International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 28-02-2026; Accepted: 30-03-2026; Published: 14-04-2026
Volume 8, Issue 2, 2026, Page No. 46-51

Corporate liability for AI-driven decisions: A comparative study

Kapil Chaprana
Department of Law, ICFAI University Dehradun, Uttarakhand, India

Abstract
The growing incorporation of Artificial Intelligence (AI) in business strategy and decision-making introduced Substantial moral and Judicial dilemmas particularly concerning liability for AI- driven actions. The use of Artificial intelligence to inform business decision making will create new legal issues that may push the limits of current legal frameworks for holding entities liable. This article will identify the current state of liability under which companies are responsible for damages caused by their AI, as well as to what extent previous models of liability such as negligence, strict liability, and vicarious liability can be applied to AI algorithms. One factor that creates substantial difficulties for establishing proximate cause or foreseeability, both of which are fundamental components of tort law, is the "black box".
To determine whether there are differences in regulation across different countries regarding AI and its use as a tool for business decision making, this article will compare the regulations from major markets around the world including India, China, Canada, Europe and the U.S., focusing on the European Union's regulatory approach through the AI Act and the revision to its Product Liability Directive.
As companies become increasingly reliant on AI for all types of strategic and operational decisions, this article identifies several gaps in current regulatory approaches and provides guidance on future development of robust, fair liability regimes that allow for continued technological innovation while also holding companies responsible for the decisions made by their AI.

Keywords: Artificial Intelligence (AI), corporate liability, AI governance, algorithmic decision-making, negligence, strict liability

Introduction

The speedy development and deployment of Artificial Intelligence technologies have transformed main industries such as finance, government healthcare, legal services, astrology and corporate decision-making process. AI driven systems help in saving time, giving important benefits in speed, efficiency, and accuracy in decision making. The Artificial Intelligence has radically changed the way in which traditional organizations or large corporations or MNCs operate as well as changing how businesses are being conducted. It has changed the way of taking decisions which was previously made through human intellect. These systems provide predictive decisions, predictive patterns, and predictive healthcare analytics through automatic hiring systems, credit scoring systems, to self-driving cars, and process vast quantities of data. The technologies are efficient and can reduce costs, but it raises critical legal questions about Corporate liability when AI driven decisions result in harm, discrimination, regulatory breaches, discriminatory employment decisions, erroneous medical recommendations, or autonomous vehicle accidents, a very important question emerges: Who should bear legal responsibility and held responsible? Is it up to developers who created it, the corporation who is deploying, to the providers of data, or the AI itself?
Corporate liability for AI decisions has become a pressing issue as governments and Judicial scholars grapple with the implications of machine-based decision-making. Traditional legal doctrines-such as strict liability, Negligence, and vicarious liability were designed for human actions and intent. The autonomous nature of AI challenges these principles, necessitating a revaluation of legal frameworks. Additionally, corporations must navigate regulatory landscapes that vary across jurisdictions, with some countries introducing AI specific laws while others rely on existing product liability statutes.
This article undertakes a comprehensive comparative analysis of how major countries like European Union, United States, India, China are adapting liability doctrines, such as negligence, product liability, and vicarious liability to address AI-driven corporate decisions. This study analyses challenges such as black box, foreseeability, accountability and transparency gaps.

Traditional Liability Doctrines

Liability for corporate actions through use of Artificial Intelligence will initially rely on established legal principles for human conduct and conventional products. However, there are significant barriers to adapting existing liability theories to autonomous systems which operate using opaque algorithmic systems.

1. Negligence

Negligence remains the predominant liability theory under common law jurisdictions. In this proof of duty of care, breach of that duty, causation and damages must be demonstrated. In the AI context, courts focus on determining whether the corporation has acted responsibly in selecting, implementing, monitoring and maintaining their use of AI systems. Courts will have to evaluate if damage was reasonably predictable, and if so, if the corporation failed to meet the expected standards of a corporation using comparables technology. However, determining whether a corporation is negligent becomes difficult when the manner in which an algorithm makes decisions is unknown due to lack of transparency and when AI exhibits emergent characteristics that are not anticipated at the time of either design or deployment.

2. Strict liability

Strict liability imposes responsibility without requiring fault to be proven; traditionally applied to activities that involve an unreasonable risk of danger or defective products. Supporters believe that strict liability would be especially useful for high-risk AI systems because it provides victims easier access to remedies, eliminates the need to prove negligence where there is ambiguity about the causal connection between an injury and a defendant's activity, and encourages companies to develop safety features into their products. The European union's new Product Liability Directive has moved closer to imposing stronger obligations upon AI systems defined as products than under existing law; this reduces barriers to recovery faced by victims. Opponents fear that applying strict liability too broadly may discourage innovation by placing undue risk on those developing and deploying beneficial forms of AI.

3. Vicarious liability

Vicarious liability makes employers responsible for wrongful acts performed by employees while performing duties within the scope of their employment. This form of corporate liability for AI occurs when the AI system functions as an agent or tool for the corporation. But the application of vicarious liability is uncertain when AI systems make many of their own decisions independently of humans who have control over them or intervene in their operation.

It also raises the issue of whether an AI system can ever be viewed as an employee or agent in the way that traditional liability has been understood when both its decision-making process is unclear and its actions unpredictable.

4. Product liability

Product liability regimes typically involve legislation that provides that manufacturers who create and sell defective products that result in harm will be held accountable……. Product liability frameworks has evolved into statutory provisions in many countries, including EU Member States via legislation such as the EU Product Liability Directive, and U.S. states via enactment of specific product liability statutes. By extension, application of product liability to AI creates new complexities including (1) whether AI software is a "product," (2) what defines a "defect" in a learning system whose behavior changes after it has been deployed, and (3) how liability should be apportioned among developers, manufacturers, distributors, and deployers. More recently, EU reform efforts have clarified these points through defining software and AI systems as "products" and modifying the definition of "defects" to accommodate behavior generated through algorithms.

However, these traditional theories are limited to attributes Ai liability therefore scholars and policymakers have proposed AI- specific liability frameworks also laws are emerging such as EU act. that address the unique characteristics of algorithmic systems. Such as operators Liability model which determine that the corporations who deploys and use AI bears primary liability for harms. No faul and compensation fund schemes have been proposed to compensate AI harms victims.

Key Legal Challenges in AI Liability

1. **The "Black Box" Problem:** The term "black box," as used here, relates to the fundamental opaqueness of many artificial intelligence (ai) systems – especially those relying on deep learning and neural networks – as the relationships between input and output cannot be reasonably explained by anyone who created the system. Opaque systems create serious barriers to legal accountability. For example, if an organization's ai system produces a discriminatory hiring decision, denies a loan request or creates a medical error; determining what caused the decision and whether the decision was wrong becomes almost impossible.

1.1 Opaque Algorithmic Decision-Making Manifests Itself in Multiple Ways.

a. Technical Opacity: Technical opacity arises from the mathematical complexity of models having millions or billions of parameters which make it nearly impossible for humans to comprehend the decision pathway produced by the model.

b. Intentional Opacity: Developers intentionally hide the logic behind their algorithms to preserve trade secrets and/or competitive advantages.

c. Emergent opacity: It exists when machine learning systems produce decision strategies that were not pre-programmed (especially in reinforcement learning), optimizing performance based upon objectives that were not previously identified.

1.2 Legal Implication: Substantial Tort law's negligence framework requires plaintiffs to prove that defendants failed to exercise reasonable care, generally requiring plaintiffs to show that specific actions or inactions constituted a failure to meet reasonable standards. When the decision-making processes of an organization's ai system are opaque, plaintiffs cannot identify any failures in the design of algorithms, training data selection, deployment practices etc. Likewise, defendants cannot easily demonstrate that they exercised reasonable care if they cannot explain how their ai systems produced decisions.

2. Challenges Related to Causation and Foreseeability.

a. Causation: In most liability theories, demonstrating causation – the connection between defendant's conduct and plaintiff's harm – is essential. Ai systems complicate analysis of causation in several ways. First, ai-driven decisions result from complex interactions among algorithms, training data, deployment contexts and human intervention creating a "problem of many hands" where responsibility is diffused across multiple actors. Second, the opaqueness of algorithmic decision-making makes it difficult for litigants to trace specific harms to specific components or design choices within an organization's ai system. Third, AI systems may exhibit behaviours during post-deployment operations which were not present during development or testing raising questions about whether such behaviours were reasonably anticipated.

b. Foreseeability: whether a reasonable person would have been able to predict/anticipate the harm — is critical to determining whether a defendant acted negligently. Ai systems challenge foreseeability in numerous ways. Models trained on historical data can perpetuate or amplify biases that developers did not anticipate. Systems deployed in novel environments may encounter edge cases or adversarial inputs that cause unexpected behaviour. Systems that learn and adapt post-deployment may develop decision strategies that diverge significantly from those originally programmed by the developer. Regulators have begun addressing these problems through modified evidentiary standards. The proposed EU AI Liability Directive includes disclosure obligations for evidence as well as presumptions regarding causality when operators fail to comply with safety obligations. Some scholars recommend shifting towards probabilistic causation standards or burden-shifting frameworks that require defendants to disprove causality once plaintiffs establish prima facie harm resulting from an organization's use of ai systems.

3. Transparency and Explainability Requirements

Realizing that lack of transparency undermines accountability, regulators have increasingly mandated transparency and explainability for high-risk applications using ai technology. The EU ai act requires organizations developing high-risk ai systems to design them so that users will be able to interpret outputs and use systems properly. The General Data Protection Regulation (GDPR) provides individuals with rights to meaningful information regarding algorithmic decision-making logic as well as the right to contest automated decisions having significant effects upon them. Requirements for explainability serve multiple legal purposes. Explainability requirements enable affected parties to understand why decisions made by an organization's ai system were made and support affected parties' ability to challenge decisions providing additional support for fairness in procedures and due process. Explainability requirements also provide regulatory agencies with oversight mechanisms allowing auditors to determine compliance with relevant laws. Finally, explainability requirements support determining who is responsible for harm causing events by creating document trails that can be used in litigation. However, explainability requirements face practical and conceptual obstacles. Technical limitations exist for fully explaining complex neural networks and therefore providing comprehensive explanation. Conflicts can arise between trade secret protections and transparency obligations. Furthermore, explanations provided can mislead if they oversimplify complex systems or if systems are designed to generate plausible but incorrect explanations. To address these tensions, legal frameworks increasingly employ risk-based approaches imposing stricter transparency obligations on higher-risk uses of ai while providing greater flexibility for lower-risk uses. Documentation requirements including records of training data, model architecture, testing protocols and deployment contexts provide alternative accountability mechanisms when full explainability is unfeasible.

Comparative Study of Nations

Some nations are developing regulations that embrace AI risks and harm caused by autonomous and algorithmic driven technology.

1. Europe

Europe would be the first country to enact an Artificial Intelligence Act and the AI Liability Directives. They are using a high risk-based model. It is all about establishing a framework of risks. AI system is considered as high risk under this model. For example, if an AI system is classified as a "high risk," then it includes technologies like biometric scanning, self-driving cars, and medical diagnostics used by law enforcement. If you identify something as a high-risk product or service, you're going to require those providers to follow more rigid guidelines regarding compliance with regulatory requirements and liability for any injuries or damage resulting from the products or services provided. So in essence, the EU is transferring the burden away from the victim and onto the provider to demonstrate causation and ensure that individuals who were injured receive compensation rather than being mired in paperwork.

1.1 The New Product Liability Directive and the EU Artificial Intelligence Act.

The adoption of the European Union's Artificial Intelligence Act (AI Act) is a major step forward for regulating technology internationally. The AI Act has been enacted by the EU and is scheduled to go into effect in 2026. The Act provides a risk-based method for classifying AI systems as acceptable risk, high risk, low risk, or no risk. Each classification comes with its own regulatory requirements commensurate to the level of potential injury or property damage that an individual could suffer due to an improperly functioning AI system. While the AI Act is not a law of the United Kingdom, it is expected to have a substantial extraterritorial impact: U.K.-based companies that sell AI systems to consumers within the EU, collect personal data relating to EU residents, or otherwise interact with EU residents through AI systems, will fall under the purview of the AI Act. A number of the most important provisions of the AI Act directly address the regulation of high-risk AI systems, including recruitment processes, credit scoring models, biometric identity verification methods and critical services. Companies utilizing such high-risk AI systems will be required to implement thorough risk assessments and mitigation strategies, maintain records of tracing and recording activities related to the development of the AI system, ensure that human operators possess control over the entire lifecycle of the AI system and adhere to strict data governance policies. Failure to comply with such provisions may result in severe penalties in the form of fines of up to €35 million, or 7 percent of global revenue; the penalty regime of the AI Act mirrors that of the General Data Protection Regulation. What makes the AI Act particularly noteworthy is its extraterritorial reach; the Act applies to both U.K.-based companies providing AI systems to EU consumers and processing data regarding EU residents. As such, U.K. companies should begin adjusting their internal policies and technological approaches in anticipation of increasing transnational legal exposures. The New Product Liability Directive (2024/2853) supplements the Act by bringing current product liability laws up-to-date to include software and AI systems. Like the Act itself, however, the

Directive is not a law of the U.K., yet it is likely to affect U.K. firms doing business in the E.U.

2. Canada

There is the emergence of legal precedent. The Moffatt v Air Canada case [2024], in Canada, courts found integrators responsible in instances where AI-based tools led to consumer harm, even in cases where the AI was considered an internal operation (i.e. a chatbot on a webpage). While the Moffatt case is not binding in the U.K., it demonstrates a judiciary willingness to impose liability upon parties operating within an environment that utilizes AI – which may be persuasive to U.K. courts. This notion is consistent with resolutions made by members of the EU Parliament indicating that entities that utilize AI systems should bear the risks associated therewith and therefore should be legally liable. Therefore, directors should accept ownership of the deployment environment and have sufficient knowledge of how AI operates as well as its capabilities and possible negative consequences. To facilitate their oversight responsibilities as it relates to implementing and monitoring AI, Clifford Chance (2024) recommends that Boards build knowledge regarding the advantages and disadvantages of AI. This does not mean that directors should become technical experts themselves; rather, they should be knowledgeable enough to ask the appropriate questions, scrutinize risk assessments and interrogate technical assumptions. Furthermore, Boards have an obligation to create and monitor internal governance structures that include auditable trails for algorithms used in decision-making processes, inter-disciplinary reviews of compliance with relevant regulations and other applicable laws and regulations and escalation procedures for matters related to AI

3. United States

The United States of America has a federal regulatory regime for artificial intelligence (AI), however, there is not a single statute addressing the issues associated with AI. Instead, Courts apply the same tort doctrines and other common law doctrines that have historically been used to determine liability when parties suffer injury or loss due to the actions or inactions of another person. Judges do so on a case-by-case basis. Using this flexible method, judges can apply existing statutes to new technologies; nevertheless, such an approach is unequal. Recently, in the United States, citizens are now questioning how to make algorithms responsible, transparent and unbiased, given the potential that AI may greatly affect society.

4. China

China has developed a series of specialized regulations governing AI across several sectors. For example, China has developed a serious recommendation system, a deepfake technology and several data-driven platforms. These regulations require businesses using these technologies to be transparent about the development and implementation of such technologies. Furthermore, businesses are required to obtain consent from users prior to collecting and processing personal data. Finally, these regulations require businesses to provide mechanisms through which users can report complaints. While the Chinese approach is less theoretical than those of the U.S. and India, the Chinese government's approach demonstrates that effective regulations can help minimize damage caused by AI. Furthermore, it shows that simply sitting idly waiting until AI becomes uncontrollable is unnecessary and that proactive steps can be taken at relatively early stages to positively impact the outcomes resulting from AI.

5. India

While India has formally discussed developing an expansive liability scheme for AI, thus far, no legislation has been enacted. Therefore, while the Indian judiciary continues to apply established tort law principles that were never intended to govern certain complex AI systems, there is no comprehensive statute regulating AI in India today. Rather, questions regarding liability for harm resulting from AI are addressed through a fragmented collection of current legal provisions scattered throughout constitutional law, tort law, consumer protection law, information technology law and industry-specific regulations. Although this piecemeal structure is somewhat successful, it is increasingly inadequate for handling the sophisticated and autonomous nature of systems driven by AI. Liability issues with respect to AI are generally dealt with indirectly via application of general laws, specifically:

Law of Torts: Statutes such as negligence, strict liability and vicarious liability can be invoked where harm is caused by AI systems. However, establishing fault and causation and demonstrating reasonable care regarding AI decision-making processes is particularly challenging due to the technical and non-transparent nature of AI systems.

Consumer Protection Act, 2019: This law guarantees solutions to flawed products and inferior services, which can be applied to AI-powered products and services. However, the Act is silent on systems that will evolve or change their behaviour once it has been deployed.

Information Technology Act, 2000: The Act establishes standards for protecting data and cyber security issues; additionally, the Act determines the liability of intermediaries involved in AI disputes. However, the scope of the Act is limited in determining responsibility for decisions made autonomously by systems that continue to learn and develop.

BNS 2023: The BNS provides criminal liability based upon mens rea. Since AI systems lack both conscious intent and awareness, determining criminal liability for AI-related damages presents significant challenges. Like the above-mentioned statutes, each statute represents a separate solution to individual problems, none of which were created in consideration of autonomous and learning systems. Consequently, substantial gaps remain in the body of regulations governing AI.

How corporations can reduce liability.

Corporation has to implement proactive governance in order to minimize legal exposure.

1. **AI Risk Assessments:** Performing routine assessment of possible harms prior to and following adoption.
2. **Accountability through Governance:** Establishing clear internal policies defining roles and responsibilities for AI deployment.

3. **Risk-Based Regulation:** Applying stricter liability and oversight for high-risk AI applications, such as healthcare or finance.
4. **Human Oversight:** Making sure that high stakes decisions are meaningfully reviewed by humans.
5. **Bias Testing:** This involves the use of audits to help in identifying discriminatory trends.
6. **Transparency Policies:** This means having a clear description of how AI is used to the affected people.
7. **Board-Level Supervision:** Adding AI oversight to corporate governance frameworks.
8. **Collaborative Liability:** Developing joint liability models among developers, operators, and corporations to reflect shared responsibility.

Such measures not only minimize liability but also increase the confidence of the population.

AI Liability Law Directions in The Future.

Currently, AI liability law faces unique challenges. future directions in AI liability law involve creating more tailored regulations that consider AI's distinct nature. One approach is to establish clear rules for transparency and accountability in AI development, ensuring that creators can foresee and mitigate risks. Another emerging idea is the concept of AI legal personality, where highly autonomous systems might hold limited legal rights and responsibilities. Additionally, international cooperation will be essential, as AI technologies often cross borders Future reforms may include:

1. Better distribution of the risks between developers and deployers,
2. Compulsory high-risk AI insurance programs,
3. Increased transparency and explainability demands,
4. Allowing highly autonomous AI systems to bear rights and responsibilities,
5. Implementing strict safety protocols and risk assessments for AI deployment,
6. AI standards harmonization at the global level.

Finally, the reform aims to strike a balance between innovation and responsibility. Excessive strict liability may deter technological advancement, whereas lack of regulation may subject people to danger.

Conclusion

Corporate liability for decisions made by artificial intelligence is a developing and complex area of law which will continue to be shaped by societal values, legal traditions and technological advancement. Analysis between jurisdictions has also exposed differing approaches from fault-based systems to precautionary regulations with emphasis on transparency and human oversight for corporate use of AI. In order to proactively manage risk in relation to liabilities associated with the use of AI by corporates they must put governance frameworks in place alongside mechanisms for risk assessments and compliance. Legal systems will continue to adapt to balance the benefits of innovation with protection against potential harms caused by the use of AI. Traditional liability rules provide some initial guidance for how to develop corporate liability for AI driven decision-making. However, these rules need to be adapted for the autonomy, opacity, un-predictability and distributed responsibility. The Black Box Problem is particularly problematic as it severely limits the ability to demonstrate causation and fore-see-ability. Therefore, new or amended liability frameworks will likely have elements of presumption of causality, burden shifting and obligations to disclose information. Corporations will need to allocate responsibilities clearly and implement adequate oversight of their use of artificial intelligence. Additionally, companies will need to ensure that members of their boards and senior executives understand the role of artificial intelligence in their business. As a result, directors and officers may now be exposed to greater potential liabilities if there are failures in AI governance. There is currently no corporate criminal liability doctrine that addresses harms caused by AI that do not otherwise involve a criminal intent.

At present, none of the jurisdictions examined have created satisfactory liability regimes. Challenges remain including evidentiary asymmetry, the lack of international cooperation regarding standards for AI related harms, the tension between encouraging innovation and ensuring accountability for those who create and utilize AI systems and fundamentally whether AI can ever be considered an agent capable of being held liable. For all of these reasons, future development will depend on continuing regulatory experimentation and learning. This study confirms that there is a need for clear, adaptive and collaborative legal frameworks to facilitate responsible global economic deployment of AI by corporation.

References

1. Henz P. Ethical and legal responsibility for artificial intelligence. Discover Artificial Intelligence, 2021, 1.
2. Kovač M. Autonomous artificial intelligence and uncontemplated hazards: towards the optimal regulatory framework. European Journal of Risk Regulation,2021:13:94.
3. Anusuya P. Legal liability of AI systems: who is accountable? International Journal for Multidisciplinary Research, 2025, 7.
4. Sharma R. Governance and oversight of AI systems. Apress eBooks, 2024, 353.
5. Gambhir M, Mehra S. AI liability and accountability: a review of emerging legal frameworks. International Journal of Science and Research,2025:14(1):1234–1245.
6. Şamil A. Legal liability of artificial intelligence operators: a global analysis. Zenodo, 2025.
7. Singh R. Legal implications of artificial intelligence: navigating the future. REDVET,2024:25(2):145–167.
8. Araromi T, Johnson K. Determination of tort liability in the deployment of artificial intelligence technology. Journal of Law, Policy and Globalization,2024:141:28–39.
9. Soyer D, Özkan I. Artificial intelligence and civil liability: do we need a new regime? International Journal of Law and Information Technology,2023:31(2):156–178.
10. Ertan B. Artificial intelligence and liability for damages. Uluslararası Sosyal Bilimler Dergisi,2025:9(41):234–256.
11. Bashayreh M, Alshibly H. Artificial intelligence and legal liability: towards an international approach of proportional liability based on risk sharing. Information and Communications Technology Law,2021:30(3):210–234.

12. Marchisio S. In support of no-fault civil liability rules for artificial intelligence. AI and Society,2021:36:1243–1256.
13. Nanayakkara R. Navigating AI risks: civil liability for physical damage in Sri Lanka: a comparative perspective. Sri Lanka Journal of Legal Studies,2024:12(1):45–67.
14. Dantas C, Silva M. Liability regulations and respective challenges in the European Union regarding the use of artificial intelligence tools. Zenodo, 2025.
15. Ampovska M. European Union civil liability frameworks in the age of artificial intelligence: assessing current regimes and future prospects. Vestnik Sankt-Peterburgskogo Universiteta,2024:15(2):312–334.
16. Scheufen M. Künstliche Intelligenz und Haftungsrecht: die e-person aus ökonomischer Sicht. Wirtschaftsdienst,2019:99(6):415–420.
17. Cutolo G. Corporate criminal liability and artificial intelligence: doctrinal overview, problems and perspectives. Open Access Journal of Criminal Investigation,2024:16(1):1–12.
18. Diamantis M. The extended corporate mind: when corporations use AI to break the law. North Carolina Law Review,2020:98(4):893–962.
19. Diamantis M. The extended corporate mind: when corporations use AI to break the law. Social Science Research Network, 2019.