

Corporate Liability for Ai-Driven Decisions: Legal Reforms and Comparative Perspectives

Riddhika Tiwari^{1*}, Prof. (Dr.) Aradhana Parmar²

¹ Research Scholar, Faculty of Law, Maharishi Arvind University, Jaipur, Rajasthan, India

riddhikatiwari7@gmail.com

² Supervisor, Faculty of Law, Maharishi Arvind University, Jaipur, Rajasthan, India

Abstract: Artificial intelligence increasingly influences corporate decisions concerning employment, credit, healthcare, insurance, and consumer services. Its benefits are accompanied by harms that can be difficult to explain, attribute, and remedy. Responsibility may be divided among developers, suppliers, deploying companies, and individual users, while affected persons lack access to the evidence needed to challenge a decision. This article examines corporate liability through doctrinal and comparative analysis, focusing on India alongside European, British, and American approaches. It considers contemporary problems involving generative AI, discriminatory automation, autonomous agents, and cross-border supply chains. The article argues that legal responsibility should reflect the applicable duty, operational control, and contribution to harm. It proposes proportionate record-keeping, meaningful human review, coordinated regulatory supervision, and carefully targeted evidentiary reforms. Effective accountability requires both preventive governance and practical remedies, without assuming that every adverse automated outcome establishes liability.

Keywords: Artificial Intelligence, Corporate Liability, Generative AI, Autonomous Agents, Algorithmic Discrimination, Consumer Protection, Causation, Comparative Law, Legal Reform

INTRODUCTION

A customer refused an insurance payment may receive an automated explanation that reveals little about the actual decision. An applicant rejected by recruitment software may never know that an inaccurate assumption determined the outcome. These situations expose a practical imbalance: companies can benefit from automated decisions while affected individuals struggle to understand who made them, what went wrong, and how to obtain correction. The legal challenge concerns access to accountability as much as the reliability of technology.

Corporate liability must nevertheless be analysed precisely. A company's responsibility differs from the personal liability of directors, employees, or developers. Contract, negligence, consumer protection, data protection, and sector-specific rules address different duties and injuries. Their requirements cannot be replaced by the general observation that AI participated in a harmful event. This article examines how existing law can respond and where targeted

reform is justified, particularly as generative systems and autonomous agents extend corporate decision-making beyond conventional predictive models.

Research Approach and Scope

The article uses doctrinal analysis of legislation, official frameworks, and enforcement materials, supported by comparative interpretation. It distinguishes binding legal duties from recommendations and proposed reforms. Examples illustrate possible disputes rather than report original empirical findings. The comparison concerns selected jurisdictions and does not assume a uniform global liability regime. Its central question is how legal systems can preserve effective redress when relevant knowledge and control are distributed across organisations.

Historical Development of Corporate and Technological Responsibility

Corporate accountability has long involved tracing responsibility through organisations. Berle and Means (1932) examined the separation of ownership and control, while Jensen and Meckling (1976) explained problems arising from divergent incentives and monitoring costs. These ideas remain relevant when companies outsource technological functions. A deploying business, software supplier, and model developer may have different objectives and unequal information, even though their activities jointly shape an individual's experience.

Turing's (1950) exploration of machine intelligence preceded systems now capable of identifying patterns and generating text, images, and recommendations. Earlier commercial computing largely supported structured processes such as payroll and inventory. Contemporary applications can influence evaluative decisions previously associated with professional judgment. Failures may therefore concern unsuitable objectives, unrepresentative data, misleading outputs, or inadequate supervision rather than a simple departure from a fixed instruction.

Legal responses initially developed through existing categories. Contract allocated commercial responsibilities; negligence examined unreasonable conduct; consumer law addressed defective goods and deficient services. Data-protection frameworks subsequently brought attention to the collection and use of personal information. GDPR became particularly influential in connecting data governance with certain solely automated decisions affecting

individuals (European Parliament & Council of the European Union, 2016). These developments did not produce one interchangeable remedy for every technological harm.

India's National Strategy for Artificial Intelligence and responsible AI documents linked development with inclusion and institutional responsibility (NITI Aayog, 2018, 2021a, 2021b). The OECD recommendation, UNESCO recommendation, and later governance instruments broadened the international discussion. Their significance lies partly in shifting attention towards the entire AI lifecycle. Responsibility now requires examining design, procurement, deployment, updates, monitoring, and withdrawal, rather than locating accountability only at the moment an output is produced.

Foundations of Corporate Liability

Negligence provides one possible framework where an applicable duty, breach, causation, and actionable damage can be established. A company may expose users to foreseeable risks by deploying an inadequately tested application or ignoring serious warnings. Whether that conduct creates liability depends on the governing law and circumstances. Neither technical complexity nor the purchase of a recognised product automatically resolves the inquiry.

Contractual liability concerns obligations between parties, including promises about performance, security, and support. Product and consumer liability may address defects, inadequate warnings, or deficient services under relevant statutes. Regulatory sanctions serve another function and should not be confused with compensation. Similarly, corporate criminal liability requires the elements of a recognised offence and applicable attribution rules. An erroneous prediction alone does not establish criminal intent, nor does every regulatory breach automatically prove a private damages claim.

The Indian Legal Framework

The Consumer Protection Act, 2019 provides important routes involving deficient services, unfair trade practices, and product liability, subject to statutory requirements. Sections 84–86 address manufacturers, product service providers, and sellers. Application to AI requires attention to the transaction, the claimant's status, and the nature of the harm. Embedded software, standalone applications, and professional services can raise different classification questions; their treatment should not be assumed in advance.

Section 166 of the Companies Act, 2013 establishes directors' duties concerning care, diligence, good faith, and independent judgment. These duties can inform scrutiny of oversight without making every director personally liable for every system failure. A claim against a company and a claim against its directors requires separate analysis. The distinction prevents organisational responsibility from being confused with automatic personal culpability.

The Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 create another relevant framework. Their implementation is phased, so the commencement position of each obligation must be checked. The legislation should not be described as providing a general private compensation remedy for every algorithmic injury. India's 2025 AI Governance Guidelines also encourage responsible adoption, but policy guidance does not itself supply a comprehensive civil liability code (Ministry of Electronics and Information Technology [MeitY], 2025a, 2025b).

Generative AI and Misleading Corporate Communications

Generative systems create risks when companies use fluent outputs in customer advice, advertising, legal summaries, or investment communications. A convincing answer may contain an invented fact or omit a qualification essential to the user's decision. Responsibility should examine the context in which the company presented the output, the assurances it gave, foreseeable reliance, and available verification. A broad disclaimer should not be assumed to defeat all otherwise applicable duties.

Synthetic media creates related problems. A company might deploy an artificial spokesperson or publish content that misleadingly implies endorsement. An external attacker might also use a deepfake to induce an employee to transfer funds. These situations require different analyses: one concerns the company's communication, while the other concerns fraud, authorisation, and reasonable controls. The label "AI-generated" cannot determine liability independently of conduct and context.

Autonomous Agents and Delegated Authority

AI agents can initiate communications, place orders, or interact with business systems within permissions granted by an organisation. Their growing operational freedom raises questions about authority and contractual responsibility. A company should define transaction limits, access rights, escalation triggers, and interruption mechanisms before permitting

consequential activity. Whether a particular transaction binds the company depends on applicable contract and agency principles, rather than an assumption that machine activity is legally irrelevant.

An agent's unexpected behaviour also requires examination of who could foresee or prevent the outcome. A developer may have supplied inadequate safeguards, while a deploying company may have granted excessive permissions. Logs and version records become important evidence. Reform should address these relationships directly instead of treating AI as a convenient bearer of responsibility without assets, organisational duties, or meaningful capacity to compensate injured persons.

Cybersecurity failures require similar attention. An attacker may manipulate inputs or exploit permissions to redirect an automated process. Liability assessment should examine relevant security duties and the reasonableness of safeguards, while avoiding the assumption that every successful attack proves negligence. Incident records can help distinguish external interference from defective corporate controls.

Algorithmic Discrimination in Employment and Financial Services

Automated decision systems can reproduce disadvantage through explicit criteria, inaccurate records, or variables that operate as proxies. The American iTutorGroup enforcement action illustrates the relevance of existing law. In 2023, the Equal Employment Opportunity Commission announced a \$365,000 settlement concerning software alleged to reject older applicants automatically. This was an automated screening case and settlement, not a ruling that all learning systems are discriminatory (U.S. Equal Employment Opportunity Commission, 2023).

Similar concerns arise in lending, insurance, and workplace evaluation, although the available legal protections differ across jurisdictions. A technically accurate prediction may still rely on legally impermissible criteria. Conversely, a statistical disparity requires investigation rather than an immediate assumption of unlawful discrimination. Companies should examine relevant groups, actual decision pathways, and realistic opportunities for correction, while respecting applicable privacy and sectoral obligations.

Healthcare and Professional Decision Support

Healthcare illustrates why the allocation of responsibility must remain sensitive to professional context. An AI application may identify an abnormal scan, recommend treatment priorities, or generate a clinical summary. The developer's representations, the institution's deployment choices, and the professional's use of the output may each matter. A tool validated for one population or clinical purpose may be unsuitable elsewhere. Institutions should therefore examine intended use, relevant validation, staff competence, and procedures for investigating discordant results before incorporating recommendations into patient care.

Professional involvement does not automatically excuse an institution that supplies an unsuitable system. Equally, an adverse medical outcome does not by itself establish that AI caused the injury. The applicable standards of care, evidence concerning the patient's condition, and contribution of other clinical decisions remain important. Comparative reform should preserve access to relevant records while respecting patient confidentiality. Where technological advice enters a professional relationship, the institution must consider how patients can obtain an explanation and how professionals can challenge the system without facing organisational pressure to accept its output.

Evidence and Causation

AI disputes often involve an imbalance in access to information. The claimant can describe the rejection or loss but may lack training information, testing results, or decision records. Causation becomes difficult when data errors, design choices, user conduct, and deployment conditions interact. Courts must distinguish uncertainty about how a system operates from evidence that the defendant's conduct legally contributed to the injury.

Proportionate disclosure can help without requiring unrestricted publication of source code or confidential data. Relevant records may include system versions, inputs, warnings, validation reports, and human interventions. Protective orders and independent expertise can preserve legitimate confidentiality. Carefully defined rebuttable presumptions deserve consideration where required evidence has been withheld or destroyed. Such presumptions are reform proposals for appropriate settings, not a statement that Indian law universally reverses proof in AI cases.

The nature of the loss also matters. Physical injury, damage to property, loss of an employment opportunity, and distress may be treated differently under different causes of action. A claimant must identify a legally recognised injury and the appropriate remedy. Economic loss rules, remoteness, mitigation, and applicable limitation periods may affect recovery. A comparative article should therefore avoid suggesting that a single reform to product liability will address all forms of algorithmic harm. A rejected applicant and an injured patient may need different legal routes even when both disputes involve an unreliable model. Legal advice and complaint systems should help individuals identify those routes instead of directing every grievance towards a technical support desk.

INTERNATIONAL PERSPECTIVES

European Union

The EU separates preventive obligations from compensation mechanisms. The AI Act establishes responsibilities differentiated by risk and organisational role, while GDPR addresses personal-data processing and specified automated decisions. Neither makes every inaccurate output actionable or every director personally liable. Compliance analysis must identify the relevant organisation, activity, provision, and applicable implementation schedule (European Parliament & Council of the European Union, 2016, 2024a).

Directive (EU) 2024/2853 modernises defective-product liability by expressly including software. It provides mechanisms for disclosure and rebuttable presumptions under defined conditions. Member States must transpose it by 9 December 2026, and its temporal scope concerns products placed on the market or put into service after that date. The directive is therefore an important comparative model, but should not be presented as an immediately universal remedy or as covering every category of economic loss (European Parliament & Council of the European Union, 2024b).

United Kingdom

British company law requires directors to exercise independent judgment and reasonable care, skill, and diligence under sections 173 and 174 of the Companies Act 2006. These duties inform oversight analysis but do not replace the requirements of a claim concerning contractual promises, negligence, data processing, or consumer treatment. For comparison

with India, the useful lesson is that technological adoption should be assessed through both organisational governance and the particular duties owed to affected persons.

United States

American accountability involves interacting federal and state rules, including employment and consumer protections. The iTutorGroup matter demonstrates that automation does not place corporate conduct outside established employment obligations. NIST's voluntary AI Risk Management Framework complements legal compliance by supporting governance, contextual assessment, measurement, and management. It does not create a general compensation entitlement or guarantee immunity from liability (Tabassi, 2023).

International Principles

The OECD and UNESCO recommendations provide shared principles concerning responsible development and human interests. The Council of Europe's 2024 Framework Convention introduces a treaty framework addressing human rights, democracy, and the rule of law. Its effects depend on participation and implementation. These instruments can inform institutional design, but their different legal forms should remain visible in comparative analysis rather than being grouped together as directly enforceable global corporate law.

Cross Border Supply Chains and Vendor Contracts

An Indian company may deploy a model developed abroad through several intermediaries. When harm occurs, jurisdiction, applicable law, service of proceedings, and enforcement may complicate redress. A commercial choice-of-law clause does not automatically determine every third-party claim. Claimants may also face practical difficulty identifying which entity controlled the relevant design or deployment decision.

Procurement contracts should therefore address responsibility for testing, updates, security, incident cooperation, and access to evidence. Indemnities can allocate losses between businesses, but cannot automatically extinguish statutory rights. Companies should avoid accepting obligations they cannot supervise because suppliers refuse essential information. Where several parties contribute to harm, contribution and allocation rules should be examined under the applicable law rather than assumed from the supply chain alone.

Human Oversight and Preventive Corporate Governance

Human review is useful only when the reviewer can understand the concern and change the result. A nominal approval step may provide little protection if employees lack time, training, or authority. Companies should identify applications affecting significant interests and assign responsibility for monitoring, complaints, and interruption. Oversight should examine operational behaviour rather than rely solely on a vendor's initial demonstrations.

Documentation should record consequential choices, known limitations, and responses to warnings. Incident investigation should preserve relevant evidence and consider whether similarly affected users require review. These practices can reduce harm and assist later legal assessment, but do not create an automatic defence. A well-written policy has limited value when reporting channels suppress inconvenient findings or correction procedures are inaccessible.

Compensation Insurance and Access to Remedies

Damages matter when correction cannot reverse an injury, but remedies may also include reconsideration, rectification, or injunctive relief where available. Procedures should be accessible to individuals unable to obtain specialist assistance. Collective mechanisms may be relevant where similar errors affect many people, subject to the governing procedural law and the need to examine individual differences.

Insurance deserves investigation for narrowly defined hazardous applications. Appropriate cover could improve compensation and encourage risk assessment, but blanket compulsory insurance may increase costs without addressing underlying failures. Policy exclusions, coverage limits, and insurer access to reliable information require attention. Insurance should support responsibility, rather than become a substitute for safe deployment or a means of obscuring who must correct a defective process.

Legal Reforms for India

India should clarify the application of existing consumer and civil liability principles before creating unnecessarily broad new categories. Sector-sensitive guidance can identify proportionate testing, documentation, and review expectations. Companies undertaking

comparable activities should receive consistent signals from relevant authorities, while specialised regulators retain the capacity to address sector-specific risks.

Reform should prioritise access to evidence, affordable expertise, and clear complaint pathways. Targeted presumptions may be justified where a defendant breaches a defined record-keeping duty, provided defendants can rebut them. Any strict liability proposal should identify the hazardous activity, protected interests, available defences, and relationship with existing remedies. Broad slogans about accountability cannot resolve these legislative choices.

Smaller enterprises need practical compliance routes, including standard contractual clauses, shared technical resources, and proportionate assurance. Regulatory experimentation should include safeguards and monitoring rather than suspend responsibility for foreseeable harm. Innovation and redress can develop together when businesses know what reasonable conduct requires and affected persons have a credible route to challenge consequential errors.

Institutional learning should also follow an incident. Investigation needs to distinguish an isolated data error from a defect affecting an entire class of decisions. Companies should preserve evidence before changing the system and assess whether earlier outcomes require reconsideration. Appropriate reporting arrangements can help regulators identify recurring patterns across suppliers and sectors. Public disclosure must remain proportionate and protect personal information, but commercial embarrassment should not determine whether serious risks reach competent authorities. Follow-up should test whether corrective measures work rather than regard the publication of a revised policy as sufficient. This approach connects liability with prevention: evidence obtained after one failure can reduce the likelihood that the same problem injures others. It also gives organisations a practical reason to examine complaints as sources of knowledge rather than merely as reputational threats.

CONCLUSION

Corporate liability for AI-driven decisions should respond to the organisation's legally relevant choices throughout development and use. Existing law offers important foundations, but fragmented responsibility and unequal access to evidence can weaken remedies. Comparative experience supports clearer duties, proportionate records, meaningful review, and careful differentiation between prevention, sanctions, and compensation. Liability must remain connected to the requirements of the particular claim. A sustainable framework enables

beneficial adoption while ensuring that technical complexity does not leave injured people without explanation, correction, or appropriate redress.

FUTURE SCOPE

Future research should examine actual disputes involving healthcare, recruitment, lending, and autonomous transactions. Empirical studies could assess whether complaint procedures and independent audits improve outcomes. Comparative work should explore cross-border enforcement, collective harm, insurance, and changing vendor relationships. Further attention is needed to interactions between multiple agents and responsibility for subsequent system updates. Reform should be evaluated through its practical effects: whether it prevents avoidable injury and makes remedies available to those who need them.

References

1. Berle, A. A., Jr., & Means, G. C. (1932). *The modern corporation and private property*. Macmillan.
2. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433–460. <https://doi.org/10.1093/mind/LIX.236.433>
3. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
4. Companies Act 2006, c. 46 (UK). (2006). <https://www.legislation.gov.uk/ukpga/2006/46/contents>
5. Companies Act, No. 18 of 2013 (India). (2013). Government of India.
6. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
7. NITI Aayog. (2018). *National strategy for artificial intelligence: #AIForAll*. Government of India.

8. Consumer Protection Act, No. 35 of 2019 (India). (2019). Government of India.
9. Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449; amended 2024). <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
10. NITI Aayog. (2021a). *Responsible AI #AIForAll: Approach document for India. Part 1—Principles for responsible AI*. Government of India. <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>
11. NITI Aayog. (2021b). *Responsible AI #AIForAll: Approach document for India. Part 2—Operationalizing principles for responsible AI*. Government of India.
12. United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
13. Digital Personal Data Protection Act, No. 22 of 2023 (India). (2023). Government of India.
14. Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-1>
15. U.S. Equal Employment Opportunity Commission. (2023, September 11). *iTutorGroup to pay \$365,000 to settle EEOC discriminatory hiring suit*. <https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit>
16. Council of Europe. (2024). *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>

17. European Parliament & Council of the European Union. (2024a). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
18. European Parliament & Council of the European Union. (2024b). Directive (EU) 2024/2853 on liability for defective products and repealing Council Directive 85/374/EEC. *Official Journal of the European Union*, 2024/2853. <https://eur-lex.europa.eu/eli/dir/2024/2853/oj>
19. Ministry of Electronics and Information Technology. (2025a). *Digital Personal Data Protection Rules, 2025*. Government of India. <https://www.meity.gov.in/digital-personal-data-protection-rules>
20. Ministry of Electronics and Information Technology. (2025b). *India AI governance guidelines*. Government of India. <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf>