg* and *Harjol Ahluwalia* may be justified in healthcare, where roles are clearer and oversight mechanisms more robust, its uncritical application in AI systems could produce unjust outcomes. It risks assigning liability to the most accessible actor rather than the most responsible one, thereby creating legal fictions of causation. Thus, while these cases provide an important precedent in recognizing institutional, it risks fostering a regime of unjust attribution and judicial overkill. Courts must resist the temptation to conflate control with fault, otherwise the legal system itself will become a barrier to the very innovation it seeks to regulate responsibly.

The concept of "control" under the Consumer Protection Act (CPA) remains jurisprudentially underdeveloped, particularly concerning the allocation of distributive and joint liability. The emergence of AI systems complicates established liability frameworks, as the AI value chain encompasses diverse actors whose roles often do not align neatly with the CPA's conventional categories of manufacturer, service provider, and seller.[87] Under the CPA, manufacturers are subject to strict liability, whereas service providers and sellers are generally held to a fault-based standard.[88] Courts have, imposed joint liability across these categories, relying on an assessment of each entity's contributory role.[89] Nevertheless, existing jurisprudence remains limited, primarily focusing on singular manufacturers and service

[85] *Savita Garg v. National Heart Institute* 2004 8 SCC 56. [Savita Garg reflects a judicial preference for holding institutions accountable in negligence cases, even when individual wrongdoers are not specifically identified..]

[86] *Spring Meadows Hospital v. Harjol Ahluwalia* (1998) 4 SCC 39.

[87] Consumer Protection Act, 2019 ss 82-86.

[88] Ibid.

[89] Bajaj Auto Limited and Ors. v. Yaradi Prabhat SC/28/A/203/2023. ("*The manufacturer, dealer, showroom, and service center were jointly and severally liable under Sections 82–86 of the Consumer Protection Act, 2019 for delivering a motorcycle with a design/manufacturing defect and failing to provide adequate service, thereby causing financial and mental hardship to the consumer.*")

providers rather than multifaceted collaborations or chains of responsibility.[90]

In the context of AI, the multiplicity of stakeholders ranging from developers and data providers to integrators and end-users, renders attribution of liability more complex. AI's inherent opacity and the diffused operational roles within its value chain challenge the CPA's pre-determined liability categories. For instance, where harm results from the actions or omissions of a service provider involved in deploying an AI system, and causation standards remain ambiguous, the CPA's strict liability provisions may still render the manufacturer liable. This outcome potentially disregards the nuanced allocation of fault among various actors in the AI supply chain, highlighting a lacuna in the current liability regime.

An overarching result is a system where causation is legally assumed rather than established. Without procedural tools that allow regulators or courts to trace fault accurately, SEBI's model risks penalizing responsible actors while failing to deter those who actually cause harm.

This growing reliance on visibility rather than fault intensifies the procedural challenge of proving causation.

[90] Jose Philip Mampillil v. Premier Automobiles Ltd., (2004) 2 SCC 278; Ashoke Khan v. Abdul Karim, 2005 SCC OnLine NCDRC 22; Jagrut Nagrik v. Proprietor Baroda Automobiles Sales and Service Indira Avenue, 2010 SCC OnLine NCDRC 250; Tata Motors Ltd. v. H.M. Somashekaraiah and Ors. MANU/SP/0006/2024.

5. Statutory Liability in Other Jurisdictions: Models and Insights

In this section, we conduct an analysis of four jurisdictions: the United States of America, European Union, Japan and Australia. We provide an overview of the jurisdictional models and extract the features of the jurisdiction in the context of statutory liability for AI systems. Subsequently, we map these models to the limitations identified in the Indian model.

Australia

Overview of Australia's Liability Framework

The positioning of liability within Australia's AI regulatory framework relies heavily on existing legal structures rather than creating novel AI-specific liability regimes.[91] In the context of AI, Australia provides for The Voluntary AI Safety Standards which are standards prepared through consultations informing guidelines for AI adoption.[92] Under current Australian law, liability for AI-related harms operates through multiple pathways: the Australian Consumer Law's product liability provisions, which impose strict liability on manufacturers for safety defects in AI systems; tort law principles, particularly negligence, though establishing causation may prove challenging given AI's complexity; and consumer protection guarantees that require suppliers to remedy defective AI-enabled goods and services.[93] The burden of proof generally remains with the victim, who must demonstrate defects, causation, and damages on the balance of probabilities.[94]

Significantly, Australia's approach does not change the traditional liability frameworks but rather expects existing laws to adapt to AI contexts, though the government has acknowledged that current regulatory frameworks may require strengthening to address AI-specific harms.[95] This creates a complex liability landscape where AI developers, deployers, and users may all bear responsibility depending on their role in the AI supply chain and the specific circumstances of any harm.

Critics argue that the government's cautious approach risks leaving significant regulatory gaps that could allow harmful AI applications to operate without adequate oversight, particularly given the rapid pace of AI technological development.[96] The absence of specific

[91] Australian Government Treasury, 'Discussion Paper on AI Liability' (October 2024) <https://treasury.gov.au/sites/default/files/2024-10/c2024-584560-dp.pdf> accessed 1 July 2025.

[92] Australian Department of Industry, Science and Resources, Voluntary AI Safety Standard (2024) <https://www.industry.gov.au/publications/voluntary-ai-safety-standard> accessed 1 July 2025.

[93] *Ibid*.

[94] Colin Scott, 'Enforcing Consumer Protection Laws' in Geraint Howells, Iain Ramsay and Thomas Wilhelmsson (eds), *Handbook of Research on International Consumer Law* (2nd edn, Edward Elgar 2018) 466.

[95] Australian Government Treasury (n 87).

[96] IA, 'Aussie AI Regulation: Not Fast Enough?' (*Australian Computer Society*, 2023) <https://ia.acs.org.au/article/2023/aussie-ai-regulation--not-fast-enough-.html> accessed 1 July 2025.

timelines for implementing mandatory guardrails has frustrated stakeholders seeking regulatory certainty, while the principles-based approach to defining high-risk AI has been criticized for lacking specificity.[97]

Reforms from the Australian Model

Value Chain Governance

Australia's approach to value-chain governance for AI liability reveals significant limitations in traditional legal frameworks designed for simpler, more linear supply chains. The Australian Consumer Law establishes a basic supplier-manufacturer model with indemnity rights, where suppliers have primary responsibility for consumer remedies but can seek indemnification from manufacturers when goods fail to meet consumer guarantees.[98] However, this binary model proves inadequate while addressing the complex, multi-party nature of AI development and deployment.

Reforms are, however, underway to address this concern. The Voluntary AI Safety Standard attempts to address some of these challenges through Guardrail 8, which requires transparency with other organizations across the AI supply chain about data, models, and systems.[99] However, this voluntary approach lacks binding enforcement mechanisms and does not establish clear liability allocation among different actors in the AI value chain. The absence of mandatory requirements for supply chain governance creates significant gaps in ensuring accountability for AI-related harms.

Product and Defect Definitions for AI Systems

Australia's legal framework demonstrates moderate adaptability in defining products and defects for AI systems, though significant implementation uncertainties remain. The ACL explicitly defines software as "goods," eliminating the previous distinction between software supplied on physical media and software delivered electronically.[100] This definition provides a foundation for applying consumer guarantees and manufacturer liability provisions to AI systems. The ACL's concept of safety defects is based on whether products meet "the level of safety the public is generally entitled to expect".[101] There is precedent for the application of Australian Consumer Law to 'algorithms'; the term 'goods' was applied to algorithmic decision making in a Federal Court case that ordered Trivago, a travel company, to pay $44.7 million in penalties for misleading consumers about room rates in the recommendations made by its algorithm.[102]

Causation and Attribution

Australia's statutory legal framework inadequately addresses causation issues related to AI liability. Traditional causation requirements under Australian Consumer Law require plaintiffs to prove that defendants were the factual ("but-for") cause of their injuries on the balance of probabilities.[103] This burden of proof, while appropriate for conventional products and services, creates insurmountable challenges in the context of AI systems.

The Review of AI and the Australian Consumer Law Discussion Paper (October 2024) highlights that the opacity and complexity of AI systems, as well as their potential for autonomous and unpredictable behavior, can make it significantly harder for consumers to establish this link.[104] To this end, the paper references international developments, such as the EU's proposed 'presumption of causality' for AI-related harms, and notes that Australia is considering whether similar measures or enhanced record-keeping and transparency requirements might be necessary to ensure consumers are not unfairly disadvantaged when seeking redress for AI-related harms.[105]

[97] Australian Government, Australia AI 2025–2028: White Paper (2024) <https://static1.squarespace.com/static/6364a71770e4605f465b714e/t/6822ed78eb625b4901b487bb/1747119494280/Australia+AI+2025-2028+-+White+Paper.pdf> accessed 1 July 2025.

[98] Australian Treasury, Consultation Paper: Supporting Responsible AI (October 2024), <https://treasury.gov.au/sites/default/files/2024-10/c2024-583535-cp.pdf> accessed 1 July 2025.

[99] Australian Department of Industry, Science and Resources (n 88).

[100] Australian Government Treasury (n 87).

[101] Ibid.

[102] Australian Competition and Consumer Commission v Trivago N.V. [2020] FCA 16.

[103] Australian Treasury, Consultation Paper: Supporting Responsible AI (October 2024) ss 138 – 150 <https://treasury.gov.au/sites/default/files/2024-10/c2024-583535-cp.pdf> accessed 1 July 2025.

[104] Australian Government Treasury (n 87).

[105] Australian Government, Supporting Responsible AI: Consultation Portal (2024) <https://consult.industry.gov.au/supporting-responsible-ai> accessed 1 July 2025.

Japan

Overview of Japan's Liability Framework

Japan's approach to legal liability in the context of AI is currently shaped by a combination of general laws, sector-specific statutes, and soft law instruments, rather than a standalone AI legislative regime. Existing mechanisms include seeking remedies under **tort law**, consumer protection, product liability, data protection, and copyright regimes. While these binding instruments provide pathways for addressing AI-related harms, they are not designed to accommodate the complexity, autonomy, and opacity associated with modern AI systems. In response, the Japanese government has initiated the development of a soft law based AI governance framework that fosters responsible innovation while enhancing legal certainty.

In February 2025, the Japanese Cabinet introduced the Bill on the Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies[106] to the National Diet. The Bill aims to facilitate the safe and proactive use of AI by encouraging private sector cooperation with public objectives in areas such as data-sharing, innovation support, and ethical alignment. However, it stops short of imposing mandatory legal duties or liabilities. Its provisions are largely promotional and symbolic in nature, signaling Japan's continued preference for an innovation-friendly and collaborative regulatory posture, rather than a prescriptive or risk-calibrated legal regime.

Reforms from the Japanese Model

Value Chain Governance

Japan's model acknowledges the multiplicity of actors in the AI value chain through the AI Guidelines for Business.[107] However, it stops short of translating this recognition into binding legal structure. In doing so, it creates a regulatory gap between soft guidance and enforceable liability, a gap that may widen as AI systems become increasingly complex and autonomous.

The **Contract Guidelines on the Use of AI and Data**,[108] issued by the METI provide a framework for drafting fair and effective contracts across different stages of AI development. Informed by updated model agreements released in 2023, the guidelines highlight critical considerations such as data usage rights, non-exclusive access to trained models, and the allocation of liability for uncertain outputs.[109] By encouraging private parties to allocate risk *ex-ante*, these guidelines aim to bridge legal gaps and promote smoother collaboration between AI vendors and users. Similarly, the **AI Guidelines for Business** (2024)[110] set out general principles such as transparency, accountability, and fairness, and encourage actors across the AI lifecycle to operationalize these values in practice – across AI developers, providers and business users. However, both instruments are **non-binding**, and do not assign legal liability to any actor for specific failures or harms.

[106] 'Japan's Lower House passes AI promotion bill' The Japan Times (25 April 2025) https://www.japantimes.co.jp/news/2025/04/25/japan/politics/lower-house-ai-bill/ accessed 12 May 2025.

[107] Ministry of Economy, Trade and Industry (Japan), AI Guidelines for Business Ver 1.0 (19 April 2024) <https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_14.pdf> accessed 1 July 2025.

[108] Ministry of Economy, Trade and Industry (Japan), 'AI Guidelines – Japanese Version' <https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pd>; Monolith Law, 'Explainer on AI Guidelines' <https://monolith.law/en/it/ai-guidelines> both accessed 1 July 2025.

[109] Ibid.

[110] Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry (Japan), AI Guidelines for Business Ver 1.0 (19 April 2024). <https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_9.pdf> accessed 12 May 2025.

Japan's only binding statutory regime that allocates liability for defective products, the Product Liability Act, recognizes a limited set of actors under: manufacturers, importers, and those who present themselves as manufacturers (e.g., by branding the product), or who are reasonably perceived as such where the actual manufacturer is unknown.[111] Retail sellers, distributors, and software or service providers do not fall within this framework unless they also meet one of the above roles.

Product and Defect Definitions for AI Systems

Japan's product liability law is based on definitions that do not easily apply to modern AI technologies. The law treats only physical goods as "products" and looks at defects based on the product's condition at the time of delivery. This makes it difficult to apply the law to standalone software or AI systems that change over time, leaving many AI-related harms outside the scope of existing liability rules.

Japan's Product Liability Act (PLA)[112] imposes liability on manufacturers for damage caused by defective products, irrespective of fault. However, it defines "product" narrowly as "movable property"[113] which has consistently been understood to mean tangible goods. This interpretation excludes standalone software, including most AI applications, from the scope of the PLA.

The PLA also defines a "defect" as a lack of safety that a product should ordinarily provide, considering its nature, foreseeable use, and the state of scientific or technical knowledge '*at the time of delivery*.'[114] This standard presents a particular challenge in the context of AI. Many AI systems, especially those based on machine learning, are designed to evolve after deployment. Where a defect emerges due to the AI's post-sale adaptation such as learning from new data or operating conditions it may fall outside the PLA's definition of a defect, as the harm could not have been foreseen at the time of sale.

This creates two key difficulties. First, manufacturers may not be held liable for harm resulting from how the AI system learns or behaves after delivery, even if the harm is substantial. Second, those harmed by such AI systems may be left without legal remedy, as the law does not clearly recognize defects that arise from post-deployment behavior. In this way, the PLA may fall short of offering meaningful consumer protection in the AI context.

Causation and Attribution

Japan's statutory liability regime does not currently offer procedural tools to meaningfully address the causation challenges posed by AI, where harm may result from autonomous or evolving functions after the point of sale. The law requires plaintiffs to prove a clear link between a defect and the damage, but offers no presumptions, disclosure rights, or procedural support to help meet this burden in complex AI cases.[115]

Under Japan's PLA, a claimant must establish a causal link between a product defect and the damage suffered.[116] However, in the context of AI systems, this requirement creates significant evidentiary burdens. As discussed earlier, the PLA only recognizes defects based on the state of the product '*at the time of delivery*.' This poses challenges for AI systems that evolve post-sale, where harm may arise from learning processes or adaptive behaviors not present at the point of delivery. These challenges are compounded by the technical opacity of AI systems.

[111] Product Liability Act 1994(Japan), art 2(3).

[112] Product Liability Act 1994(Japan).

[113] Product Liability Act 1994 (Japan), art 2(1).

[114] Product Liability Act 1994 (Japan), art 2(2).

[115] Under Japanese law, there is no disclosure obligation or extensive discovery process in contrast with common law jurisdictions. Evidence is generally introduced by the parties through their own efforts. The court may order the submission of documents and the commissioning of examinations when a motion is filed by a party, and it is difficult for that party to collect documentary evidence from the other side that would be clearly necessary to prove their case (Article 132-4 of the Code of Civil Procedure.). <https://iclg.com/practice-areas/product-liability-laws-and-regulations/japan> accessed 1 July 2025.

[116] *International Comparative Legal Guides*, 'Product Liability Laws and Regulations Japan 2024' (ICLG, 2024) <https://iclg.com/practice-areas/product-liability-laws-and-regulations/japan#:~:text=As%20a%20general%20rule%2C%20the%20party%20bringing,injured%20party)%20bears%20the%20burden%20of%20proof.&text=For%20breach%20of%20contract%20claims%2C%20the%20plaintiff,has%20caused%20some%20damage%20to%20the%20plaintiff> accessed 1 July 2025.

United States of America

Overview of the US liability framework

American AI regulation is characterized by deep fragmentation. The American model relies heavily on existing legal frameworks, voluntary industry guidelines, and patchwork state-level legislation rather than comprehensive federal AI-specific laws.[117] Unlike jurisdictions such as the European Union, the U.S. has not enacted a comprehensive AI law. Instead, it has depended on a decentralized, sector-specific regulatory strategy primarily driven by voluntary commitments from private companies and guidance from federal agencies.[118]

This approach underwent a dramatic shift with the Trump Administration's January 2025 Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence," which rescinded President Biden's comprehensive AI Executive Order 14110 titled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which outlined a comprehensive federal approach to the development, deployment, and governance of AI technologies, aiming to promote innovation while ensuring ethical, secure, and responsible use.[119] The adoption of a cautious stance towards regulation was further solidified by the inclusion of a 10-year moratorium on state AI regulation through the "One Big Beautiful Bill Act" (H.R. 1), which passed the House of Representatives in May 2025.[120] This provision would prohibit states from enforcing "any law or regulation regulating artificial intelligence models, artificial intelligence systems, or automated decision systems" for a decade, effectively nullifying existing state AI laws and preventing new ones

.

Contrastingly, state-level AI regulations have created a complex patchwork that exemplifies the federal-state tensions in American AI governance, with California, Utah, and Colorado each adopting distinct approaches that reflect their policy priorities and constituencies. The features of these models have been discussed below.

Liability in the United States, fall broadly under the tort liability regime as opposed to the statutory liability unlike India and Australia. This paper is limited to statutory liability, thus, tort liability framework falls outside its scope.

Reforms from the American Model

For this section, we analyze three States: California, Colorado and Utah, as they have enacted AI specific statutes that possess contextual relevance to liability. The Colorado AI Act has influenced other States in the context of regulation and leads as a source of legislation.[121] Similarly, the concentration of the technology industry and Silicon Valley makes the legislative approach of California critical.[122]

[117] Zartis, 'US Artificial Intelligence Regulations in 2025: A Concise Summary' (2025) <https://www.zartis.com/us-artificial-intelligence-regulations-in-2025-a-concise-summary/> accessed 1 July 2025.

[118] Tatevik Davtyan, The US Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained (9 September 2024) <https://papers.ssrn.com/sol3/Delivery.cfm/4954290.pdf?abstractid=4954290> accessed 1 July 2025.

[119] The White House, 'Removing Barriers to American Leadership in Artificial Intelligence' (Presidential Actions, 1 January 2025)<https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>; Federal Register, 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' (1 November 2023) <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence > both accessed 1 July 2025.

[120] US House of Representatives, H.R.1, 119th Congress (2025) <https://www.congress.gov/bill/119th-congress/house-bill/1/text> accessed 1 July 2025.

[121] Flaster Greenberg, 'Understanding Colorado's Landmark AI Legislation and Its Impact on Business' (2024) <https://www.flastergreenberg.com/newsroom-articles-understanding-colorado-landmark-ai-legislation-impact-business.html> accessed 1 July 2025.

[122] Mark Lemley and Bryan Casey, 'The Silicon Valley Effect' (Stanford Law School, 2024) <https://law.stanford.edu/publications/the-silicon-valley-effect/>; Cade Metz, 'California's A.I. Rules Could Be a National Model' The New York Times (14 August 2024) <https://www.nytimes.com/2024/08/14/technology/ai-california-bill-silicon-valley.html> both accessed 1 July 2025.

Value Chain Governance

The Colorado AI Act places specific duties on both developers (those who create or substantially modify AI systems) and deployers (those who use or implement these systems), requiring reasonable care to prevent algorithmic discrimination and mandating risk disclosures.[123] This structure directly recognizes the AI value chain by imposing compliance and transparency obligations on both upstream (developers) and downstream (deployers) actors, regardless of whether the AI is embedded in a traditional product or operates as a standalone service. California's regulatory framework applies to entities that create, market, or disseminate AI systems, as well as those that deploy them, and includes additional requirements for generative AI providers, such as transparency about training data and contractual obligations for watermarking AI-generated content.[124]

These requirements are aimed at both developers and providers, reflecting an explicit recognition of the AI value chain and the need for accountability at multiple stages, from creation to deployment and end use. The Utah Artificial Intelligence Policy Act focuses on generative AI, requiring providers to disclose when consumers are interacting with such systems and holding both developers and users liable for compliance with consumer protection laws. The law explicitly removes the defense of attributing liability to the AI system, ensuring that all actors in the AI value chain—from developers to deployers—are accountable for the actions and outputs of AI products.

Product and Defect Definitions for AI Systems

Under the state laws of Colorado, California, and Utah, "AI products" are generally defined within the broader framework of artificial intelligence systems, with each state adopting a functional, system-based approach rather than a product-specific one.

While none of these states use the term "AI product" in a narrow commercial sense, their laws define AI systems broadly to encompass both products and services, and they recognize the AI value chain by assigning regulatory responsibilities to both developers and deployers, ensuring accountability at every stage from creation to consumer interaction.Colorado defines an "artificial intelligence system" as any machine-based system that infers from inputs to generate outputs—such as content, decisions, predictions, or recommendations—that can influence physical or virtual environments.[125] The Colorado AI Act focuses on "high-risk" AI systems, which are those that make or substantially influence consequential decisions in areas like employment, healthcare, or finance. California uses a similar definition, describing AI as an engineered or machine-based system that, with varying autonomy, can infer from inputs how to generate outputs that influence physical or virtual environments.[126] California laws also specifically define "generative AI" as systems capable of producing synthetic content (text, images, video, audio) that emulates their training data.[127] Utah defines artificial intelligence as a machine-based system that makes predictions, recommendations, or decisions influencing real or virtual environments, and further defines "generative AI" as systems trained on data that interact with people using text, audio, or visual communication to generate non-scripted, human-like outputs with limited or no human oversight.[128]

Causation and Attribution

More recently, regulators have also attempted to evaluate the idea of a quasi-liability safe harbor for AI. In California, Senate Bill 813 proposes the establishment of Multistakeholder Regulatory Organizations MROs) — private entities which would be designated by the California Attorney General to certify the safety and compliance of AI models and applications. These certifications would serve not only as new governance benchmarks but also provide broad immunity against personal injury and property damage claims.[129]

[123] Ibid.

[124] California Assembly Bill No 2885, 'Artificial Intelligence' (2023–2024) ch 843 (approved 28 September 2024) <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2885>accessed 1 July 2025.

[125] Colorado Artificial Intelligence Act, SB 24-205 (signed into law 17 May 2024, effective 1 February 2026) <https://leg.colorado.gov/bills/sb24-205> accessed 1 July 2025.

[126] California Assembly Bill No 2885 (n 120).

[127] Ibid.

[128] Utah Code Title 13, Chapter 72, *Artificial Intelligence Policy Act* (enacted by Chapter 186, 2024 General Session, effective 1 May 2024) <https://le.utah.gov/xcode/Title13/Chapter72/C13-72_2024050120240501.pdf > accessed 1 July 2025.

[129] California SB-813. California Senate Bill 813 establishes a liability framework for AI systems through private "Multistakeholder Regulatory Organizations" (MROs) designated by the Attorney General. The bill creates a safe harbor provision that originally provided near-total civil immunity from the claims stated above for AI models and applications certified by an MRO, except in cases of intentional misconduct. Notably, however, proposed amendments would replace this immunity with a rebuttable presumption of due care for developers of certified AI systems, which could be overcome by contrary evidence. The framework requires MROs to submit comprehensive plans covering auditing approaches, risk mitigation for high-impact threats, disclosure requirements, and certification procedures. This public-private partnership approach attempts to balance innovation with safety but faces significant criticism regarding its potential to undermine liability incentives that traditionally promote safety and protect consumers.

European Union (EU)

Overview of EU's Liability Framework

Europe Union has developed a two-pronged approach to address AI-related risks and harms, combining *ex ante* obligations on AI system providers with *ex post* liability rules for damage caused by AI.[130] On the preventive side, the Artificial Intelligence Act (**AI Act**)[131] – the world's first comprehensive AI law – was formally adopted in 2024 as an EU Regulation[132], applying uniformly across Member States.[133] The AI Act takes a risk-based approach, imposing strict duties on "high-risk" AI systems (e.g. requirements for risk management, data governance, transparency, human oversight, and post-market monitoring).

On the compensatory side, the EU has overhauled its decades-old Product Liability Directive (**PLD**) to address the complexities of AI.[134] In late 2024, the EU approved a new Product Liability Directive, replacing the 1985 regime.[135] The revised PLD extends strict liability to AI and software, redefining "defect" to reflect risks from algorithmic opacity, self-learning, and evolving updates. As an EU Directive, the PLD must be transposed into national laws,[136] but it establishes harmonized rules that Member States must follow.

To complement the AI Act and PLD, the European Commission in September 2022 proposed an Artificial Intelligence Liability Directive (**AILD**)[137] aimed at easing victims' burdens in fault-based claims. The AILD was intended to ensure that individuals harmed by AI enjoy the same level of protection as those harmed by traditional technologies. It introduced uniform rules to tackle the proof difficulties posed by AI's complexity – notably, a right for claimants to seek evidence disclosure about high-risk AI systems, and a rebuttable presumption of causality linking a defendant's fault to an AI-caused harm under certain conditions. This proposal was envisioned as a sister instrument to the PLD (covering cases of fault or fundamental-rights violations by AI that fall outside strict product liability). However, after prolonged political impasse, the Commission withdrew the AILD in February 2025 due to lack of consensus and concerns about regulatory overlap.[138]

The AI Act takes a largely linear view of the AI value chain, assigning responsibility to a single entity placing the system on the market. However, in practice, AI systems often involve complex, multi-actor configurations that the current model may not fully capture.[139] Given that the AI Act and the PLD have not been fully operational, and that there is limited judicial precedent regarding their enforcement, it remains to be seen how well it captures different entities in the AI ecosystem.

[130] European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM(2021) 206 final, 21 April 2021, sections 5.2.3 and 5.6 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206> accessed 1 July 2025.

[131] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act) [2024] OJ L 212/1 <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> accessed 1 July 2025.

[132] A regulation is a legal act of the European Union which becomes immediately enforceable as law in all member states simultaneously. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

[133] European Union, 'Types of EU legislation' (European Union) <https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en> accessed 27 May 2025.

[134] European Commission, 'Proposal for a Directive on Liability for Defective Products' COM (2022) 495 final,<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>accessed 1 July 2025.

[135] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065> accessed 1 July 2025.

[136] European Union (n 129).

[137] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' COM(2022) 496 final, 28 September 2022 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496> accessed 27 May 2025.

[138] IAPP, 'European Commission Withdraws AI Liability Directive from Consideration' (2025) <https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration> accessed 1 July 2025.

[139] Christoph Busch and others, Reconciling the AI Value Chain with the EU Artificial Intelligence Act (CEPS In-Depth Analysis No 2022-03, September 2022) <https://www.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-03_Reconciling-the-AI-Value-Chain-with-the-EU-Artificial-Intelligence-Act.pdf>accessed 1 July 2025.

EU's framework for AI liability now rests on the layered combination of applying the directly applicable AI Act and the revised PLD, with national tort law filling gaps for non-product AI harms (guided by EU principles and standards). This layered regime seeks to modernize liability law for AI while balancing Member States' prerogatives in civil law.

Reforms from the European Model

Value Chain Governance

The EU model explicitly acknowledges the multiplicity of actors involved in AI systems and allocates legal responsibility across the AI life cycle. Specifically, the AI Act assigns compliance obligations to providers, users (deployers), importers, distributors, and authorized representatives of AI systems. By defining these roles and duties, EU law creates an accountability chain from development to deployment, ensuring that tasks like risk mitigation, quality control, and post-market monitoring are clearly pinned on responsible parties. The AI Act adopts a value chain approach by assigning collective responsibility to all entities involved in the development and operation of AI systems placed on the market. This contrasts with the actor-specific focus of the DSA and DMA, reflecting a more networked model of institutional accountability.[140]

Building on this, the new PLD expands the range of economic operators who can be held strictly liable for a defective AI product. Liability no longer stops at the original manufacturer. Under the revised PLD, importers, distributors, and even fulfilment service providers (e.g. e-commerce platforms handling logistics) can be liable if they make a defective AI system available in the EU market. Important, anyone who substantially modifies a product or software post-sale in a way that impacts safety is treated as a manufacturer for liability purposes. This means, for example, that an AI developer who provides software updates or machine-learning model improvements after the product's release can be held liable if those changes introduce a defect. The Directive thus matches liability with the locus of control; those who have control over AI systems risk at any stage (from coding to deployment to updating) can be accountable.

Product and Defect Definitions for AI Systems

The revised PLD expands the scope of strict liability to intangible and digital products, explicitly including software and AI systems within the definition of "product". Manufacturers (producers) remain strictly liable for defects in their products, but "defect" is now defined in a more expansive way to reflect modern technologies – a product is defective if it fails to provide the safety the public is reasonably entitled to expect, taking into account not only its design and intended use but also factors like algorithmic opacity, self-learning capabilities, and the need for software updates over time."[141] The evolving capabilities of AI systems necessitate a redefinition of 'defect' in product liability law, taking into account the shifting dynamics of control and risk awareness between manufacturers and end-users,[142] and the EU framework appears to have attempted to achieve the same.

Additionally, the EU has adapted the classic "consumer expectation" test to better fit AI.[143] The core principle remains that a product is defective if it does not provide the level of safety that the public is entitled to expect, given all the circumstances. However, the new law spells out that those circumstances include features unique to AI and software. For instance, foreseeable misuse and the product's ability to learn and adapt must be considered in assessing defect. This means a court evaluating an AI-driven product will ask not only about its design and warnings at the time of sale, but also whether the AI could evolve in a way that creates risk. If an AI system is designed to continuously improve (e.g. through machine learning) but lacks proper safeguards to prevent it from "learning" dangerous behaviors, that could be deemed a defect in design or lack of safety.

Causation and Attribution

Recognizing that AI's complexity can make it exceptionally hard for victims to pinpoint how and why harm occurred, the EU has introduced novel procedural tools to ease claimants' evidentiary burden.[144] Under the revised PLD, courts have new powers to help bridge the information asymmetry between AI developers and those harmed

[140] Anna Beckers, 'Global Value Chains in EU Law' (2023) 42 *Yearbook of European Law* 322 <https://doi.org/10.1093/yel/yead010> accessed 1 July 2025.

[141] Under liability law to encompass the realities of AI systems. Under the new PLD, the term *product* now explicitly includes software and digital intangibles – such as computer programs, applications, operating systems, and AI models – regardless of whether they are embedded in a physical device or provided as a cloud service.

[142] Buiten (n 74).

[143] Ibid.

[144] European Parliamentary Research Service, Artificial Intelligence Liability in the EU: Study (Study 762861, 2024) <https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf>accessed 1 July 2025.

by AI.[145] First, injured persons can request disclosure of relevant technical information from manufacturers to help substantiate a claim.[146] If, for example, an autonomous vehicle's AI malfunctioned, a court may compel the producer to supply logs, data, or design records necessary to prove a defect – a significant change in a legal tradition that previously had no discovery process in many EU countries.[147]

The law balances this by requiring that requests be specific and proportionate, and it protects trade secrets during disclosure.[148] Crucially, if a manufacturer unjustifiably refuses to provide evidence that a court deems necessary, the PLD empowers courts to presume that the product was defective. In other words, stonewalling now backfires, and lack of transparency can trigger an adverse inference that the AI system had something wrong with it.[149]

Beyond evidence disclosure, the PLD establishes rebuttable presumptions to help prove defect and causation in AI cases.[150] If a claimant can show that an AI product violated a mandatory safety standard (for instance, it failed to meet requirements set by the AI Act or other regulations), or that it exhibited an obvious malfunction during normal use, then the court will presume the product was defective without requiring further proof.[151] These presumptions directly tackle scenarios where AI failures might be evident (e.g. a delivery drone suddenly falls from the sky) but the underlying technical flaw is difficult to explain – the law spares the victim from needing an exact root-cause analysis by shifting the onus to the producer to prove the product was *not* defective.[152] Similarly, once a defect is established, if the resulting harm is of a kind typically associated with that defect, the law allows a presumption of causality between the defect and the damage.[153] For example, if a healthcare AI system has a proven defect in its diagnostic algorithm and a patient suffered an injury that is consistent with that kind of diagnostic error, the court can presume the defect caused the injury. This spares claimants from the nearly impossible task of retracing an AI's complex decision process to link cause and effect.

It is worth noting that the (now-abandoned) AILD would have provided similar procedural mechanisms for fault-based tort claims beyond the product liability sphere.[154] The AILD had proposed that if a claimant proved that an AI system's operator or provider violated a duty of care – for example, breached an AI Act obligation like transparency or human oversight – and that this likely contributed to the harm, the court would presume a causal link between the breach and the AI's output (or failure to output) that caused damage.[155] This presumption of fault-based causation, coupled with the AILD's own disclosure provisions, was designed to make negligence and anti-discrimination claims involving AI more viable by alleviating the proof of the exact algorithmic causal chain.[156] Although the directive will not proceed, its spirit survives in the PLD's overlapping presumptions and in the broader legal discourse.

[145] Giulia Gentile, 'AI Liability After AILD Withdrawal: Why EU Law Still Matters' (Oxford Business Law Blog, 17 April 2025)<https://blogs.law.ox.ac.uk/oblb/blog-post/2025/04/ai-liability-after-aild-withdrawal-why-eu-law-still-matters >accessed 1 July 2025.

[146] Ibid.

[147] Ibid.

[148] Ljupcho Grozdanovski, 'My AI, My Code, My Secret – Trade Secrecy, Informational Transparency And Meaningful Litigant Participation Under The European Union's AI Liability Directive Proposal' (2025) *56 Computer Law & Security Review* 106117 <https://www.sciencedirect.com/science/article/abs/pii/S0267364925000123> accessed 1 July 2025.

[149] Ibid.

[150] Miriam Buiten, Alexandre de Streel and Martin Peitz, 'The Law and Economics of AI Liability' (2023) 48 *Computer Law & Security Review* 105794 <https://www.sciencedirect.com/science/article/pii/S0267364923000055> accessed 1 July 2025.

[151] Ibid.

[152] Ibid.

[153] Ibid.

[154] Gentile (n 140).

[155] Ibid.

[156] European Parliamentary Research Service (n 140).

6. Proposed Considerations for Reforming India's AI Liability Regime

A Review of Control as a Feature of Indian Liability Law

This paper has argued that India's existing legal framework may be ill-equipped to address the liability challenges posed by artificial intelligence (AI). As AI systems become more autonomous, data-driven, and multi-actor in nature, traditional models of liability - rooted in clear causation, manufacturer-defined responsibility, and static products, begin to unravel. Through comparative engagement, we have explored how other jurisdictions are attempting to fill these gaps. However, these efforts remain partial. No jurisdiction provides a fully coherent liability framework for AI systems, even where legislative reform is advanced.[157]

Nonetheless, the European Union's approach, particularly through the Revised Product Liability Directive and the Artificial Intelligence Act - marks a shift toward aligning liability with actors that exercise factual control over AI systems.[158] These instruments redefine roles across the AI value chain and provide procedural innovations like rebuttable presumptions, evidence disclosure rights, and product definitions inclusive of software.[159] Both Japan and Australia also seemingly recognize the value-chain approach to governance, indicating its usefulness.

An explicit recognition of the unique characteristics of the AI value chain is essential to ensure a consistent and equitable application of control-based liability regimes. Uniform implementation is particularly important to avoid unduly burdening actors, such as AI manufacturers, who may have minimal or no causal connection to the resulting harm. Imposing strict liability on such entities could have a chilling effect on innovation, discouraging manufacturers from engaging in the development of AI technologies.[160] Moreover, it important to consider the potential downstream impact of attribution of liability to manufacturers, especially when they are not involved in model training.[161] Holding manufacturers liable when they are not involved in training the AI highlights the need for a tailored approach to assigning responsibility in the AI industry.

Isomorphic mimicry of foreign statutes risks importing institutional assumptions that may not suit Indian regulatory realities, such as strong *ex ante* oversight or technical capacity for detailed algorithmic audits. Instead, we propose a conceptual shift: India may consider a move toward a more defined control-based theory of liability, where legal responsibility corresponds to the degree of influence and control exercised at various points in the AI lifecycle. This approach can borrow high-level principles from the EU model: such as role-differentiation, rebuttable presumptions, or layered risk classification, but must be supplemented by indigenous design choices suited to Indian conditions.[162]

This shift may offer a limited but practical response to two persistent challenges in AI liability. First, it may help structure value-chain governance by aligning responsibility with the actual role and influence of each actor, thereby allowing liability to be distributed more proportionately across developers, deployers, and other participants. Second, in environments where causation is difficult to trace, due to autonomous behavior, data-driven evolution, or system complexity - control could serve as a workable proxy. This would been curating a standard of control which identifies its locus and conveys its meaning to all stakeholders in the ecosystem, taking it beyond the notions currently present in the CPA as noted earlier. While not a complete substitute, tethering liability to control in a more defined manner may help approximate responsibility by focusing on which actors were best positioned to prevent or mitigate harm. In doing so, the approach may enable a more balanced and context-sensitive allocation of legal accountability *(Refer Illustration 7)*.

Clarifying the Meaning of Product and Defect

A central issue in applying traditional product liability frameworks to artificial intelligence is the inadequacy of legacy definitions of "product" and "defect." These definitions were originally designed for static, tangible goods, and struggle to accommodate the layered, adaptive, and software-

[157] Christiane Wendehorst and Reiner Schulze, 'Liability for Artificial Intelligence and EU Consumer Law' (2022) *Journal of European Consumer and Market Law.*

[158] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) *Computer Law Review International.*

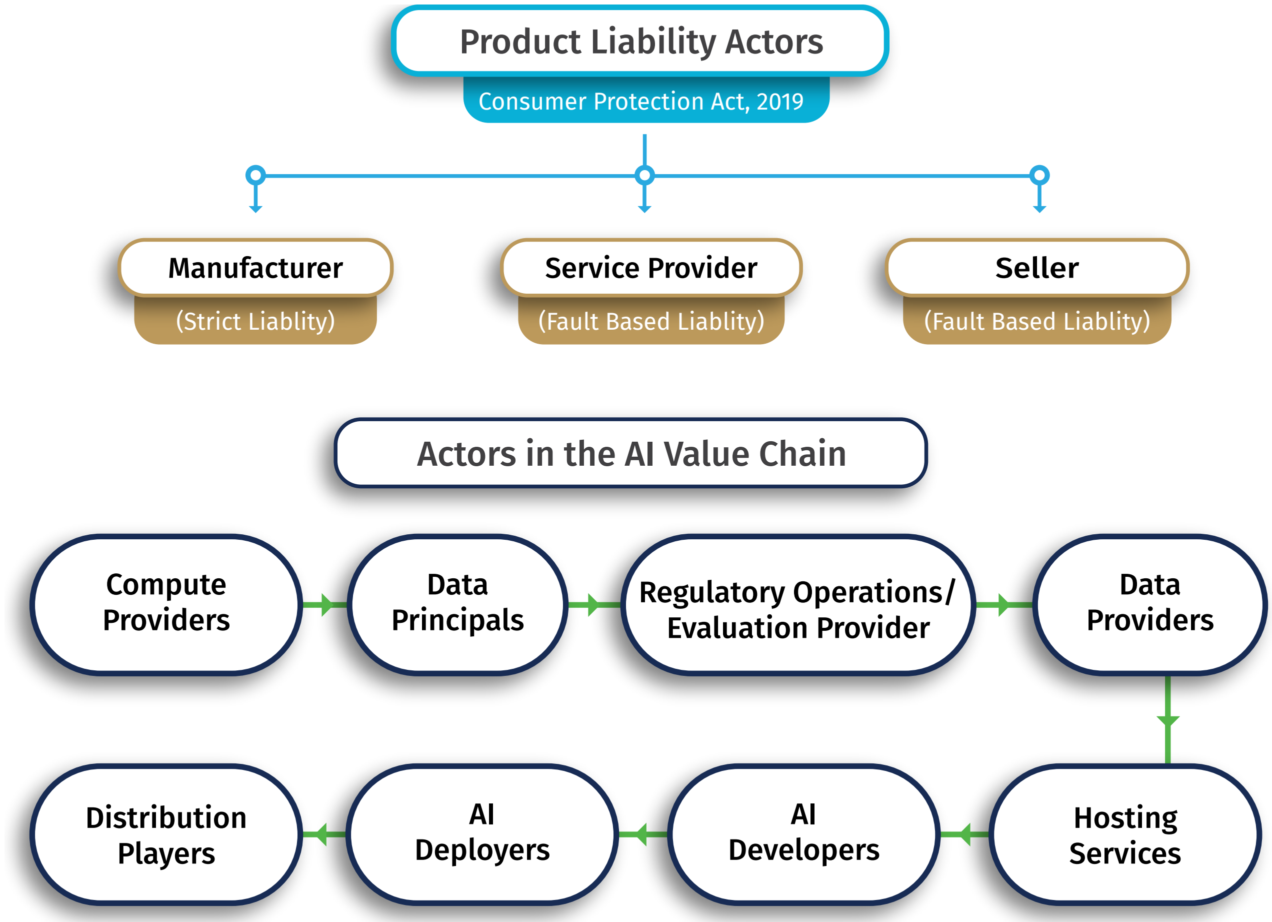
[159] European Commission (n 130).

[160] See generally, Kathryn E Spier and Rory Van Loo, *Foundations for Platform Liability* (2025) https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=5016&context=faculty_scholarship.; British Columbia Law Institute, *Report on Artificial Intelligence and Civil Liability* (April 2024) https://www.bcli.org/wp-content/uploads/Report-AI-and-civil-liability-final.pdf.

[161] Alberto Galasso and Hong Luo, *When Does Product Liability Risk Chill Innovation? Evidence from Medical Implants*, NBER Working Paper No 25068 (National Bureau of Economic Research, September 2018) https://www.nber.org/system/files/working_papers/w25068/w25068.pdf.

[162] Elements of a control-based liability framework do exist within Indian law. The CPA, for instance, refers to a product seller's "substantial control" over inter alia, designing, testing, or manufacturing the product in determining their liability, suggesting some level of recognition of control as a relevant legal standard. Consumer Protection Act 2019, s 86(a).

Illustration 7: Actors in the AI Value Chain vs. Entities recognized under the CPA



integrated nature of modern AI systems. Under Indian law, the CPA, 2019 continues to adopt a conventional conception of a product as a finished good, manufactured or assembled by a clearly identifiable entity.[163] The concept of a "defect" under the Indian consumer protection law is more focused on well-established risks and engages minimally with the novel capabilities of AI. Such criteria may be ill-suited to address algorithmic failures, statistical biases, or harms resulting from autonomous decision-making.[164] It also may lead to tension between the evolution of defects vis-a-vis harm under the Act.

The revised Product Liability Directive in the European Union responds to this challenge by expanding the definition of "product" to explicitly include software, including standalone digital products and embedded code.[165] Further, it introduces a broader understanding of "defect" that includes not only physical malfunction but also failure to perform safely as persons are generally entitled to expect, including in cases involving data-driven or probabilistic harms.[166] These changes aim to reflect the evolving risk environment associated with AI, particularly where harm may arise from algorithmic opacity, autonomous decision-making, or unforeseen interactions between subsystems.[167]

Drawing from the EU's expanded definitions, India may consider developing a layered understanding of digital

[163] *Consumer Protection Act 2019*, s 2(34);Statement of Objects and Reasons – CPA 1986 focused on traditional goods, and did not even have a dedicated product liability regime expressly – and claims were decided on existing definitions of 'defect' and 'deficiency in service' < https://ncdrc.nic.in/bare_acts/consumer%20protection%20act-1986.html> ;
Statements of Objects and Reasons – CPA 2019 focused largely on harms arising from conventional goods and services, and even focused the newly introduced product liability regime for them < https://prsindia.org/files/bills_acts/bills_parliament/2019/THE%20CONSUMER%20PROTECTION%20BILL,%202019%20Bill%20Text.pdf > both accessed 1 July 2025.

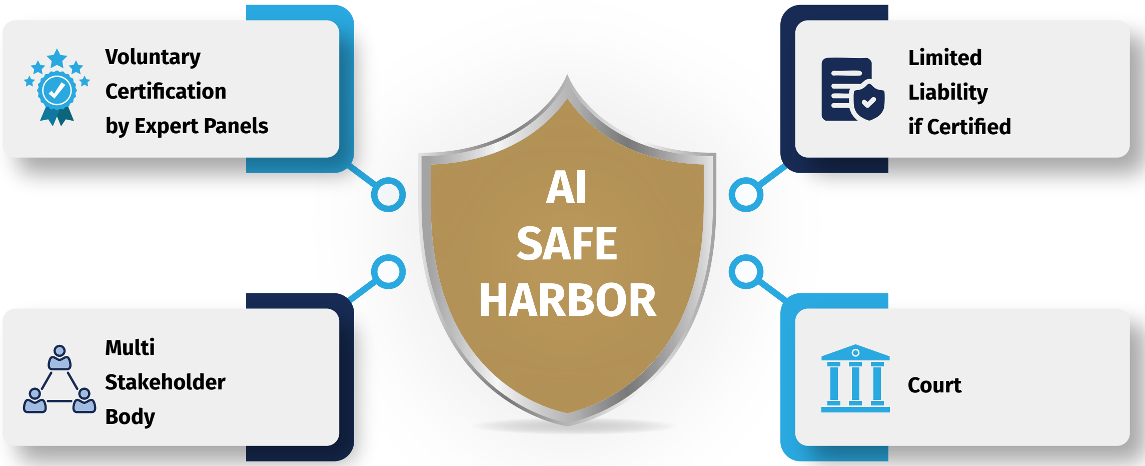
[164] Daniel F Llorca and others, 'Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof' (2023) 76 *Journal of Artificial Intelligence Research* 613.

[165] European Commission, 'Proposal for a Directive on Liability for Defective Products' COM(2022) 495 final, art 4.

[166] *ibid* art 6 (broadening "defect" to include failure to meet safety expectations under ordinary use).

[167] Wendehorst and Schulze (n 153).

Illustration 8: A pathway for AI Safe Harbour


Voluntary Certification by Expert Panels
Limited Liability if Certified
AI SAFE HARBOR
Multi Stakeholder Body
Court

Public-private Model to Manage AI Risk Without Overregulation

products that includes software, models, and datasets, and a broader concept of defect that factors in algorithmic opacity, adaptive behavior, and loss of expected safety.[168] Any amendments must, however, be consistent with the letter and spirit of Indian product liability law, and not unreservedly expand its scope to address harms identified in a European context.

Liability Safe Harbor (Refer Illustration 8)

California SB 813 introduces a "certification shield" framework that provides AI developers with an affirmative defense against certain civil liability claims when their systems receive certification from approved Multistakeholder Regulatory Organizations (MROs).[169] Rather than imposing direct government regulation, SB 813 establishes an innovative public-private governance model where independent third-party panels of AI experts and academics create workable safety standards while fostering innovation.[170] This model creates a "AI safe harbor" for AI systems that comply with private body standards ensuring that the standards are up-to-date with the novel changes in technology.

India may wish to study the feasibility of adopting a similar public-private partnership approach as an alternative to purely regulatory frameworks, building on its existing strengths in collaborative AI development. This approach fosters greater collaboration on understanding AI risk and complements any high-level regulation (such as legislation) that the government may wish to undertake going forward.

Unsolved Questions

Any Indian framework emerging from this discussion will necessarily remain provisional and subject to refinement. Several foundational questions, such as how to apportion liability across multiple actors in the AI value chain or how to attribute harm caused by autonomous or adaptive behavior, remain unsettled even in mature legal systems. Instruments like the proposed EU AILD have attempted to ease the burden of proof by introducing rebuttable presumptions of causation and fault. However, these procedural innovations have not fully resolved the underlying challenge: AI systems often operate as opaque, data-driven technologies whose decision-making logic may not be fully explainable, even to their developers. In such cases, proving causal links between input, system behavior, and harm becomes inherently uncertain, and judicial reliance on presumptions or probabilistic reasoning may still fall short of legal clarity.

Moreover, there exists an inherent tension between the goals of innovation and regulation. Overly rigid liability regimes may stifle AI development by deterring experimentation and discouraging small developers or

[168] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) *Computer Law Review International*.

[169] California Senate Bill 813, Artificial Intelligence Liability Framework (2023–2024) <https://legiscan.com/CA/text/SB813/id/3191116> accessed 1 July 2025.

[170] Law and AI, 'Comments on the Draft Report of the Joint California Policy Working Group on AI Accountability' (2024) <https://law-ai.org/comments-on-draft-report-of-joint-california-policy-working-group/>; Pillsbury Law, 'California SB 813 Introduces AI Development Certification and MRO Oversight' (2024) <https://www.pillsburylaw.com/en/news-and-insights/california-sb813-ai-development-certification.html> both accessed 1 July 2025.

startups from entering the market. On the other hand, weak or underdeveloped liability standards risk eroding public trust and leaving victims without effective remedies. Striking the right balance is especially difficult in rapidly evolving domains, where both technological capabilities and social risks are still being understood.

In India, these questions are further complicated by institutional constraints such as uneven judicial capacity, limited access to technical expertise, and sector-specific regulatory gaps. While India may draw useful lessons from global frameworks, its liability model must account for domestic realities, particularly the need for accessible dispute resolution, harmonization with sectoral regulators, and scalable enforcement mechanisms. The immediate task is not to design an exhaustive liability framework, but to articulate a coherent foundational model that places control and causal contribution across the AI value chain at its core, while leaving space for future refinement through jurisprudence, sectoral codes, and regulatory experimentation.

Finally, such a model must be capable of addressing not just abstract liability but concrete doctrinal concerns. For instance, current tools may fall short when it comes to defining a “product” or “defect” in relation to software systems or assessing performance variability across different user environments. Without the ability to evaluate risk thresholds and contextualized safety expectations, traditional legal categories may prove inadequate in capturing the full range of AI harms. Bridging these conceptual gaps will require iterative legal innovation, guided by evolving jurisprudence and grounded in local institutional practice.

7. A Specialized, Phased AI Dispute Resolution Framework in India

Technology is increasingly influencing justice functions without the accountability or public interest duties that bind courts. This blurring of boundaries raises concerns about whether traditional legal institutions remain equipped to protect rights in the digital era, especially in disputes involving AI or content moderation.[171] Given the complexity of proving harm or liability in relation to AI as discussed in Section 4 of this paper, conventional courts may be ill-equipped to resolve AI disputes without specialized procedural support.

Adding to this complexity is a notable judicial capacity gap. Legal education and judicial experience typically do not cover the architecture of machine learning models or the statistical nature of their outputs. As a result, judges may lack the tools to interpret algorithmic logic or to distinguish between legitimate and flawed expert testimony. This lack of fluency increases the risk of legal misapplication, especially in disputes where technical details are central to determining liability or due process.

Compounding these challenges is the issue of evidence asymmetry. In most AI disputes, the relevant information such as the algorithm's source code, training datasets, model parameters, and decision logs remains with the developer or deploying entity. Plaintiffs, especially individuals or small entities, are often unable to access this proprietary data even when it is crucial to establishing fault or causation.[172] This imbalance makes it disproportionately difficult for claimants to succeed, potentially undermining access to justice.[173] Together, these challenges highlight the need for a tailored dispute resolution framework that addresses AI-specific complexities through institutional and procedural innovation.

Insights from Regulatory Pathways: Institutional Lessons for AI Dispute Resolution

Integrating Technical Expertise into Dispute Resolution

India has a well-established tradition of constituting specialized adjudicatory bodies for domains that demand subject-matter expertise. Institutions such as the National Company Law Tribunal (NCLT), the National Green Tribunal (NGT), and the erstwhile Intellectual Property Appellate Board (IPAB) exemplify this approach. These bodies combine judicial officers with technical members to enhance decision-making in complex areas. The Supreme Court has also upheld the validity of such hybrid arrangements, provided that judicial independence is preserved.[174] Even within ordinary courts, mechanisms for integrating technical support exist. For instance, the Patents Act, 1970[175] allows courts to appoint scientific advisers in patent cases to investigate and report on technical matters, a practice frequently relied upon in high-stakes patent litigation. Further, certain regulatory bodies have begun addressing AI-related risks within their sectoral mandates. Regulators such as SEBI and RBI have issued sector-specific norms, including SEBI's guidance on algorithmic trading systems aimed at enhancing transparency and auditability as discussed in Section 3 of this paper.

The IPAB experience

The experience with the IPAB offers instructive lessons for future AI adjudication. The IPAB was established under the Trade Marks Act, 1999[176] and later received jurisdiction over patents and geographical indications via amendments to the Patents Act, 1970 and the Geographical Indications of Goods (Registration and Protection) Act, 1999. It was conceived as a specialist tribunal comprising one Judicial Member and one Technical Member to expedite the resolution of technically complex IP cases. Appeals from decisions of the Patent Office[177] and Trademark Registry[178] were routed to the IPAB. Upon notification, even pending High Court matters were transferred to the IPAB. Though judicial review remained available under Articles 226 and 136 of the Constitution, the IPAB served as the central appellate forum for IP disputes.[179]

Despite this structure, the IPAB encountered serious implementation hurdles. Chronic vacancies and

[171] N Helberger, 'The rise of technology courts, or: How technology companies re-invent adjudication for a digital world' (2025) 56 Computer Law & Security Review 106118, 6, 9

[172] J Metcalf, R Singh, E Moss, E Tafesse and EA Watkins, 'Taking algorithms to courts: A relational approach to algorithmic accountability' in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (2023) 1450, 1457 (section 4.1)

[173] A Deeks, 'The judicial demand for explainable artificial intelligence' (2019) 119(7) Columbia Law Review 1829, Part III

[174] L. Chandra Kumar versus Union of India and Ors, 1997; Union of India vs R. Gandhi and Ors., 2010 (261) ELT3 (S.C.), Supreme Court of India

[175] The Patents Act 1970, s 115.

[176] Trade Marks Act 1999, s 83.

[177] Patent Act 1970, s 117A.

[178] Trade Marks Act 1999, s 91.

[179] *L. Chandra Kumar versus Union of India and Ors* 1997 (3) SCC 261.

procedural inefficiencies undermined its intended efficiency. Constitutional concerns of dampening judicial review further weakened its functioning. In *Shamnad Basheer v. Union of India*,[180] the Madras High Court struck down provisions that allowed non-judicial appointees to hold key posts, finding them violative of separation of powers, independence of judiciary and basic structure of the Constitution. Ultimately, the IPAB was abolished under the Tribunals Reforms Act, 2021 and its jurisdiction was transferred back to the High Courts.[181] Some High Courts, notably the Delhi High Court, responded by establishing dedicated IP benches to retain the benefits of subject-matter expertise within the conventional judiciary.[182]

These developments offer both a cautionary tale and a potential template. A future AI dispute forum must carefully navigate structural and constitutional concerns. Learning from both the strengths and failures of the IPAB, policymakers should consider carefully structured mechanisms that combine domain expertise, technological adaptability, and constitutional safeguards.

The Approach

The examples discussed above outline the deep challenges involved in justifying a bespoke AI court for India. Less discussed, but equally pertinent, is the history of substantive law that animated standalone tribunals. Almost always, specialized courts were preceded by a comprehensive law on the subject; the IPAB, for instance, adjudicated matters related to IP law.[183]

Contrastingly, India lacks a comprehensive AI law.[184] This absence does not diminish the need to address AI governance comprehensively, but it does support a phased strategy to establishing dispute resolution mechanisms that solve for the challenges discussed while avoiding the pitfalls of premature tribunalization. This phased strategy would involve solving four problems: enable addressing AI governance questions across India's fragmented AI law framework to develop interoperable jurisprudence, navigate concerns around a legislative basis for an AI court, and identify applicable legal principles (including those derived from common law) for broad-based AI governance.

Accordingly, we recommend, for consideration, a phased and proportionate approach. This approach begins with the

[180] *Shamnad Basheer v Union of India* W.P. No. 1256 of 2011 (Madras HC).

[181] Ragini Shah, 'The Tribunals Reform Ordinance, 2021 Abolishes IPAB In An Effort To "Streamline" Tribunals' (LiveLaw, 16 April 2021) https://www.livelaw.in/law-firms/articles/the-tribunals-reform-ordinance-ipab-streamline-tribunals-172664 accessed 22 July 2025.

[182] The Intellectual Property Division of the Delhi High Court is a specialized bench established under the Delhi High Court Intellectual Property Rights Division Rules, 2022, dedicated to handling matters relating to patents, trademarks, copyrights, and other IP statutes. *Delhi High Court*, 'Delhi High Court Intellectual Property Rights Division Rules, 2022' (Notification No 13/Rules/DHC, 24 February 2022) (corrected 11 April 2022) https://delhihighcourt.nic.in/files/Notifications%20and%20Practice%20Directions/notificationfile_wd6kndkfb4g.pdf accessed 22 July 2025.

[183] Patents Act, 1970, Trade Marks Act, 1999, Copyright Act, 1957, and Geographical Indications of Goods (Registration and Protection) Act, 1999.

[184] The forthcoming Digital India Act may eventually provide this foundation, but until its contours are fully known, any such move may be premature. 'Upcoming Digital India Act to curb high-risk AI, misinformation: Centre' Business Standard (23 May 2023) https://www.business-standard.com/india-news/upcoming-digital-india-act-to-curb-high-risk-ai-misinformation-centre-123052300473_1.html accessed 22 July 2025.

creation of dedicated AI benches within existing High Courts or sectoral forums, supported by technical experts.[185] Over time, and in step with the development of statutory and doctrinal clarity, this can evolve into a specialized AI court. This model draws from the lessons of the IPAB experience, balances innovation with institutional prudence, and allows for adaptability as India's AI regulatory ecosystem matures.

In the *first phase*, existing judicial forums may be retrofitted to accommodate AI-related disputes. This may be achieved by establishing dedicated benches on AI and emerging technologies within High Courts or by expanding the mandate of existing IT-focused benches to include AI. These benches should be supported by a structured mechanism for drawing on technical expertise. A precedent already exists in Section 115 of the Patents Act, 1970, which allows courts to appoint scientific advisers. A similar framework could be designed for AI experts, who may assist judges in interpreting algorithmic decisions, evaluating causal chains, or reviewing technical documentation, without compromising the neutrality of the adjudicatory process.

In the *second phase*, in the wake of the legal ecosystem around AI liability maturing through statutory development (such as under the Digital India Act) and regulatory guidance, a specialized AI court may be considered. Such a court could be authorized to hear appeals or references from sectoral regulators like the Central Consumer Protection Authority (CCPA), the Telecom Regulatory Authority of India (TRAI), or the RBI, thereby aggregating adjudicatory expertise without duplicating institutional capacity. This transition would require clear articulation of jurisdiction, composition, and procedural norms, drawing on the structural learnings from both the IPAB and sectoral adjudication models.[186]

[185] Perhaps, a single bench may be initially created at one High Court, as a form of sandbox.

[186] It must be noted that this paper does not address the detailed design of such dedicated benches. Critical questions relating to their composition, the mode and term of appointment of technical experts, training requirements, procedural safeguards, and the institutional mechanisms necessary to ensure accountability and impartiality are beyond the present scope. These design considerations will require separate and sustained policy attention as India's AI governance framework evolves.

8. Conclusion

This paper examines the urgent need to rethink India’s legal approach to liability for harms caused by artificial intelligence (AI) systems. It identifies three key gaps in the current framework: the absence of legal recognition for multiple actors in the AI value chain, unclear definitions of “product” and “defect” in relation to AI systems, and the lack of effective procedures for proving causation. Drawing on lessons from the European Union, the United States, Australia, and Japan, the paper presents conceptual solutions to these issues that are rooted in legal doctrine.

These solutions aim to ensure that responsibility is assigned based on actual control and influence, supporting both innovation and accountability. However, the paper does not propose specific laws or mechanisms for implementation.

The choice of legal instruments, whether through new legislation, regulatory action, or judicial interpretation, will be developed in future work. As AI systems become more widespread and impactful, India will need a liability framework that provides legal clarity, accounts for the technical complexity of AI, and ensures fairness for all stakeholders involved.

Authors

This report has been authored by the following members from Shardul Amarchand Mangaldas & Co.

Dr. Shardul S. Shroff
Executive Chairman

KS Roshan Menon
Principal Associate

Vishwajeet Deshmukh
Associate

In addition to the authors above, former Research Fellow **Anmol Bharuka** also contributed to this report in the capacity of an author.

Disclaimer
This publication has been prepared by Shardul Amarchand Mangaldas & Co. ("SAM & Co.") for general informational purposes only and does not constitute legal, tax, financial or any other professional advice. The information has been compiled from sources believed to be credible; however, it is provided on an "as is" basis without any representation or warranty, express or implied, as to its accuracy or completeness, and SAM & Co. shall not be liable for any loss arising from reliance on this publication. Readers are advised to seek appropriate professional advice before taking any action.

All images used in this publication have been sourced from www.freepik.com and are used for illustrative purposes only.

OUR OFFICES: NEW DELHI | MUMBAI | GURUGRAM | BENGALURU | CHENNAI | AHMEDABAD | KOLKATA