

Artificial Intelligence, Consumer Harm, and Tort Liability: Emerging Legal Challenges in India

Shibanee Acharya^{1*}, Ashish Kumar Mishra², Omkar Acharya³

¹Department Research Fellow, PG Department of Law, Fakir Mohan University,
Balasore – 756019, Odisha, India

²Advocate, Orissa High Court

³LL.M. Student, PG Department of Law, Fakir Mohan University,
Balasore – 756019, Odisha, India

**Address for Correspondence*

Abstract

Artificial Intelligence has transformed the delivery of goods and services across sectors such as healthcare, finance, e-commerce, transportation, insurance, and digital platforms. AI-driven technologies offer significant benefits by enhancing efficiency, accuracy, and consumer convenience. However, their increasing integration into consumer markets has also created new forms of harm arising from algorithmic errors, autonomous decision-making, biased outcomes, privacy violations, cybersecurity breaches, and product malfunctions. These developments challenge the traditional principles of tort law, which are primarily based on human fault, foreseeability, causation, and liability. The autonomous and opaque nature of AI systems complicates the identification of responsible parties, raising critical questions regarding the liability of developers, manufacturers, service providers, platform operators, and users.

This study examines the emerging legal challenges associated with AI-induced consumer harm in India through the lens of tort law. It critically analyses the applicability of established tort principles, including negligence, strict liability, product liability, vicarious liability, and duty of care, in addressing harms caused by intelligent and autonomous systems. The research further explores the interaction between tort law and the Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and evolving regulatory initiatives concerning AI governance. Comparative perspectives from jurisdictions such as the European Union, the United Kingdom, and the United States are also examined to identify best practices and potential reforms.

Adopting a doctrinal and analytical research methodology, the study evaluates statutory provisions, judicial decisions, policy documents, and scholarly literature to assess whether the existing Indian legal framework adequately protects consumers affected by AI-related harms. The research identifies significant gaps in accountability, transparency, explainability, causation standards, and compensation mechanisms, particularly where AI systems operate with substantial autonomy.

The study concludes that India's current tort framework requires substantial adaptation to effectively respond to AI-enabled consumer injuries. It recommends the development of AI-specific liability

principles, enhanced regulatory oversight, mandatory transparency and explainability obligations, clearer allocation of responsibility among AI stakeholders, compulsory risk assessment for high-risk AI applications, and stronger consumer redress mechanisms. By proposing a balanced framework that promotes technological innovation while safeguarding consumer rights, this research contributes to the evolving discourse on AI governance and tort liability in India.

Keywords: Artificial Intelligence, Consumer Harm, Tort Liability, Negligence, Product Liability, Consumer Protection, Algorithmic Bias, Digital Personal Data Protection, AI Governance.

1. Introduction

Early AI research focused on robots in manufacturing and the implications of robotization for industrial development.¹ The focus subsequently shifted to decision support systems that enabled data-driven decision-making from voluminous business data using AI-based techniques. AI has evolved from rule-based systems following explicit instructions to models leveraging massive datasets and powerful computing to exhibit human-like cognitive functions.² AI demonstrates features of general-purpose technologies, generating and accelerating further innovations across sectors. The pattern of AI technology development shows similarity to the emergence of major technological paradigms in the past, suggesting AI may generate a paradigmatic shift. AI patenting accelerated and became more pervasive between 2000 and 2016, with innovators shifting from ICT core industries to non-ICT service sectors.³ Generative AI represents a watershed moment, enabling autonomous generation of novel outcomes with significant implications for platform value creation and stakeholder interactions.⁴

1.1 Background of the Study

Businesses exploit AI to offer personalized experiences, support purchase activities, and manage post-purchase services. Four dominant mechanisms through which AI influences consumer decisions are personalization and recommender systems, predictive analytics, dynamic pricing, and AI-enabled customer service.⁵ Over 77% of Indian startups invest in advanced technologies including AI, machine learning, and IoT to achieve operational efficiency and enhance customer experiences.⁶ AI-powered solutions have made financial services more accessible and efficient, particularly for underserved

¹ Dwivedi, Y. K., Sharma, A., Rana, N. P., Giannakis, M., Goel, P., & Dutot, V. (2023). Evolution of artificial intelligence research in Technological Forecasting and Social Change: Research topics, trends, and future directions. *Technological Forecasting and Social Change*. <https://doi.org/10.1016/j.techfore.2023.122579>

² Vinothkumar, J., & Karunamurthy, A. (2023). Recent Advancements in Artificial Intelligence Technology: Trends and Implications. *Quing: International Journal of Multidisciplinary Scientific Research and Development*. <https://doi.org/10.54368/qijmsrd.2.1.0003>

³ Damioli, G., Van Roy, V., Vértessy, D., & Vivarelli, M. (2024). Is artificial intelligence leading to a new technological paradigm?. *Structural Change and Economic Dynamics*. <https://doi.org/10.1016/j.strueco.2024.12.006>

⁴ Wessel, M., Adam, M., Benlian, A., Majchrzak, A., & Thies, F. (2025). Generative AI and its Transformative Value for Digital Platforms. *Journal of Management Information Systems*, 42, 346 - 369. <https://doi.org/10.1080/07421222.2025.2487315>

⁵ Sunmola, P. T. (2026). Artificial Intelligence and Consumer Decision-Making in Business Administration: A Systematic Literature Review and the Enhanced TTG Framework. *International Journal of Business Administration*. <https://doi.org/10.5430/ijba.v17n1p83>

⁶ Khullar, S., Joshi, M., & Devi, P. (2025). AI for Startups in India: Pathways to Innovation and Competitiveness. *International Journal of Science and Research Archive*. <https://doi.org/10.30574/ijrsra.2025.16.3.2620>

populations, with UPI processing over 15 billion transactions monthly by August 2024.⁷ AI-driven micro-lending platforms like Capital Float and Aye Finance address a \$380 billion credit gap by assessing creditworthiness using alternative data.

Indian brands across e-commerce, fintech, and consumer goods deploy AI-based chatbots, recommendation engines, and sentiment analysis tools to tailor interactions. Flipkart uses AI algorithms for dynamic product recommendations while HDFC Bank employs AI for customer service automation.⁸ AI-driven productivity growth in modern services operates as a general-purpose technology, generating sizeable GDP gains with relatively stronger welfare effects for rural and lower-income households. Urban areas lead in AI-enabled consumer product adoption due to established infrastructure, while rural regions lag behind due to limited infrastructure and lower awareness.⁹

AI's rapid deployment in consumer contexts raises persistent risks including algorithmic bias, limited transparency, perceived unfairness, and potential erosion of consumer autonomy. As AI's ability to operate on behalf of users improves and data collection increases, the visibility and awareness of AI decreases, creating a paradox where more convenience equates to more substantial privacy risks.¹⁰ Informational asymmetry between consumers and businesses means consumers require protection, as the caveat emptor principle no longer applies to AI-mediated commercial practices.¹¹ When consumer distrust of algorithmic systems becomes widespread, it can compromise institutional legitimacy and the infrastructure of AI-supported services.¹²

1.2. Review of Literature

India's legal framework for AI-related consumer harm is nascent, with no specific AI liability law enacted and existing statutes providing only indirect coverage (Pai, 2024).¹³ The global literature converges on a central tension: traditional tort law concepts of fault, defect, and causation fit poorly with AI's autonomy, opacity, and unpredictability, leaving consumers who suffer harm with considerable evidentiary burdens (Scherer, 2015).¹⁴

India has no specific law governing AI, and the predominant existing framework—the Information Technology Act of 2000 predates AI and addresses cyber security, data protection, and electronic records only tangentially. The NITI Aayog's National Strategy for AI, released in 2018, serves as a development roadmap rather than a binding regulatory document and does not provide concrete guidelines on liability management. India's Patents Act expressly exempts algorithms from patent eligibility, which may

⁷ Das, S. K. (2024). Bridging India's Financial Divide: The Power of Artificial Intelligence and Machine Learning. *International Journal For Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2024.v06i05.29801>

⁸ Patil, L. P., & Patil, A. L. (2025). Artificial Intelligence in Marketing: Transforming Consumer Engagement & Personalization. *European Economic Letters (EEL)*. <https://doi.org/10.52783/eel.v15i3.3496>

⁹ Addy, M., Rasheed, D., & Patnaik, R. (2025). Emergence of Intelligent Systems in Consumer Products: Strategic Impacts and Opportunities in India. *International Journal of Accounting and Economics Studies*. <https://doi.org/10.14419/59bxn151>

¹⁰ Menard, P., & Bott, G. J. (2024). Artificial intelligence misuse and concern for information privacy: New construct validation and future directions. *Information Systems Journal*, 35, 322 - 367. <https://doi.org/10.1111/isj.12544>

¹¹ Fekete, O. (2025). Should We be Afraid of AI-based Manipulation? Consumer Protection in the Shadow of Artificial Intelligence. *Comenius : Bratislava legal forum*. <https://doi.org/10.46282/bpf.2025.21>

¹² Zheng, Z., Tan, Q. L., Zheng, X., & Yang, Y. (2025). The Dark Side of AI in Insurance: A Systematic Review of Mechanisms Linking AI Design Features to Consumer Harm. *Journal of Consumer Affairs*. <https://doi.org/10.1111/joca.70034>

¹³ Pai, S. N., Jeyaraman, M., Jeyaraman, N., & Yadav, S. (2024). Doctor, Bot, or Both: Questioning the Medicolegal Liability of Artificial Intelligence in Indian Healthcare. *Cureus*, 16. <https://doi.org/10.7759/cureus.69230>

¹⁴ Scherer, M. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29, 353. <https://doi.org/10.2139/ssrn.2609777>

disincentivize AI solution development (Ganapathy, 2021).¹⁵ The Supreme Court of India has declared the Right to Privacy a fundamental right, and the Personal Data Protection Bill (2018) drafted by the Srikrishna Committee represents a first step toward data privacy regulation relevant to AI. The proposed Digital Information Security in Healthcare Act (DISHA) may eventually cover some AI healthcare issues, but no sector-specific AI legislation has been enacted.

AI's autonomous decision-making capability challenges existing tort liability models product liability, negligence, and strict liability because harm may arise without a clear human actor at fault (Bisoyi, 2022).¹⁶ The "black-box" nature of many AI algorithms prevents users from explaining how a decision was reached, complicating medical malpractice and product liability claims. AI's inherent unpredictability makes it difficult to define what constitutes a product defect, and proving that a defect caused harm and that a specific developer was responsible places a considerable evidentiary burden on injured consumers (Bottomley, 2023).¹⁷

When multiple AI systems are used together, as is common in healthcare, attributing fault among developers, data collectors, annotators, manufacturers, and end-users may become impossible under traditional tort frameworks (Fernández Llorca, 2022).¹⁸ The complex supply chain of AI from training framework developers to hardware manufacturers means many actors hold partial control without complete oversight, creating liability gaps rather than clear fault lines (Custers, 2025).¹⁹

Healthcare represents the most active domain for AI deployment in India, from diagnostics to robotic surgery, and raises acute medicolegal liability questions. If an AI system causes patient harm in India, it remains unclear who would be held liable—the physician, the manufacturer, the software developer, or the institution. Vicarious responsibility could extend to the overseeing surgeon, the manufacturing company, and the specific engineer who designed the system, but the culpability of each protagonist remains unresolved. Notably, IBM's Watson has been treated as a consulting physician rather than a product, complicating the application of product liability frameworks.

The regulatory framework for medical AI liability is inadequate globally and requires urgent intervention, as no single regulation governs the liability of various parties across the AI supply chain (Sablone, 2024).²⁰ Regulations should distinguish between diagnostic errors, technology malfunctions, and errors from inaccurate training data, as each carries different liability implications. AI systems need extensive clinical validation before full integration into healthcare delivery, but mandating slow, expensive clinical trials could delay benefits.

The European Union leads globally with its proposed AI liability directive, which seeks to ease compensation claims for AI-caused harm, and its updated product liability directive clarifying that AI

¹⁵ Ganapathy, K. (2021). Artificial Intelligence and Healthcare Regulatory and Legal Concerns. *Telehealth and Medicine Today*. <https://doi.org/10.30953/tmt.v6.252>

¹⁶ Bisoyi, A. (2022). Ownership, liability, patentability, and creativity issues in artificial intelligence. *Information Security Journal: A Global Perspective*, 31, 377 - 386. <https://doi.org/10.1080/19393555.2022.2060879>

¹⁷ Bottomley, D., & Thaldar, D. (2023). Liability for harm caused by AI in healthcare: an overview of the core legal concepts. *Frontiers in Pharmacology*, 14. <https://doi.org/10.3389/fphar.2023.1297353>

¹⁸ Fernández Llorca, D., Charisi, V., Hamon, R., Sanchez, I. E., & Gómez, E. (2022). Liability regimes in the age of AI: a use-case driven analysis of the burden of proof. *J. Artif. Intell. Res.*, 76, 613-644. <https://doi.org/10.1613/jair.1.14565>

¹⁹ Custers, B., Lahmann, H., & Scott, B. I. (2025). From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies. *AI & Society*, 40, 4035 - 4050. <https://doi.org/10.1007/s00146-024-02137-1>

²⁰ Sablone, S., Bellino, M., Cardinale, A. N., Esposito, M., Sessa, F., & Salerno, M. (2024). Artificial intelligence in healthcare: an Italian perspective on ethical and medico-legal implications. *Frontiers in Medicine*, 11. <https://doi.org/10.3389/fmed.2024.1343456>

systems fall under product liability rules. No individual nation has yet enacted a comprehensive AI law, and India's position mirrors this global uncertainty. Until robust legal frameworks are established, healthcare professionals in India should exercise vigilance when using AI tools, as they may still bear significant liability under existing principles. The fundamental challenge remains adapting traditional tort concepts to AI's novel characteristics or moving toward alternative dispute and reconciliation mechanisms that prioritize learning and safety over adversarial fault-finding.

1.3 Research Questions

- What forms of consumer harm arise from AI technologies?
- Whether existing tort law principles adequately address AI-related harms?
- Can the Consumer Protection Act, 2019 effectively compensate AI-induced consumer injuries?
- What legal reforms are required to establish AI accountability in India?

1.4 Objectives of the Study

- To examine AI technologies and their impact on consumers.
- To analyse tort law principles applicable to AI-related harm.
- To evaluate the adequacy of the Consumer Protection Act, 2019.
- To study comparative AI liability frameworks.
- To propose legal reforms for India.

1.5 Research Hypotheses

- Existing tort law is inadequate to address autonomous AI-related injuries.
- Consumer Protection Act, 2019 only partially addresses AI-based consumer harm.
- India requires a dedicated AI liability framework.

1.6 Methodology and Design

The strongest methodology is a doctrinal and comparative legal study using statutes, policy documents, case law, and foreign models, especially EU liability reforms and product-liability adaptation debates.²¹ The literature also supports analysing AI harms through the elements of tort fault, defect, causation, and damage because AI systems make each harder to prove, especially where black-box systems or multiple actors are involved.²²

- **Research methodology:** doctrinal analysis, comparative analysis, and problem-based case study review.²³
- **Sources:** Indian statutes and policies, judicial decisions, Law Commission-style secondary materials, and comparative EU or international instruments.

²¹ Gowda, T. R. (2026). ARTIFICIAL INTELLIGENCE AND LAW: IS THE INDIAN LEGAL FRAMEWORK READY?. *Indian Journal of Legal Review*. <https://doi.org/10.65393/jprb7370>

²² Ertan, F. (2025). Artificial Intelligence and Liability for Damages. *International Journal of Social Sciences*. <https://doi.org/10.52096/usbd.9.41.16>

²³ Abouhaiba, N., Khoulil, S. A., & Khater, M. (2026). Towards Protecting the Injured Party from Errors and Hallucinations of Artificial Intelligence: A Contemporary Legal Perspective. *F1000Research*, 15. <https://doi.org/10.12688/f1000research.179603.1>

- **Analytical lens:** negligence, product liability, strict liability, burden of proof, transparency, and compensation mechanisms such as insurance or funds.²⁴

Taken together, the literature supports a study framed around India's fragmented AI governance, the difficulty of fitting AI harm into traditional tort doctrine, and the need for comparative, reform-oriented legal analysis.

2. Conceptual Framework of Artificial Intelligence and Consumer Harm

2.1 Meaning and Evolution

Artificial intelligence is commonly defined as a system's ability to interpret external data, learn from it, and use those learnings to achieve goals through flexible adaptation.²⁵ Other definitions emphasize AI as the study and engineering of computations that enable perception, reasoning, and action, or as computer systems performing tasks that normally require human intelligence.²⁶ Recent scholarship also treats AI as a sociocultural force, not only a technical artifact, because its deployment reshapes accountability, bias, and the future of work.

The modern history of AI is usually traced to Turing's 1950 account of machine intelligence and the 1956 Dartmouth Conference, which coined the term "artificial intelligence". Its development then moved through repeated cycles of optimism and "AI winters," before resurging in the 21st century through machine learning, deep learning, larger datasets, and greater computing power. This evolution also reflects a shift from AI as a scientific field to a commercialized and social phenomenon embedded in everyday markets.²⁷

2.2 Types and Applications

AI is classified in several ways. One influential scheme distinguishes analytical, human-inspired, and humanized AI according to whether systems exhibit cognitive, emotional, and social intelligence.²⁸ The same paper also distinguishes artificial narrow, general, and super intelligence by evolutionary stage. Other literature separates symbolic/classical and connectionist AI, while some broader typologies group AI literature into scientific, technical, and cultural perspectives.²⁹

AI affects consumers through personalization and recommender systems.³⁰ It also operates through predictive analytics, dynamic pricing, and customer service automation. Consumer-facing examples include wearables, smart speakers, playlists, photo tools, retail profiling, insurance claims systems, and targeted advertising.

²⁴ Bruyne, J. D., & Dheu, O. (2023). Artificial Intelligence and Tort Law: A 'Multi-faceted' Reality. *European Review of Private Law*. <https://doi.org/10.54648/erpl2023021>

²⁵ Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61, 14 - 5. <https://doi.org/10.1177/0008125619864925>

²⁶ Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*. <https://doi.org/10.3389/fhumd.2024.1421273>

²⁷ Chumakov, E. (2025). History and definitions of AI. *European Psychiatry*, 68, S61 - S61. <https://doi.org/10.1192/j.eurpsy.2025.238>

²⁸ Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61, 14 - 5. <https://doi.org/10.1177/0008125619864925>

²⁹ Sabouret, N., & Assis, L. D. (2020). Understanding Artificial Intelligence. *The Reasonable Robot*. <https://doi.org/10.1017/9781108631761.002>

³⁰ Puntoni, S., Reczek, R., Giesler, M., & Botti, S. (2020). Consumers and Artificial Intelligence: An Experiential Perspective. *Journal of Marketing*, 85, 131 - 151. <https://doi.org/10.1177/0022242920953847>

2.3 Consumer Harm and Vulnerability

Consumer harm in the AI literature extends beyond physical or economic injury. It includes informational harm, discriminatory treatment, emotional distress, loss of control, erosion of trust, and reduced decisional autonomy.³¹ One influential account defines algorithmic harm as the exploitation of absent information or behavioural biases, causing consumers to buy low-value products or overpay for valuable ones. These harms can also fall unevenly on identifiable groups, including women and people of colour.³²

2.4 Ethical Issues

The most consistent ethical principles are fairness, transparency, accountability, privacy, and explainability. Fairness matters because AI systems can reproduce historical bias in areas such as hiring, lending, retail profiling, and risk scoring when trained on biased data.³³ Transparency matters because opaque systems obscure how decisions are made and weaken trust, challenge, and redress.

Privacy and consent are central because consumer-facing AI often relies on extensive personal data collection. Autonomy is threatened when AI enables covert influence, seamless nudging, or manipulation in decision environments. Accountability remains difficult where automated systems act with little human oversight or where harms emerge from opaque model behaviour.³⁴

The ethical challenges of AI arise not merely from the technology itself but from how AI is designed, trained, deployed, and governed. An ethically responsible AI framework should therefore ensure that technological innovation is accompanied by fairness, transparency, privacy protection, human oversight, accountability, and effective remedies for individuals harmed by AI systems.

3. Theoretical and Legal Framework of Tort Law and AI Liability

Traditional tort law rests on human-centric doctrines of fault, duty, and foreseeability that struggle to accommodate AI's autonomy and opacity.³⁵ Scholars broadly agree that applying these established principles to AI requires either careful adaptation or a shift toward strict liability and shared responsibility models.³⁶

3.1 Fundamental Principles and Strict Liability

Tort liability arises from a breach of a general legal duty not to harm others, requiring proof of fault, damage, and a causal relationship between them.³⁷ Under traditional common law, tort is predominantly fault-based, requiring an assessment of the tortfeasor's state of mind or adherence to a reasonable standard

³¹ Zheng, Z., Tan, Q. L., Zheng, X., & Yang, Y. (2025). The Dark Side of AI in Insurance: A Systematic Review of Mechanisms Linking AI Design Features to Consumer Harm. *Journal of Consumer Affairs*. <https://doi.org/10.1111/joca.70034>

³² Bar-Gill, O., Sunstein, C., & Talgam-Cohen, I. (2023). Algorithmic Harm in Consumer Markets. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4321763>

³³ Bahangulu, J. K., & Owusu-Berko, L. (2025). Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency and compliance in AI-powered business analytics applications. *World Journal of Advanced Research and Reviews*. <https://doi.org/10.30574/wjarr.2025.25.2.0571>

³⁴ Radanliev, P. (2025). AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development. *Applied Artificial Intelligence*, 39. <https://doi.org/10.1080/08839514.2025.2463722>

³⁵ Sullivan, H. R., & Schweikart, S. J. (2019). Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?. *AMA journal of ethics*, 21 2, E160-166 . <https://doi.org/10.1001/amajethics.2019.160>

³⁶ Marchisio, E. (2021). In support of “no-fault” civil liability rules for artificial intelligence. *SN Social Sciences*, 1. <https://doi.org/10.1007/s43545-020-00043-z>

³⁷ Hassan, K. M., & Atwan, R. S. (2025). The Civil Liability of Artificial Intelligence Applications: Between the Limitations of Traditional Liability and the Evolution of the Product Concept. *Indian Journal of Information Sources and Services*. <https://doi.org/10.51983/ijiss-2025.ijiss.15.3.31>

of care. Strict liability departs from this fault requirement, holding parties accountable for harm regardless of intent or negligence. In the AI context, strict liability is increasingly proposed as a necessary evolution because it simplifies compensation by focusing on the harm rather than on proving elusive technical fault.³⁸

A strict liability regime for AI can optimize the level of care taken by developers by forcing the internalization of risk costs, though it must be carefully tailored to avoid stifling innovation. Some scholars propose a tiered approach: strict liability for personal injury and death caused by AI, but a bespoke fault-based regime for dignitary or reputational injuries.³⁹ Furthermore, strict liability is considered institutionally rational for generative AI because it circumvents the multi-party attribution games and technological black boxes that defeat negligence claims.

3.2 Product Liability and Vicarious Responsibility

Applying product liability to AI is complicated by the technology's dynamic learning nature, which deviates from static, traditional product definitions. While strict product liability can compensate victims without requiring proof of fault, it necessitates proving that a defect exists and caused the harm an immense evidentiary burden when AI behaviour is opaque and unpredictable. Because AI systems continuously learn from external data, establishing a unified legal standard for what constitutes an algorithmic defect remains a fundamental challenge.

Vicarious liability and principal-agent frameworks offer another avenue, potentially holding physicians or operators responsible for AI decisions, though this risks reducing the adoption of AI tools due to misplaced liability fears. Because AI development involves a complex supply chain of developers, data providers, and manufacturers, attributing fault to a single party under traditional vicarious liability rules is often impossible.⁴⁰

3.3 Professional Negligence and Emerging Concepts

Professional negligence in AI deployment, particularly in healthcare, complicates the standard of care because professionals may not be able to explain recommendations generated by black-box algorithms.⁴¹ If a physician relies on an AI clinical decision support program that issues an incorrect recommendation, the physician may be held liable for negligence if a reasonably competent specialist would have noticed and ignored the error. However, the lack of a clear definition of responsibility for both the AI and the physician complicates the ability to assess fault-based liability.

Emerging concepts to address AI liability gaps include granting legal personhood to AI, though this remains controversial and legally untested.⁴² Shared responsibility models are gaining traction, proposing that all stakeholders in the AI supply chain are liable unless they can prove they did not owe a duty of

³⁸ Mao, C. (2025). Shifting Liability Principles for Generative Artificial Intelligence from a Law and Economics Perspective: From Negligence Liability to Strict Liability. *Journal of Global Economy, Business and Finance*. [https://doi.org/10.53469/jgeb.2025.07\(06\).13](https://doi.org/10.53469/jgeb.2025.07(06).13)

³⁹ Soyer, B., & Tettenborn, A. (2022). Artificial intelligence and civil liability - do we need a new regime?. *Int. J. Law Inf. Technol.*, 30, 385-397. <https://doi.org/10.1093/ijlit/eaad001>

⁴⁰ Carlson, K. W. (2025). Review: Addressing the challenges of harmonizing law and artificial intelligence technology in modern society. *SuperIntelligence - Robotics - Safety & Alignment*. <https://doi.org/10.70777/si.v2i2.14807>

⁴¹ Sullivan, H. R., & Schweikart, S. J. (2019). Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?. *AMA journal of ethics*, 21 2, E160-166 . <https://doi.org/10.1001/amajethics.2019.160>

⁴² Rosemadi, J. F., & Jamaludin, S. (2022). The Liability of Artificial Intelligence's Moral Dilemma. *F1000Research*, 11, 1079. <https://doi.org/10.12688/f1000research.73640.1>

care, thereby transforming liability gaps into liability overlaps. No-fault compensation schemes and mandatory AI liability insurance are also proposed as financial management tools to ensure victim remedies without disincentivizing technological innovation.⁴³

3.4 Challenges in Applying Traditional Tort Principles to AI

The foremost challenge in applying traditional tort principles to AI is the "black-box" problem, where the opacity of algorithmic processes prevents users and courts from determining how a specific decision was reached.⁴⁴ This opacity creates an epistemological challenge to legal reasoning, as traditional "but-for" tests of causation are intrinsically limited when applied to black-box machine learning systems.⁴⁵ The unpredictability of AI systems makes it difficult to define what constitutes a defect and to prove that the defect caused the specific harm.

The informational gap between plaintiffs and AI controllers necessitates creative legal solutions like updated collective liability and presumptions of causation to relieve victims of prohibitive evidentiary burdens.⁴⁶ AI behaviour is influenced by algorithms, data inputs, and operational models, complicating the determination of fault across a web of developers, users, and manufacturers. AI's autonomous and self-learning capabilities mean its actions after release can be unforeseeable, potentially absolving designers of liability but leaving injured parties without redress.

Because AI presents a new dimensional challenge to the corpus of existing tort law, a uniform liability rule is unworkable; instead, diverse approaches tailored to different AI applications and harm types are required.⁴⁷ Ultimately, the central challenge is adapting traditional concepts of liability to AI's novel nature or moving away from fault-based liability toward reconciliation and risk-allocation frameworks.

4. Consumer Protection and Regulatory Framework for AI in India

India's regulatory landscape for AI spans consumer protection law, data privacy, cyber law, contract law, competition law, and emerging governance initiatives, but existing frameworks were designed for pre-AI markets and leave significant gaps in algorithmic accountability, liability, and enforcement.⁴⁸

4.1 Consumer Protection Act, 2019

The Consumer Protection Act, 2019 replaced the 1986 Act and introduced e-commerce-specific regulation through the Consumer Protection (E-Commerce) Rules, 2020, requiring platforms to disclose transaction terms, product attributes, and complaint-resolution mechanisms.⁴⁹ The Act established the Central

⁴³ Marchisio, E. (2021). In support of "no-fault" civil liability rules for artificial intelligence. *SN Social Sciences*, 1. <https://doi.org/10.1007/s43545-020-00043-z>

⁴⁴ Fraser, H., Simcock, R., & Snoswell, A. J. (2022). AI Opacity and Explainability in Tort Litigation. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. <https://doi.org/10.1145/3531146.3533084>

⁴⁵ J. (2025). Causation in AI Tort Litigation: Legal Dilemmas of Algorithmic Black Boxes and Burden of Proof Allocation. *Legal Compliance*. <https://doi.org/10.63808/lc.v1i2.127>

⁴⁶ Diega, G. N. L., & Bezerra, L. (2024). Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive. *Int. J. Law Inf. Technol.*, 32. <https://doi.org/10.1093/ijlit/eaac021>

⁴⁷ Abraham, K. S., & Sharkey, C. M. (2026). Untangling AI Liability. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.6293099>

⁴⁸ Mone, V., Thommandru, A., Maratovich, F. F., Khurramovich, K. F., & Mirziyatovna, A. K. (2026). AI Price Tags and Privacy: When Your Data Sets Your Price. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 16. <https://doi.org/10.1002/widm.70070>

⁴⁹ Johri, S. (2023). Emerging artificial intelligence and its cascading effects on consumer protection in India: An analytical study. *World Journal of Advanced Research and Reviews*. <https://doi.org/10.30574/wjarr.2023.19.3.2032>

Consumer Protection Authority (CCPA) with powers to investigate unfair trade practices, recall products, and suspend platforms. Product liability provisions cover manufacturing defects, but scholars argue the Act should explicitly classify AI systems as "products" to hold developers liable for algorithmic harms. The Act addresses deficiency in service and unfair trade practices, yet algorithmic "black box" decision-making creates information asymmetries that traditional consumer protection doctrines struggle to address.⁵⁰

4.2 Digital Personal Data Protection Act, 2023

The DPDPA introduces consent-based data processing, purpose limitation, and data fiduciary obligations, providing a foundational privacy framework for AI systems that rely on personal data. The Act incorporates Consent Managers to ensure AI systems manage consumer data responsibly. However, the DPDPA does not address algorithmic bias, transparency in automated decision-making, or accountability for AI-driven outcomes.⁵¹ Its transparency requirements apply only to "significant data fiduciaries," exempting smaller operators and criminal actors on decentralized platforms. The Act excludes purely synthetic information not tied to real individuals, allowing AI-generated identities to evade regulatory coverage.⁵²

4.3 Information Technology Act, 2000

The IT Act remains the cornerstone of India's cyber law framework, addressing hacking, data breaches, and electronic transactions. Its provisions were designed for conventional digital issues and do not contemplate autonomous decision-making, machine learning processes, or algorithmic opacity. Section 43A, which addresses reasonable security practices, could be interpreted to include liability for AI-caused harm, but currently lacks specificity on developer or deployer accountability. The Act does not extend regulatory authority to mobile applications or social media companies in ways that protect consumer rights in AI-mediated services. The proposed Digital India Act aims to replace the IT Act with a framework better suited to AI-era challenges.⁵³

4.4 Competition Law and Digital Markets

AI-driven pricing systems enable sophisticated consumer discrimination through device-based differentials and usage-pattern exploitation, challenging traditional competition frameworks. Algorithmic "hub-and-spoke conspiracies" facilitate collusion without explicit coordination between competitors, evading existing antitrust detection.⁵⁴ India's reactive consumer protection model contrasts with the EU's proactive transparency requirements under the Digital Services Act and Digital Markets Act, which

⁵⁰ Acharya, S., Das, B., Mishra, A., & Acharya, O. (2025). Transparency and Explainability of Algorithms from a Consumer Law Perspective. *Advanced International Journal for Research*. <https://doi.org/10.63363/aijfr.2025.v06i06.2652>

⁵¹ S.K.V, S. V., & D.N, N. (2024). Legal Challenges of Artificial Intelligence in India's Cyber Law Framework: Examining Data Privacy and Algorithmic Accountability Via a Comparative Global Perspective. *International Journal For Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2024.v06i06.31347>

⁵² Singh, P. (2025). Deepfakes, identity theft, and the dark web: Legal gaps in AI-Generated fraud, an Indian perspective. *International Journal of Civil Law and Legal Research*. <https://doi.org/10.22271/civillaw.2025.v5.i2b.148>

⁵³ Kaur, G. (2024). Navigating The Legal Landscape: Addressing AI-Driven Innovations and Challenges in Indian Fintech. *Journal of Informatics Education and Research*. <https://doi.org/10.52783/jier.v4i3.1361>

⁵⁴ Mone, V., Thommandru, A., Maratovich, F. F., Khurramovich, K. F., & Mirziyatovna, A. K. (2026). AI Price Tags and Privacy: When Your Data Sets Your Price. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 16. <https://doi.org/10.1002/widm.70070>

address platform accountability and systemic market power. Existing legal frameworks designed for pre-digital markets cannot effectively address technologically sophisticated forms of consumer harm and market manipulation.

4.5 AI Governance Initiatives

India's AI governance has advanced through non-binding policy guidelines rather than binding legislation, creating a fragmented regulatory landscape.

- NITI Aayog issued Principles for Responsible AI, establishing ethical guidelines without statutory force.
- MeitY advisories and the proposed Digital India Act aim to replace the IT Act with AI-relevant provisions, but remain in draft form.
- IndiaAI Mission promotes AI development and innovation, though comprehensive regulatory frameworks are still anticipated.
- BIS standards and sectoral regulators (RBI, SEBI, IRDAI) have issued domain-specific AI guidelines, but these remain insufficient for AI's rapidly evolving risks.

4.6 Gaps in India's Existing Legal Framework

India lacks a comprehensive AI-specific legal framework, relying on statutes enacted before sophisticated algorithmic systems emerged. The fragmented approach combining the IT Act, DPDPA, Consumer Protection Act, and non-binding guidelines fails to address algorithmic transparency, accountability, and liability coherently. Key deficiencies include the absence of a "right to explanation" for automated decisions, unclear liability allocation among developers and deployers, and no mandate for algorithmic auditing. Citizen awareness of algorithmic data processing remains very low, compounding regulatory weaknesses.⁵⁵ Scholars consistently recommend a risk-based regulatory approach modeled on the EU AI Act, with binding obligations for high-risk AI systems and independent oversight authorities. Without such reforms, India's digital governance framework risks obsolescence in the face of rapidly advancing AI-enabled threats.

5. Comparative Study of AI Liability Frameworks

The EU has developed the most comprehensive AI liability architecture through a three-instrument approach, while the UK, US, Canada, and Singapore rely on sector-specific or decentralized models; India's fragmented framework lacks binding AI-specific liability rules and could draw lessons from the EU's risk-based regime and the UK's targeted legislation.⁵⁶

5.1 European Union

The EU's AI liability framework rests on three interconnected instruments: the AI Act (Regulation 2024/1689), the revised Product Liability Directive (Directive 2024/2853), and the proposed AI Liability

⁵⁵ A., & Ahmad, K. (2025). Impact of Artificial Intelligence on Digital Personal Data: An Analysis of Citizen Awareness and Statutory Guidance for AI Based Data Processing in India. *2025 2nd Global AI Summit - International Conference on Artificial Intelligence and Emerging Technology (AI Summit)*, 341-346. <https://doi.org/10.1109/aisummit66170.2025.11411280>

⁵⁶ Rathore, G. S., & Jasrotia, P. (2025). REGULATORY FRAMEWORKS FOR ARTIFICIAL INTELLIGENCE IN THE EUROPEAN UNION AND INDIA: A COMPARATIVE STUDY. *PARIPEX INDIAN JOURNAL OF RESEARCH*. <https://doi.org/10.36106/paripex/2403073>

Directive, which was withdrawn in 2025. The AI Act establishes a risk-based classification system imposing obligations on providers and deployers of high-risk AI systems through mandatory conformity assessments.⁵⁷ Critically, the AI Act contains no individual rights of affected persons, making the liability directives essential for ex-post redress.

The revised PLD explicitly covers software and AI systems, introducing a rebuttable presumption of causation to address evidential difficulties in technically complex cases.⁵⁸ The AILD, before its withdrawal, was designed to harmonize fault-based liability through disclosure mechanisms and presumptions of causation, but rejected strict liability in favour of procedural reforms. Scholars argue this represents a half-hearted approach primarily resting on disclosure and narrowly defined presumptions rather than comprehensive strict liability.⁵⁹

Significant gaps persist despite this three-instrument architecture. The directives leave liability gaps for black-box medical AI systems where patients cannot successfully sue manufacturers or providers under either strict or fault-based regimes. The dual-directive structure creates delimitation problems, as companies may mischaracterize standard software as AI, leading victims to choose the wrong compensation regime. The AILD's reliance on the AI Act's risk concept is misplaced, since tort liability intervenes after risk materializes, not before.

5.2 United Kingdom and United States

The UK enacted the Automated and Electric Vehicles Act 2018, the world's first legislation addressing liability for self-driving incidents by assigning insurer responsibility. For AI-generated legal advice, UK common law of negligence presupposes a human professional at the centre of the advisory relationship, leaving no clean liability pathway when AI operates outside that relationship. The UK's flexible, sector-specific strategy facilitates agile responses but risks inconsistent coverage across domains.⁶⁰

The US employs a decentralized, voluntary governance model relying on frameworks such as the AI Bill of Rights and the NIST AI Risk Management Framework rather than binding legislation.⁶¹ US courts emphasize causation, foreseeability, and negligence standards, with liability shared between manufacturers, operators, and infrastructure providers in autonomous vehicle cases. The US and India share a fragmented state-law approach to autonomous vehicle regulation, contrasting with the UK's unified legislation.

⁵⁷ Kalagi, S., Gubbewad, R. S., & Gondale, A. (2024). LEGAL LIABILITIES OF ARTIFICIAL INTELLIGENCE: AN OVERVIEW. *Journal of Law and Sustainable Development*. <https://doi.org/10.55908/sdgs.v12i8.3861>

⁵⁸ Waqar, T. (2026). AI-Generated Legal Advice: Liability Frameworks Under UK and EU Law . *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.6407018>

⁵⁹ Hacker, P. (2022). The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future. *ArXiv, abs/2211.13960*. <https://doi.org/10.48550/arxiv.2211.13960>

⁶⁰ Al-Maamari, A. (2025). Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, U.S., UK, and China. *2025 International Conference on Sustainable Technology and Engineering (i-COSTE)*, 1-5. <https://doi.org/10.1109/i-coste68047.2025.11467397>

⁶¹ Okuno, M. J., & Okuno, H. G. (2025). Legal frameworks for AI service business participants: a comparative analysis of liability protection across jurisdictions. *AI & SOCIETY*, 40, 5667 - 5683. <https://doi.org/10.1007/s00146-025-02288-9>

5.3 Canada, Singapore, and OECD Principles

Canada and Singapore adopt flexible regulatory models alongside international alignment efforts. Singapore takes an agile approach to AI regulation, favouring adaptive governance over comprehensive legislation.

The OECD AI Principles (2019) provide a foundational international framework emphasizing transparency, accountability, and fairness. The European Parliament revised the AI Act's AI definition to align with the OECD standard, reflecting the need for global consistency. International initiatives including the G7 Hiroshima AI Process (2023) and METI guidelines complement the OECD Principles in promoting regulatory alignment.

5.4 Comparative Lessons for India

India's AI governance remains fragmented, relying on the IT Act 2000, the DPDPA 2023, and non-binding NITI Aayog guidelines rather than comprehensive AI-specific liability legislation. The EU follows a clearer, rights-based model with formal risk-based obligations, whereas India's approach features strong policy rhetoric but no binding protections. India and the US share a loose interweaving network of state laws for autonomous vehicles, while the UK's pioneering AEVA 2018 demonstrates the value of targeted legislation.

India should adopt the EU's risk-based classification system with binding obligations for high-risk AI systems. A hybrid liability model combining US proximate causation doctrine with EU tiered risk classification could balance innovation and accountability.⁶² India should introduce a legally enforceable right to explanation for automated decisions, a gap the EU AILD attempted but failed to fill. Algorithmic impact assessments and mandatory insurance pools could ensure compensation where liability attribution is indeterminate.

Both the EU and India's NITI Aayog recognize that regulatory insight must serve as ethical reinforcement for AI practice, but India lacks the binding enforcement mechanisms that the EU's directive-based system provides. Existing fraud statutes across India, the US, and the EU exhibit anthropocentric biases by predicating liability on demonstrable human intent, rendering them ill-equipped for algorithmic deception. Without comprehensive reform, India risks fragmented litigation, legal uncertainty, and under-enforcement of AI accountability norms.⁶³

6. Case Studies and Judicial Analysis

Courts across jurisdictions are encountering AI-related consumer harms — from recruitment discrimination to autonomous vehicle accidents — and applying classical liability principles with mixed success.⁶⁴ Indian judicial developments remain largely doctrinal, while international case law demonstrates rapid adaptation of negligence and product liability doctrines to algorithmic harms.

⁶² Ajakaye, F. (2024). A Model for Regulating Artificial Intelligence Liability through Comparative Jurisprudence between the U.S. and EU. *International Journal of Social Science Exceptional Research*. <https://doi.org/10.54660/ijsser.2024.3.5.106-127>

⁶³ Luncă, D. (2025). Towards a Coherent EU Civil Liability Regime for AI-Caused Harm. *European Journal of Law and Public Administration*. <https://doi.org/10.18662/eljpa/12.1/253>

⁶⁴ Ismaeel, S., Alammari, K., & Younus, Z. G. (2026). Evidentiary Challenges in AI-Mediated E-Commerce Disputes. *Justicia Islamica*. <https://doi.org/10.21154/justicia.v23i1.11809>

6.1 AI-Related Consumer Harm Cases

Algorithmic recruitment and credit-scoring systems embed discriminatory bias that disproportionately disadvantages marginalized groups, yet existing statutes exhibit anthropocentric biases by predicated liability on demonstrable human intent.⁶⁵ In autonomous vehicle accidents, liability may be shared between manufacturers, operators, and infrastructure providers, but proving which AI component caused the crash remains exceptionally difficult due to opacity and continuous learning. AI medical diagnosis errors expose gaps in medical malpractice doctrine, as the standard of care and the physician–patient relationship are disrupted when diagnostic algorithms operate as a "second set of eyes".

Facial recognition litigation and algorithmic pricing disputes raise privacy invasion concerns, as AI surveillance enables unauthorized collection of biometric data and personal information without consent. Algorithmic pricing in e-commerce generates information asymmetries that erode consumer protection when recommendation engines facilitate sales of hazardous products.

6.2 Indian Judicial Developments and International Case Studies

Indian privacy jurisprudence and AI governance remain at the doctrine level, with the NITI Aayog's National Strategy for AI (2018) and the Digital Personal Data Protection Act (2023) providing policy direction without binding liability rules. In developed countries, legislation and judicial practices addressing AI harm are already systematized, whereas in developing countries like India the issue remains largely theoretical.⁶⁶ Indian courts have not yet developed specific jurisprudence on medical negligence involving AI-assisted healthcare or digital consumer disputes, relying instead on traditional tort and contract law frameworks.

European courts are rapidly applying classical liability principles negligence, fault, and product liability to AI-generated harms, with new case law emerging on copyright and the use of copyrighted content. The UAE judiciary has shown remarkable flexibility by expanding judicial presumptions and assuming fault in high-risk activities to address AI harms. US courts historically dismissed algorithmic liability claims early by invoking Section 230 immunity, but recent jurisprudence signals a critical turning point as courts begin permitting these cases to proceed past procedural challenges.⁶⁷

6.3 Judicial Trends and Emerging Liability Principles

Judicial trends reveal a shift from fault-based to risk-based liability models, as courts recognize that AI's opacity, unpredictability, and continuous learning make traditional causation standards inadequate. The presence or absence of human contribution in AI outputs has become a fundamental criterion in determining liability across jurisdictions. Scholars propose a "common enterprise" strict liability approach treating physicians, manufacturers, and hospitals as a collective entity, shifting away from individualistic notions of responsibility.⁶⁸

⁶⁵ Gautam, P., & Singh, S. (2025). LIABILITY FOR HARM CAUSED BY AUTONOMOUS AI SYSTEMS. *International Journal on Science and Technology*. <https://doi.org/10.71097/ijst.v16.i4.9209>

⁶⁶ Alqodsi, E., & Gura, D. (2023). High tech and legal challenges: Artificial intelligence-caused damage regulation. *Cogent Social Sciences*, 9. <https://doi.org/10.1080/23311886.2023.2270751>

⁶⁷ Henson, R. (2026). Artificial Intelligence, Judicial Evolution, and Insurance. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.6874119>

⁶⁸ Cestonaro, C., Delicati, A., Marcante, B., Caenazzo, L., & Tozzo, P. (2023). Defining medical liability when artificial intelligence is applied on diagnostic algorithms: a systematic review. *Frontiers in Medicine*, 10. <https://doi.org/10.3389/fmed.2023.1305756>

Rebuttable presumptions of causation and mandatory algorithmic explainability standards are proposed to ease the burden of proof for victims. Compulsory insurance and compensation funds are recommended to ensure redress where liability attribution is indeterminate. Sui generis dispute resolution institutions for AI healthcare harm could replace litigation with reconciliation, holding investigative powers and developing guidelines. No-fault redress rules would compensate injured persons without requiring proof of fault against any individual.

AI's multiplicity of actors developers, data providers, operators, and users complicates liability allocation, necessitating enhanced duties of care and shared liability among tortfeasors. The burden of proving a reasonable alternative design that could have avoided harm can be enormous and, in some cases, unfeasible for victims to address. Without effective and accessible compensation mechanisms, the legitimacy of AI technology itself is at risk.

7. Challenges, Recommendations and Conclusion

The main issues are fragmented law, attribution problems, opacity, and weak redress; the literature consistently recommends a risk-based, explainability-centered liability framework.

7.1 Major Challenges

Current AI liability regimes are widely described as inadequate for autonomous, opaque systems, especially where no AI-specific statute clearly allocates responsibility. Multi-actor AI supply chains create a “many hands” problem, because design, training, deployment, and use are split across developers, deployers, data providers, and users. Black-box systems make it hard to reconstruct why a decision occurred, which directly obstructs accountability and judicial proof.

Cross-border deployment further weakens enforcement because territorially bounded liability rules do not fit globally deployed AI services and fragmented regulation complicates compliance and redress. The burden of proof is a recurring barrier: victims often cannot prove defect, fault, or causation because AI systems are complex, opaque, and unpredictable even when defendants disclose logs or documentation.

7.2 Reform Recommendations

The strongest legislative recommendation is a comprehensive AI liability framework that aligns ex ante regulation with ex post compensation and clearly defines the responsibilities of developers, deployers, manufacturers, and professional users. Several papers support strict or presumptive liability for high-risk AI, while reserving lighter presumptions or fault-based rules for lower-risk systems to avoid over-deterrence. The literature also supports mandatory explainability and disclosure duties, including access to evidence, standardized explainability methods, and algorithmic audits.

- Consumer protection should require stronger product liability, AI-specific disclosures, and accessible redress for safety and rights-based harms.
- Tort reform should use rebuttable presumptions, reverse burden rules in appropriate cases, and shared or proportional liability where control is distributed.
- Institutional reform should add regulatory sandboxes, technical oversight capacity, and specialized redress bodies such as ombudsman-like or sui generis dispute mechanisms.

Ethical Governance

Ethical governance recommendations center on transparency, human oversight, and independent auditing as liability-enabling measures, not just soft-law aspirations. Researchers repeatedly argue that explainability standards should be strong enough to empower claimants yet calibrated to protect confidentiality and innovation. Insurance is treated as a necessary backstop: proposals include mandatory insurance pools, subsidized coverage for SMEs, public-private risk sharing, and collective compensation funds for attribution-resistant harms.

Across these challenges and recommendations, the clearest comparative lesson is that AI liability needs risk-based rules, explainability duties, burden-shifting, and workable compensation mechanisms. For India, that points toward a dedicated AI liability statute backed by disclosure, audits, shared liability, and specialized redress institutions.

7.3 Conclusion

Artificial Intelligence has emerged as a transformative technology capable of significantly improving the delivery of goods and services, decision-making, automation and consumer convenience. At the same time, the increasing deployment of AI in consumer-facing activities has created new forms of harm that challenge traditional principles of tort law. The central difficulty is that conventional tort law is largely structured around identifiable human actors, foreseeable conduct and relatively clear causal relationships. AI systems, however, frequently operate through complex algorithms, large datasets, autonomous decision-making and interconnected networks involving developers, manufacturers, deployers, intermediaries and service providers. Consequently, determining who is responsible when an AI system causes consumer harm may become particularly difficult. The "many hands" problem identified in the Indian responsible-AI discourse illustrates how responsibility may be distributed among several actors, making attribution of fault and establishment of causation challenging under existing legal principles.

The Indian legal framework presently addresses different dimensions of AI-related harm through a combination of existing laws rather than through a comprehensive AI-specific liability regime. The Consumer Protection Act, 2019, principles of negligence and other tortious remedies, contractual obligations, intellectual property law, cyber law and data-protection principles can collectively provide avenues of redress. However, these mechanisms may not always adequately address the distinctive characteristics of autonomous and continuously evolving AI systems. In particular, questions concerning algorithmic opacity, evidentiary burdens, foreseeability, product defects, intermediary responsibility, contributory negligence and compensation remain insufficiently developed.

The future development of AI liability in India should consequently move beyond a purely fault-based approach where appropriate and consider risk-based, product-liability and enterprise-liability principles for high-risk AI applications. Developers and deployers should have continuing duties to test, monitor, audit and update AI systems throughout their lifecycle. NITI Aayog's responsible-AI framework similarly emphasises lifecycle monitoring, safeguards, grievance redressal and compensation mechanisms for unintended or unexpected harm.

At the same time, regulation must maintain a careful balance between consumer protection and technological innovation. Excessively burdensome liability may discourage beneficial AI development, whereas inadequate regulation may leave consumers without effective remedies. A proportionate, risk-



based regulatory framework would therefore be preferable, with stronger obligations imposed on AI systems capable of producing substantial physical, economic, discriminatory or privacy-related harm. The emerging legal challenge is therefore not simply whether AI can be regulated, but how existing principles of justice and liability can be adapted to a technological environment in which decisions may be made by systems rather than directly by human beings. The future of Indian tort and consumer law must respond to this transformation by ensuring that technological complexity does not become a shield against legal responsibility. A robust and adaptive liability framework can enable India to realise the benefits of AI while ensuring that consumers do not bear disproportionate risks arising from its development and deployment.