CORPORATE LIABILITY IN THE AGE OF ARTIFICIAL INTELLIGENCE: RETHINKING ACCOUNTABILITY FOR AI AND MACHINE LEARNING SYSTEMS

Achsah Mary JO, BCOM LLB, Christ Academy Institute of Law, Bengaluru

ABSTRACT

The introduction of Artificial Intelligence (AI) and Machine Learning (ML) technologies produced profound societal changes. For instance, an AI technology can analyze vast amounts of data and a Machine Learning technology can make predictive analyses. Together, they open novel and highly productive opportunities in economically critical industries such as healthcare, finance, insurance, and education. Consequently, they create unprecedented levels of advancement and expansion. The potential of Machine Learning and AI must, however, be tempered. Transparency, accountability, and fairness are some of the equally important yet challenging issues that come with the advancement of such technologies. Some of the most critical of societal constructs become compromised, if not eliminated, by the Machine Learning and AI systems in 'real time' use. The 'Black Box' phenomenon aptly describes critical constructs of accountability and responsibility, as well as the intricacies of the automated decision systems of AI technologies. When harm occurs in a decision system, the decision algorithm offers no clear accountability.

As more and more automated systems undergo use in organizational decision systems, the systems' radical autonomy raises fundamental legal questions. In particular, a liability gap is created and the answer to the age-old question of 'who is liable' (the programmer, the AI or the corporation?) in a novel context of machine AI is still eluding the legal system. In this paper, we analyze the questions arising from the liability gap.

Corporate liability reform in the era of AI is both a requirement under law and social obligation. The art of correlating technological advancement and fairness, equity, and decency to humankind will ultimately determine whether or not AI enhances or erodes legitimacy in corporate governance in the 21st century. Therefore, this paper addresses how corporate liability laws must evolve to address accountability for harms or decisions arising from autonomous AI systems.

Keywords: Artificial Intelligence, Machine Learning, Corporate Liability, Accountability, Transparency, Black Box Phenomenon, Corporate Governance.

1. Introduction

'With great power comes great responsibility' – Elon Musk

The popularity of the artificial intelligence and machine-learning technologies in the context of a broad spectrum of businesses necessitate the revision of the current provisions of corporate liability[1]. Although digital tools can entirely revolutionize many industries, they create complex safety challenges and underlying rights-related challenges that the existing legal framework is unprepared to handle. The situation is even more complicated when AI systems are more autonomous and capable of making choices and decisions that do not align with the traditional principles of fault and causality, thus compromising current risk-assessment models[2].

Also, the frequently unclear relationships between developers, service providers, and final us ers hinder the consciousness of the division of duties in the independent decision-making procedures [3]. Therefore, human mistakes are less likely to be the cause of errors than rather a complex intra-system interaction. The suggested revision in the legislation aims to align the traditional tort law with the dangers of AI by addressing an extremely challenging task of retrieving evidence and assigning causation that, otherwise, are virtually impossible to achieve in an AI-related case.

2. The Evolution of Corporate Liability

2.1 Traditional Doctrines of Corporate Liability

A number of core theories have developed to address the inherent tension between a corporation's artificial legal identity and the human purpose required to commit a wrongdoing.

[1] *Jorge Llorca, Pablo Martínez & Carlos López, Corporate Accountability and Artificial Intelligence: Challenges for Global Governance, 38 AI & Soc'y 1021 (2023).*
[2] *Giusella N. Diega & Maria Bezerra, AI, Autonomy, and Liability in Emerging Technologies, 39 J.L., Tech. & Ethics 115 (2024).*
Ying Wang, Autonomous Decision Systems and the Future of Legal Causation, 38 Harv. J.L. & Tech. 421 (2025).
[3] *Takashi Okuno & Rin Okuno, Distributed Agency and Responsibility in Machine Learning Ecosystems, 17 Law, Innovation & Tech. 54 (2025).*

For instance, the **Doctrine of Attribution** developed to address the initial problem that a company could not be prosecuted for a crime because it lacked a human mind. In this instance, courts started to "pierce" the corporation's corporate veil, attributing to the corporation itself the intent and conduct of the company's "directing mind and will"—which applied to the directors or top executives [4]. In Lennard's Carrying Co. Ltd. v. Asiatic Petroleum Co. Ltd. [5], the court determined that corporate accountability occurred when the actions or inactions of individuals in charge mirrored those of the corporation, providing a clear illustration of how this theory operates.

Concurrently, American case law gave rise to the Doctrine of Respondeat Superior [6], also known as vicarious liability, which permits a corporation to be held accountable for the unlawful acts of its employees that are committed while the company is conducting business.

The doctrine mandates that an employee's actions be at least partially intended to benefit the firm, even though this may not have been expressly sanctioned by management or the corporation's governing body.

2.2 Challenges of Emerging Technologies

AI and machine learning are transforming business. AI is being used to prepare for the future, detect rule violations, assess risks, and make decisions. When AI takes on these responsibilities, we must consider who is in control, whether we can predict what it will do, and how we will handle it. Correctly developing legal regulations is critical.

When AI functions autonomously, it becomes more difficult to demonstrate mens rea (guilty mentality). When an algorithm's autonomous judgments result in issues such as discriminatory employment practices, faulty investment forecasts, or inappropriate data utilization, it might be difficult to assign blame to the human developer, user, or firm that deployed the system. Traditional legal theories based on human agency and decision-making are significantly impacted by these accountability gaps.

Legal conversations throughout the world are increasingly focused on ways to build AI-specific

[4] *Paul Davies, Corporate Law and Accountability in the 21st Century (Oxford Univ. Press 2020).*
[5] *Lennard's Carrying Co. v. Asiatic Petroleum Co., [1915] A.C. 705 (H.L.).*
[6] *Yavar Bathaee, The Artificial Intelligence Black Box and the Failure of Intent and Causation, 31 Harv. J.L. & Tech. 889 (2018).*

governance frameworks, such as explainability standards, algorithmic auditing, and required risk assessments, in order to narrow the liability gap. Even in countries like India, there is an increasing recognition of the need for AI governance policies that reframe corporate liability in an automated context while maintaining fairness and transparency.

Even though we previously had clear guidelines on corporate liability for human actions under traditional laws of accountability, we must eventually transition to shared liability models in which liability is shared between humans who develop and use AI technology and the technological systems themselves.

3. Understanding Artificial Intelligence and Machine Learning.

3.1 Overview

The extensive area related to creating computer systems that carry out tasks usually related to human intelligence - like learning, reasoning, and making decisions - is known as artificial intelligence (AI) [7]. AI systems can independently deliver information or take actions by examining and interpreting data. A significant aspect of artificial intelligence is machine learning, which emphasizes algorithms that enable computers to learn from data. These methods improve computer capabilities over time without the need for specific programming. Machine learning (ML) entails developing models that can identify patterns, forecast outcomes, and adjust to new situations. Neural networks and deep learning are regarded as more sophisticated approaches within the scope of machine learning.

3.2 Key Characteristics and Capabilities

The use of AI and machine learning is advantageous as it gives a chance to reveal the implicit patterns in big data records and render new information applicable. They are flexible, so they may be applied to help in decision-making, data organization, predictive modeling, and automation in various applications.

The machine learning algorithms are able to identify trends that can be employed to make better decisions. The applications are widely used in such fields as health care, translation services,

[7] *Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (4th ed. 2021).*

and finance. The deep learning implementation works in the areas of the perception of language and the perception of images.

In preparing and applying AI, the ethical concerns ought to be introduced in the initial phases. We should defeat bigotry and promote integrity, justice and secrecy. The greater the involvement aspect of the AI in the decisions, the greater the fact that the individual rights are highly important to safeguard. This is due to such significant actions as the need to know how AI can arrive at a decision, the need to protect personal information, and what should happen in the event AI commits an error. It is in addressing these problems that we will be able to safeguard the users and promote responsible AI development, and innovation will be safe and healthy.

4. Attribution and Causation Challenges in AI Systems

4.1 The Black Box Dilemma

It is a difficult task to determine who is liable in case of any malfunction in AI, partly because of the black box problem. A complex machine learning model such as a deep learning network is difficult to understand what happens within these models. They are usually hard to comprehend even by those that make them. These algorithms have an enormous number of layers and settings that change depending on learning and hence it is not easy to know why a decision was arrived at. When AI has made a mistake of some sort, there is simply a possibility to know why.

This ambiguity makes legal stuff more baffling like who has done it and what they should have done. Both rely on the facts of what a man should or should not do or who should blame. One such problem is when a self-driving car collides or a robot refuses to give loans to a person on the basis of biased information, courts will have a difficult time finding who is at fault, the coder, the organization or the AI. And even harder to check out things due to the fact that it is not really easy to keep secret source codes in order to safeguard business interests [8]. Moving towards the AI that can explain itself (XAI) and holding algorithms to account are some of the ways those in charge are attempting to mitigate these issues. The assumption here is that AI

[8] *Ryan Calo, Artificial Intelligence Policy: Ethics, Governance, and Accountability, 18 Ann. Rev. L. & Soc. Sci. 245 (2022).*

systems need to be audited and interpreted to find out who is in-charge in event of malfunction.

4.2 Distributed Responsibility and Multiple Participants

No longer is there a single company that deals with AI. The AI does not work alone and the actions taken by the AI are controlled by so many people, including data scientists, programmers, technology corporations, and those who use the systems I have observed that there are too many variables in the equation and it is almost impossible to identify a single villain when things go wrong. Even in case of an AI failure, such as a mistake, the offender might be as innocent as a mistake or a faulty code piece. That hesitation breeds a deeper mistrust that causes it to be difficult to keep anyone completely responsible.

By way of example, AI application in recruitment: the algorithm is more likely to end up with recruitment of candidates based on biased training data, and it is not always able to be adjusted to the needs of a particular organization. This brings into focus the fact that it is very problematic to use these systems in making vital decisions. Who is at fault? Who is presenting the data, who is the one developing the tool, or is it the company itself? Collective responsibility suggested by lawyers is provided based on the freedom of control and awareness of risks. There is a possibility that people creating AI tools will be held accountable in case of their design errors. The failures could be attributed to the users who might fail to monitor the AI. To resolve failures, the contracts should contain information on safety precautions i.e. the frequent inspections so that everybody is aware of his/her role and responsibility.

4.3 Foreseeability and Oversight

Consequently, the notion of being capable of foretelling what can occur and remaining within the framework has been an immense contention in tort and corporate liability legislation throughout a short period of time. However, now it becomes disorienting with AI. The point is that AI is constantly evolving due to the continuous learning process.

I continue to hear that AI is developing in a manner that we can hardly predict and to be truthful, the wilder aspects that emerge when it begins to self-create are frightening. The mere concepts of causal testing will most likely be lost in dilemmas of advanced algorithms and the procedure of finding the actual causative agents will become more of a nightmare. In addition to that, AI-based systems are increasingly becoming important in performing more tasks, seemingly at the

cost of conventional control systems.

The majority of users just implement AI systems and use them without putting strict controls, which raises the issue of carelessness in creating a stricter system of governance. I have read that despite the introduction of technologies like autonomous vehicles and medical technologies, regulatory agencies are considering adopting strict liability laws to overcome the natural impossibility of the artificial intelligences [9].

Also, the corporate bodies are also encouraged to keep a strict watch over the AI-based system, carry out frequent diagnostics, and thoroughly scan the code to rule out any unexpected situations. In general, the problems of prediction and management lead to the necessity of the new conceptual approach to causation. The model must consider the evolving and varying nature of AI systems that are constant [10]. The construction of such a model is essential to maintain the technological development and make it responsible, equitable, and properly regulated.

5. Re-evaluating Existing Liability Frameworks

5.1 Product Liability

Conventionally, product liability puts the producers in a bad position where any damage that leads to a fault is firmly placed on them but the type of AI complicates this ideology since software and AI systems can be developed or learn even when they have entered the market. The manufacturing firm or the beneficiary, who as a party have the greatest capacity and ability to alleviate a risk, is said to be liable in most of the situations but, developers, operators and other parties may be held liable, jointly or severally. The modern-day systems treat AI as a product subject to strict liability, such as the liability of the further software alteration or the ongoing learning and resulting defects. In most instances, the manufacturer or the primary beneficiary, which has the most control and ability to reduce risks, is considered liable, however, developers, operators and other parties may also be held liable either jointly or severally. This will be aimed at striking a balance between consumer protection and the necessity of encouraging risk reduction by the most qualified to handle it.

[9] *Llorca et al., 38 AI & Soc'y 1021 (2023).*
[10] *NITI Aayog, Responsible AI for All: Operationalizing Principles for Trusted AI (Gov't of India 2021).*

5.2 Negligence

AI negligence is about whether AI developers, those who use it, or those who put it to use, were careful enough when they made, tested, grew, and looked after the AI. To prove negligence, the person claiming fault usually has to show that the other party had a responsibility to be careful toward them, that they weren't careful enough, that this lack of care caused harm, and that they actually suffered harm. Courts will see if the people involved were careless in not predicting or reducing possible harm from what the AI did. Some scholars support a negligence framework, particularly in cases where AI behavior can be compared to human behavior, arguing that defendants should be liable if AI causes harm to the plaintiff because of carelessness in the AI's lifecycle. This fault-based negligence framework avoids default complexity from multiple stakeholders by identifying who did, or did not, fulfill their duty of care.

5.3 Strict Liability

Strict liability frameworks impose liability on specific parties regardless of fault, on the premise that certain activities are too high-risk to rely on the presence or absence of care. For example, some jurisdictions impose strict liability to an AI provider and deployer when using a "high-risk" AI, when it has caused physical or virtual damage. In particular, the proposed revisions to the EU Product Liability Directive would find AI providers and deployers strictly liable to a plaintiff for damages to third parties, even those under their control, when AI caused the damage or harm, regardless of whether they acted diligently or responsibly to prevent it. The only exceptions would be force majeure or recklessness on the part of the plaintiff.

5.4 Contractual Liability

Contractual liability is one where AI makes mistakes and cannot perform a duty that was established in a contract between two businesses, or a business and customers. In case AI stuff fails to perform as anticipated, the breach of contract may be asserted. There are plenty of AI contracts that attempt to restrict the responsibility, but they tend to not be able to escape an event that results in death or injury. In addition, when a company relies on AI to perform a task that is already part of a contract, it may become complicated to determine the number of errors that are acceptable and when the AI will be at fault. The contracts can help the companies to share the risk, but they must be prepared carefully to consider all the weird AI things.

6. Proposing New Frameworks for AI Corporate Liability

6.1 Risk-Based Approaches

This AI corporate liability plan focuses not on responsibility but on outcomes. It classifies AI systems as risky to individuals, society and critical systems. It is akin to the EU AI Act and other innovations. The plan ensures that the rules are suited to the risk. In super risky stuff, such as self-driving cars or medical tests, are more difficult to be responsible and open. The fewer the rules, the less risky the things are. The plan aims at auditing risks continuously, reporting potential issues to everyone, engaging external auditors, and updating the rules when the AI is updated. Companies should apply powerful internal management strategies such as ethics teams, individuals who are monitoring the AI, and what the AI may potentially do. This assists in addressing the risks in the functionality of the AI.

6.2 Developer and Operator Responsibility

The contemporary approaches to liability are also putting an increasingly heavier burden on the question of shared and varied accountability of the creators of AI models and their training, and the users who use these systems in practice in practice. The developers are recommended to ensure that the model is robust, to carry out resilience tests, to ensure transparency that is necessary by ensuring availability of documentation that can be in the form of data cards and audit trails as are in the U.S. Department of Homeland Security Roles and Responsibilities Framework. Rather, the authorities must look to ensure the risks, trial AI in practice, and a means to put a stop to things should they become erroneous. This is to imply that all people will be held accountable, whether it is during the collection of data or during the utilization of the system. All the participants must be cautious. Individuals who draw the rules are demanding that corporations should be accountable, transparent and can be monitored in the manner they are operated.

6.3 Insurance and Compensation Mechanisms

Insurance could be a nice method of addressing the dangers associated with AI. AI liability insurance can be seen as an insurance policy and a means to put a check on things. It can make those who are injured by AI get money quicker. In addition, it puts companies on their toes and makes them safer and rule-abiding.

By examining such factors as the complexity of an AI system, the extent to which it is autonomous, and the extent of damage that it might produce, insurers can estimate the riskiness of a given system. This is then used by them to charge insurance policies. Audit cards and system cards can provide the insurers with what they desire to view how risky matters are. In addition, reduced insurance premiums may encourage more responsible and open AI development, incorporating responsibility into the profits of the company.

All this helps to have a middle ground view on who is to blame when AI gets things wrong. It combines prevention, shared responsibility, and money stuff to promote new ideas without compromising the safety of the people as smart systems become an even larger part of our life.

7. Case Studies and Emerging Precedents

7.1 Autonomous Vehicles

The crashes of self-driving cars have altered the perception of companies in the eyes of the people. As a case in point, in 2025, Tesla was partially found guilty by a jury in a fatal crash involving Autopilot. The decision made by the jury was that Tesla was 33 percent negligent and should pay $243 million due to the marketing of the Autopilot made safety claims and the system was not designed properly. In this scenario, it is clear that there is the need to communicate risks and safe designs. Other companies that have received regulatory attention and vehicle recall due to accidents include Waymo and Cruise. The responsibility of the accident is still under dispute by lawyers as to whether it is the driver, the manufacturer or the software developer. It is a complex problem, particularly with cars that get full automated. All this underlines the necessity of introducing clear rules of liability, especially since AI is applied differently in self-driving cars.

7.2 Algorithmic Bias in Decision-Making

The presence of algorithmic bias cannot be considered extraordinary in such areas of life as recruitment, financial affairs, and policing. This is usually due to bad data or less-built model which will consequently result in unfair results. Judges are increasingly accepting the view that companies may encounter legal complications in the event of anti-discrimination and consumer protection legislation due to biased choices by their AI systems.

Based on the latest court decisions, the companies have to make sure that they are not biased,

well informed on the means by which their AI reaches their conclusions and resolve the emerging issues promptly. Regulators around the world are thinking or even enforcing regulations that require checks on fairness and transparency regarding the functioning of algorithms. They consider this to be a necessity of companies being responsible.

7.3 Cyber security Breaches Attributed to AI

The AI cyber security tools may be viewed as two sided swords. They enhance the security though they can leave loopholes with a possibility of further breach and abuse of information. Examples of evidence in the criminal law that show that companies are stable in the event of an AI security failure include failure to stop malicious AI attacks or failure to steal data using AI. The security of AI should be good in their risk management mechanisms. Be sensitive and prepared to act immediately whenever the cyber problem arises due to the malfunctions of AI.

8. Policy Recommendations and Future Directions

8.1 Legislative Reforms

The artificial intelligence is an issue that must be dealt with by legislators within the international community reworking the liability policies. They should cease to base on the part of blaming someone when something is not fine and in its turn, they focus on the individual who will assume the risk. This is particularly in the case of AI technology that can be of imminent destruction. The European parliament is driving towards being strict when it comes to the high-risk AI. It is projected to demystify accountability and make legal process easier and increase safer technology.

The governments should also create AI liability insurance, which will make the victims compensated even though it may not be easy to identify who is to blame. They could also borrow money to compensate. The new legislations must also foster transparency, trusted technology, human agency and confidentiality. They also must not be mistaken in other places as the rule of other places is the same.

8.2 Industry Best Practices and Standards

The first should be the leaders in the industries to practice AI governance. They can make their own laws, they are centered around the implementation of the AI in an ethical approach, and

they can create it to the good of the people, and they also make sure that they keep a check on the risks. Among the good ideas, some of them involve documenting the manner in which the AI is coming up with the decisions, to ensure that the decisions being made are not biased or risky and informing the workers about the decisions and educating them on the risks and AI regulations. The second approach towards controlling risks is the possibility of the insurance companies investigating the insurance of AI errors. In the short run, the standard-setting bodies will certainly be involved in the formulation of technical and ethical rules and regulations which will facilitate simpler AI systems verification and consequent confidence with the consumers and rule-making authorities.

8.3 Creating Codes of Conduct, Design, and Continuous Involvement Strategies

A good example of establishing and promoting corporate transparency is the emerging emphasis on regulatory compliance through a code of conduct. A code of conduct is an approach to implementing measures within the AI framework while having safe accountability measures and being endorsed by the organization for compliance. In the absence of legislated legal liability or regulatory standards around corporate liability, organizations can utilize codes of conduct as acceptable metrics of transparency and prevent breach of the standard of care or commitment to corporate social responsibility when operationalizing AI systems.

8.4 AI and a Code of Conduct

As corporate conduct is increasingly held accountable against standard codes of conduct, codes of conduct will increasingly be treated as regulatory compliance. As such there are two areas that codes of conduct can have an influence over within the AI framework. First, the AI framework is contingent on duty to attend to potential risk and duty to respond to those risks; for these duties, organizations can take pre-emptive measures to mitigate potential risk and emerge with standard in action. Second, as new AI applications emerge, even more accountability measures may emerge alongside those codes of conduct that emerge to align AI system use with existing human society and public values.

8.5 Insurance and Compensation Regulations

Policy solutions based on Insurance are emerging as a potential means of mitigating risk and loss arising from AI-related injuries. AI liability insurance, in many respects, serves as a

financial safety net for businesses, and regulates behavior through market mechanisms. It provides speedier financial compensation to individuals who have suffered bodily injury as a result of using AI-based methods, and incentivizes firms to exert greater energy toward customer safety and compliance with safety regulations. Insurers are increasingly testing innovative means to estimate the price of liability insurance, given calculated risks associated with different AI-based products or service applications regarding difficulty of implementation, autonomy, or physical harm. Additionally, policy-monitoring measures, such as system cards and audit cards allow insurers to better evaluate true exposures. Ethical design and consideration of safety regulations can also be subject to the impact of liability insurance.

9. Conclusion

The high rate of introducing artificial intelligence and machine learning in the business practi ces has expanded the range of actions that may be deemed as both lawful and morally accepta ble. The autonomy of AI has made it difficult to distinguish between what people intend to undertake and what machines are undertaking because of their own choice of systems and learn by themselves. The law sector and regulatory agencies are moving towards the realization that the application of automation does not undermine the responsibility of a business company; it increases it. This compels companies to reevaluate their management, risk management and ethical policies.

The use of automation does not reduce the corporate responsibility, instead, it reinforces it, an d more and more legal practitioners and regulatory agencies are acknowledging the fact.
However, new laws are also opened by these issues. New initiatives in the global community, such as the AI Act by the European Union, the revised Product Liability Directive, indicate a shift to risk-based and strict-risk approaches, with emphasis on openness, record-keeping, and customer protection. On the same note, such places as the United States and India are contemplating ambivalent approaches to the regulation of such a mix, business responsibility, developer obligations, and the imperative of verifying algorithms.

The legal environment is being changed due to corporate governance of AI.
At this point, corporate boards and executives should be careful about the artificial intelligenc e systems and demand that they are understandable and include ethical aspects in strategic mo dels. Such aspects as insurance and third-party liability will guarantee the people who suffer

due to AI being provided with the necessary support, and the developers will be taking the relevant risks.

The necessity to make corporate bodies responsible in the framework of artificial intelligence can be traced to a change in the fact that operational responsibility is more of an essential than just a set of rules of conduct that the company needs to follow; this is a paradigm shift in the corporate behavior. The necessity to make corporate bodies responsible in the framework of artificial intelligence can be traced to a change in the fact that operational responsibility is more of an essential than just a set of rules of conduct that the company needs to follow; this is a paradigm shift in the corporate behavior. The future of corporate liability with AI is determined by the necessity to strike a balance between the novelty of ideas and what is fair. Technology is supposed to be used in serving the society through promoting transparency, fairness, and accountability. The regulation clauses have to be changed alongside improvements of the AI-technology, which makes it obvious that corporate responsibility will be inclined towards the same direction as technological development.

REFERENCES

1. Books

- *Davies, Paul. Corporate Law and Accountability in the 21st Century (Oxford Univ. Press 2020).*
- *Goodfellow, Ian, Yoshua Bengio & Aaron Courville. Deep Learning (MIT Press 2016).*
- *Russell, Stuart, & Peter Norvig. Artificial Intelligence: A Modern Approach (4th ed. 2021).*

2. Journal Articles

- *Bathaee, Yavar. The Artificial Intelligence Black Box and the Failure of Intent and Causation, 31 Harv. J.L. & Tech. 889 (2018).*
- *Burrell, Jenny. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms, 3 Big Data & Soc'y 1 (2016).*
- *Calo, Ryan. Artificial Intelligence Policy: Ethics, Governance, and Accountability, 18 Ann. Rev. L. & Soc. Sci. 245 (2022).*
- *Diega, Giusella N., & Maria Bezerra. AI, Autonomy, and Liability in Emerging Technologies, 39 J.L., Tech. & Ethics 115 (2024).*
- *Gless, Silvia, Eric Silverman & Thomas Weigend. If Robots Cause Harm: Who Is to Blame?, 42 Oxford J. Legal Stud. 205 (2022).*
- *Jobin, Anna, Marcello Ienca & Effy Vayena. The Global Landscape of AI Ethics Guidelines, 1 Nat. Mach. Intelligence 389 (2019).*
- *LeCun, Yann, Yoshua Bengio & Geoffrey Hinton. Deep Learning, 521 Nature 436 (2015).*
- *Llorca, Jorge, Pablo Martínez & Carlos López. Corporate Accountability and Artificial Intelligence, 38 AI & Soc'y 1021 (2023).*
- *Okuno, Takashi, & Rin Okuno. Distributed Agency and Responsibility in Machine Learning*

Ecosystems, 17 Law, Innovation & Tech. 54 (2025).

- *Ramaswamy, Russell K. Corporate Criminal Liability and Vicarious Responsibility in India, 12 Indian J. Legal Stud. 77 (2022).*
- *Wang, Ying. Autonomous Decision Systems and the Future of Legal Causation, 38 Harv. J.L. & Tech. 421 (2025).*

3. Government / Institutional Reports

- European Commission. *AI Liability Directive Proposal: Harmonising Civil Liability Rules for Artificial Intelligence* (2024).
- European Parliament. *Directive on Civil Liability for High-Risk AI Systems* (2024).
- NITI Aayog. *Responsible AI for All: Operationalising Principles for Trusted AI* (Gov't of India 2021).

4. News Sources

- *Reuters. Tesla Liable for Partial Fault in Fatal Autopilot Crash, Jury Rules, Reuters (Feb. 10, 2025).*

5. Cases

- *Lennard's Carrying Co. v. Asiatic Petroleum Co.*, [1915] A.C. 705 (H.L.).