ALGORITHMIC ACCOUNTABILITY IN CORPORATE DECISION-MAKING: RECONSTRUCTING LIABILITY FRAMEWORKS FOR AI-DRIVEN GOVERNANCE

- Lakshya Kaushish* & Deepanshi Tiwari**

Abstract

The integration of Artificial Intelligence (AI) in business decisions, including strategic planning, hiring, and firing, has resulted in a significant accountability gap. Self-driving algorithm perpetrators are incapable of being held accountable by conventional legal systems, which are predicated on the actions and intentions of individuals. This doctrinal impasse exposes businesses to new risks and leaves the most vulnerable members of society, namely, the victims of biased or flawed AI, without any form of assistance. This paper suggests a liability framework for corporate governance that is AI-driven. The paper suggests a novel theoretical standard that is divided into two components. The initial prong establishes a new standard for the corporate duty of care by mandating Algorithmic Impact Assessments, independent "criterion" audits, and robust Explainable AI (XAI). The second section proposes a tiered liability system, expands product liability categories, and adds algorithmic oversight to fiduciary responsibilities. This research emphasises the "downtrodden concerns" of algorithmic bias victims to show how to ensure that technological advances are consistent with corporate responsibility, justice, and fairness.

Keywords*: Algorithmic Accountability, Corporate Governance, AI Liability, Legal Personhood, Algorithmic Bias, Product Liability, and Explainable AI.*

INTRODUCTION

The integration of Artificial Intelligence (AI) into the core of corporate governance is a big change in how organisations make decisions.[1] AI systems have evolved from automating

* LL.M.- O.P. Jindal Global University, Sonipat; Email: lak.kau01@gmail.com
** B.A.LL.B. (H)- Shri Ramswaroop Memorial University, Lucknow; Email: 15deepanshi@gmail.com

basic tasks to now playing a significant role in strategic planning, financial analysis, and even tasks that were previously performed by human corporate officers.[2] Companies utilise AI to optimise supply chains, check creditworthiness for loans, and sort through résumés during the hiring process, thereby promising unparalleled efficiency and data-driven insight.[3] Nevertheless, this technological advancement has surpassed the development of commensurate legal and ethical guardrails, creating a profound accountability vacuum.[4]

The primary inquiry that motivates this investigation is the reason why conventional law fails to address the harm caused by AI. When an autonomous algorithm persists in discriminating against job applicants, denying a loan based on biased data, or causing substantial financial losses, the conventional methods of assigning legal responsibility are rendered obsolete.[5] The complex, multi-actor ecosystem of AI development and deployment presents a challenge for our legal system, which is predicated on centuries of precedent regarding human agency, intent (*mens rea*), and foreseeability.[6] It is difficult to identify a responsible party in this environment. This is not merely a minor legal discrepancy that can be rectified.[7]

The resolution of this lack of accountability necessitates a meticulous and comprehensive reconstruction of the regulations that impose accountability on businesses. It is impossible to effectuate this type of transformation through incremental, independent reforms. Rather, it necessitates a multilayered strategy that integrates new substantive liability regulations with proactive procedural obligations. We can establish a governance framework that ensures that companies are accountable for the technologies they employ, that innovation is consistent with fundamental rights, and that individuals who are harmed have a genuine avenue to receive assistance.

---

[1] S. van der Zande, *et.al.*, "Artificial Intelligence in Corporate Governance: A Triptych", 13 *Erasmus Law Review* 1 (2020).

[2] R. Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, Cambridge, 2020).

[3] See Michael L. Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment", 164 University of Pennsylvania Law Review 871 (2016); M. Timmons, *et.al.*, "The Implications of AI in Corporate Governance", 178 *Journal of Business Ethics* 327 (2023).

[4] R. Abbott and B. Marchant, "The Reasonable Computer: Disrupting the Paradigm of Tort Law", 86 *George Washington Law Review* 1 (2018).

[5] Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap", 51 U.C. *Davis Law Review* 399 (2017).

[6] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, Cambridge, MA, 2015).

[7] M. E. Kaminski, "The Right to Explanation, Explained", 34 *Berkeley Technology Law Journal* 189 (2019).

THE DOCTRINAL IMPASSE: THE REASONS OLD LIABILITY RULES ARE INEFFECTIVE

The independence, lack of transparency, and lack of human nature of modern AI systems have resulted in the testing of long-standing legal doctrines in ways that they were not intended to handle.[8] The attempt to incorporate the new wine of AI into the old bottles of tort, contract, and corporate law demonstrates that these doctrines are fundamentally incompatible, resulting in a doctrinal impasse that systematically fails to assign responsibility for algorithmic harm.

A. The Breakdown of Corporate Law Analogies

Throughout history, corporate law has employed the concepts of fiduciary duty and personhood to ensure that individuals are held accountable. Both pillars collapse when autonomous AI is introduced.

1. A Digital Scapegoat for the Fiction of Legal Personhood

Legal systems grant corporations "*legal personhood*," which enables them to own property, sign contracts, and, most importantly, be held accountable in court. This is possible because corporations are ultimately managed and controlled by accountable human agents, despite not being individuals. It is doctrinally incoherent and perilous to propose that AI should be accorded the same rights and responsibilities as a human, such as "*electronic personhood*."[9] AI systems lack the subjective agency, intent (*mens rea*), and moral capacity that are essential for the existence of legal rights and obligations.[10] They operate on a data-driven logic that is devoid of the ethical reasoning that is associated with human accountability. For instance, AI is perceived as a legally incapacitated individual who is not subject to criminal liability in both Iranian and Saudi Arabian law.[11]

[8] *Ibid*. at 192.

[9] *See*, European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of Artificial Intelligence, Robotics and related technologies, Res. 2020/2012(INL) (Oct. 20, 2020).

[10] S. Chopra and L. White, *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press, Ann Arbor, 2011).

[11] A. Al-Ghamdi and M. Al-Shehri, "Criminal Liability of Artificial Intelligence: A Comparative Study of Iranian and Saudi Arabian Law", 12 *Journal of Intelligent Systems and Control Engineering* 24 (2024).

Consequently, the business analogy is no longer useful. An accountability shield would be established by granting AI personhood, allowing human creators and corporate deployers to transfer blame to a "*digital scapegoat with no assets, no morals, and no consequences*."[12] This would not address the accountability gap; rather, it would render it a permanent feature, providing individuals with a means to evade regulation rather than a means to obtain justice. The absence of legal personhood for AI is not a deficiency that necessitates closure; it is a simple fact. The individuals and organisations that develop, implement, and capitalise on these systems must be held accountable.[13]

2. The Fiduciary Duty Crisis: A Brief Overview of a Breached Trust

The most critical aspect of corporate governance is the fiduciary duty that officers and directors have to the corporation and its shareholders. This encompasses the obligations of loyalty and care.[14] The duty of care requires directors to exercise the same degree of caution as a reasonable individual in a comparable position, while the duty of loyalty requires them to act in the corporation's best interests without any conflicts of interest. These obligations are directly contradicted by the delegation of significant decision-making authority to AI systems.

In contrast to a human, an AI is incapable of employing ethical considerations or reasoned judgement; it is limited to adhering to its programming in accordance with the data it was trained on.[15] If the data is biassed or the algorithm is flawed, the AI may make a negligent decision, but it did not violate a duty. A duty of loyalty requires loyalty, which an AI cannot provide. This results in a crisis: Can a board of directors fulfil its fiduciary duties by relying on a flawed system? In automated governance, assigning such responsibility to an inanimate entity requires redefining fiduciary duties. This contradicts the corporate integrity-promoting philosophy of "*encapsulated trust*".[16]

---

[12] Robert Casey, "AI's Leaps Forward Force Talks About Legal Personhood for Tech", Bloomberg Law, May 28, 2025, *available at*: https://news.bloomberglaw.com/artificial-intelligence/ais-leaps-forward-force-talks-about-legal-personhood-for-tech (last visited on: 27.06.2025).

[13] Michael Ryan, "The Future of AI in Corporate Governance: The Role of the Board", 2021 *Journal of Business Law* 1 (2021).

[14] S. M. Siebecker, "Trust & Truth: Corporate Responsibility in the Age of AI", 81 *Fordham Law Review* 2315 (2020).

[15] M. Dastani and A. Yazdanpanah, "AI in Corporate Governance: Legal, Ethical, and Fiduciary Challenges", *International Journal of Law and Social Sciences* (In Press, 2025).

[16] *Supra* note 14 at 2320.

B. The Issue of Negligence: Torts Without Tortfeasors

The primary method of obtaining compensation for harm that is not covered by a contract is through tort law, particularly the doctrine of negligence. But the primary components of it-duty, breach, causation, and damages-do not align well with the structure and operation of AI systems.[17]

1. The Missing Elements in Negligence

In order to establish negligence, a plaintiff must demonstrate that the defendant violated a duty of care owed to them, which resulted in their injury. This chain of responsibility is disrupted in an AI-related case.[18] In the event that an AI-powered medical diagnostic tool makes a poor recommendation that causes harm to a patient, who is responsible for violating the law? The algorithm was created by the developer, implemented by the hospital (integrator), utilised by the doctor (user), or trained on biassed data provided by an individual. It is frequently difficult to identify the individual who is responsible for liabilities that are shared by multiple parties.[19]

The law was established on the premise that humans make mistakes, not that machines are unrestrained in their actions. Consequently, there are "*torts without tortfeasors*," which refers to a situation in which there is evident harm but no single individual can be identified as having committed a clear breach under conventional standards.[20] Due to its capability to learn and function autonomously, AI creates a legal barrier that obscures its human decisions and errors and makes it difficult to identify the perpetrator.

2. The "*Black Box*" and the Difficulty of Establishing Causation

The plaintiff faces significant challenges in establishing causation, even if a duty and breach can be demonstrated. The inner workings of intricate machine learning models are frequently a "*black box,*" even to the individuals who developed them.[21] A plaintiff who wishes to establish that a specific design flaw was the cause of their injury would require access to

[17] *Supra* note 7 at 195.
[18] Ethos Risk Services, "AI Liability and Negligence Cases: Who's Responsible?", *available at*: https://ethosrisk.com/blog/ai-liability-and-negligence-cases-whos-responsible/ (last visited on: 27.06.2025).
[19] *Ibid*.
[20] *Supra* note 5 at 410.
[21] *Supra* note 6 at 8.

proprietary code, training data, and model parameters-assets that companies safeguard as trade secrets.[22]

The plaintiff successfully argued in *Wickersham v. Ford* that a delay in deployment was caused by a poorly designed airbag algorithm.[23] Exceptions like this uphold the rule. This algorithm was simple and deterministic, and the plaintiff's expert had worked with it before. Contemporary, non-deterministic neural networks that transform as they process new data make it difficult to identify a single flaw that caused a specific harmful output from a technical and legal perspective. This effectively transfers the responsibility for justice to the victim, who possesses the least information and resources, necessitating that they deconstruct and demonstrate the flaws in a complex system that is owned by a powerful corporation. This is not merely a procedural issue; it is also a structural issue that complicates the process of obtaining justice.

C. Contract Law in the Era of Artificial Intelligence That Executes Actions

The emergence of "*agentic*" AI-systems that can act autonomously to achieve objectives on behalf of a user-has placed a strain on contract law, which regulates enforceable agreements.[24] In the United States, electronic transaction laws, such as the Uniform Electronic Transactions Act (UETA) and the federal E-SIGN Act, stipulate that contracts executed by "electronic agents" are valid. Nevertheless, these laws were formulated with the intention of governing simpler, automated systems.[25] They were intended for systems that adhere to pre-programmed rules, rather than AI that can "*adjust to new information, find better ways to get things done, or make choices based on probabilities*."[26]

This raises new questions regarding accountability. If an AI assistant is instructed to acquire a specific item but "*hallucinates*" and executes an entirely unintended contract, who is accountable? Conventional contract law presupposes that individuals reach a consensus on a

[22] K. Yeung, "Algorithmic regulation: A critical interrogation", 12 Regulation & Governance 1 (2018).
[23] *Wickersham* v. *Ford Motor Company*, 194 F. Supp. 3d 434 (S.D. Tex. 2016). See also Zachary Muller, "Liability for a defectively designed algorithm: Wickersham v. Ford", 53 *Columbia Journal of Law & Social Problems* 149 (2019).
[24] Proskauer Rose LLP, "Contract Law in the Age of Agentic AI: Who's Really Clicking 'Accept'?", Proskauer on Privacy, *available at*: https://www.proskaueronprivacy.com/2025/05/contract-law-in-the-age-of-agentic-ai/ (last visited on: 27.06.2025).
[25] G. Smith, *et.al.*, Liability for Harms from AI Systems: The Application of U.S. Tort Law and Liability to Harms from Artificial Intelligence Systems (RAND Corporation, Santa Monica, CA, 2024).
[26] *Supra* note 12.

matter based on their intentions and behaviors. However, in the case of agentic AI, there may not be a distinct human "*actor*" to hold accountable in the event of a deal's failure; rather, there may only be a machine making decisions that were not predetermined.[27] Lack of clarity increases risk and makes business transaction prediction difficult. Implementing existing laws as a patchwork solution without significant changes is inadequate and worsens the situation. Small businesses and startups lack the legal resources to navigate a fragmented and unpredictable environment, making it worse for them. It also lacks explicit victim protections.[28]

AN EXAMINATION OF THE RESPONSES OF VARIOUS COUNTRIES TO GLOBAL REGULATIONS

Nations have developed three AI governance approaches to address the above issues. Regulation differs greatly in the EU, US, and India. The EU uses a rights-based, comprehensive model, the US a market-driven patchwork, and India a light-touch, innovative strategy.

A. The European Union's Rights-Based, Risk-Tiered Model

The EU has established itself as a global leader in the establishment of AI regulation standards by adopting a comprehensive, rights-based approach that prioritises safety and fundamental rights through a proactive, ex-ante framework.[29]

1. The AI Act: A Risk-Based Architecture

The AI Act is the most critical component of this approach. It establishes a classification system that is based on risk.[30] AI applications are classified according to their potential for causing harm:

- *Unacceptable Risk:* Systems that are evidently detrimental to safety, employment, and rights are prohibited. Biometric identification in public places in real time (with a few

[27] *Ibid*.
[28] *See*, M. C. Elish, "The limits of liability in the age of AI", The New York Times, Nov. 1, 2023; J. Cobbe, "Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making", 37 *Legal Studies* 445 (2017).
[29] C. Cath, "Governing artificial intelligence: ethical, legal and technical challenges and opportunities", 376 *Philosophical Transactions of the Royal Society* A 20180080 (2018).
[30] European Commission, "Proposal for a Regulation on a framework for Artificial Intelligence (Artificial Intelligence Act)", COM (2021) 206 final.

exceptions), governments scoring people's social lives, and AI that alters how people act to circumvent free will (such as voice-activated toys that encourage dangerous behavior).[31]

- *High-Risk:* Safety or basic rights-compromising systems are high-risk. Before being sold, these systems must undergo conformity assessments, have high-quality data governance to reduce bias, have detailed technical documentation, and be designed for effective human oversight. They are used in hiring and managing workers, running critical infrastructure, education, law enforcement, and accessing vital services.[32]
- *Low Risk:* Chatbots and similar systems are required to adhere to basic transparency standards, which ensures that users are aware they are conversing with a machine.[33]
- *Minimal Risk:* The Act does not impose any additional legal obligations on the majority of AI systems, which fall under this category.[34]

2. Modernizing Liability: The PLD and the Deferred AILD

The EU can directly address liability through the Revised Product Liability Directive (PLD). This directive is a significant modification in that it clarifies the definition of "*product*" by incorporating software and AI systems.[35] It also updates the concept of a "*defect*" to encompass harms caused by an AI's ability to learn on its own or by security holes, and it holds manufacturers and suppliers accountable for data loss-related damages. This implies that liability may continue to be applicable even if a product causes harm after it has been used, as it undergoes changes over time.[36]

However, the EU's objectives have been compromised by a clear conflict between innovation and regulation. The most effective illustration of this is the AI Liability Directive (AILD) that has been proposed. The AILD was intended to collaborate with the AI Act and PLD to

[31] The European Union AI Act, 2024, art. 5.
[32] *Ibid.*, art. 6. See also European Parliament, "Report on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts" (A9-0188/2023).
[33] The European Union AI Act, 2024, art. 52.
[34] *Ibid.*, art. 4.
[35] European Commission, "Proposal for a Directive on liability for defective products", COM(2022) 495 final.
[36] Clifford Chance, "The EU introduces new rules on AI liability", *available at*: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/01/the-eu-introduces-new-rules-on-ai-liability.pdf (last visited on: 27.06.2025).

facilitate the process of establishing a case for victims of AI-related harm.[37] The burden of proof in fault-based claims would have been shifted, requiring AI providers to demonstrate that they were adhering to their duty of care, as a result of its primary features, a "*disclosure obligation*" and a "*rebuttable presumption of causality*."[38] In late 2024, the AILD was suspended in a significant policy change, which was perceived by many as a concession to industry pressure and a desire to remain competitive with the United States and China.[39] The EU's system for redress is significantly weakened by the death of the AILD, demonstrating the difficulty of maintaining a balance between robust citizen protection and economic requirements.

B. The Market-Driven Patchwork of the United States

The EU's regulatory system is more centralised, while the US has a more fragmented, market-driven approach that mostly uses existing laws and gives more power to sectoral regulators.[40] As a result, there is now a "*patchwork*" of laws and court decisions that don't give businesses legal certainty or consistent protection for consumers.[41] Most of the time, people who are hurt by AI sue under traditional tort and contract law, but this isn't always the best way to do it, and the results vary a lot from place to place.[42] Section 230 of the Communications Decency Act is a big legal problem because courts have said that it protects online platforms from being held responsible for harm caused by algorithmically recommended third-party content. This makes it hard to hold people accountable in the digital world.[43]

---

[37] European Parliament, "Briefing EU Legislation in Progress: Artificial intelligence liability directive", *available at*: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf (last visited on: 14.07.2025).

[38] McCann FitzGerald, "The Artificial Intelligence Liability Directive – Time to catch up", *available at*: https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/the-artificial-intelligence-liability-directive-time-to-catch-up (last visited on: 27.06.2025).

[39] T. Evas, "The EU's AI Power Play: Between Deregulation and Innovation", Carnegie Endowment for International Peace, May 20, 2025.

[40] *Supra* note 29.

[41] *Supra* note 7 at 200.

[42] *Supra* note 25.

[43] J. M. Balkin, "The Three Laws of Robotics in the Age of Big Data", 78 *Ohio State Law Journal* 1217 (2017). *See also*, Congressional Research Service, "Legal Liability for Content Recommended by Algorithms", R47753 (2023).

The primary federal legislative proposal is the Algorithmic Accountability Act (AAA), which was reintroduced in 2023.[44] The AAA is a prime example of the United States' more cautious, ex-post approach. The AAA lacks the extensive pre-market requirements of the EU AI Act. Rather, it emphasises evaluation and transparency. Companies that implement "automated critical decision processes" to determine housing, employment, credit, and other matters would be required to conduct impact assessments and submit them to the Federal Trade Commission (FTC).[45] The bill is a "*targeted response*" that is intended to collect information and grant the FTC additional authority. However, it does not establish new liability regimes or significantly alter substantive law.[46] It demonstrates a preference for addressing established harms rather than regulating potential risks prior to their occurrence.

C. India's "*Pro-Innovation*" Position

India is adopting a third approach, which is predicated on a "*light-touch*" regulatory philosophy and a "*pro-innovation*" approach.[47] The primary objective is to establish a domestic AI ecosystem and achieve "Sovereign AI"-self-sufficiency in a critical technology-in order to stimulate economic growth.[48] To achieve this, India has opted not to implement binding, prescriptive laws, as is the case in the EU, but rather to rely on a "*patchwork*" of existing laws and non-binding ethical guidelines.[49]

The current landscape is governed by the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023, which was recently enacted.[50] AI systems that manage personal data are indirectly impacted by these laws. Governance is primarily founded on policy documents such as the "*Principles for Responsible AI*" of NITI Aayog, which establish ethical standards for transparency, accountability, and fairness. However, these

[44] The Algorithmic Accountability Act of 2023, H.R. 5628, 118th Cong. (2023).
[45] Ron Wyden, "Algorithmic Accountability Act of 2023 Summary", *available at*: https://www.wyden.senate.gov/imo/media/doc/algorithmic_accountability_act_of_2023_summary.pdf (last visited on: 27.06.2025).
[46] *Ibid*.
[47] AZoRobotics, "AI Regulation in India: A Pro-Innovation Approach", *available at*: https://www.azorobotics.com/Article.aspx?ArticleID=742 (last visited on: 27.06.2025).
[48] ECIPE, "AI and India's National Interest", *available at*: https://ecipe.org/publications/ai-and-indias-national-interest/ (last visited on June 27, 2025).
[49] Law.Asia, "India's AI regulation in focus as government seeks unified approach", *available at*: https://law.asia/india-ai-regulation-focus-unified-approach/ (last visited on: 27.06.2025).
[50] See The Information Technology Act, 2000 (Act 21 of 2000); The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

documents lack the authority to enforce them.[51] Instead of prioritising regulatory constraints, this methodology prioritises flexibility and development.

However, the framework of India is undergoing structural changes. The Digital India Act (DIA) is anticipated to be a groundbreaking piece of legislation, as it will introduce the country's first AI-specific provisions.[52] The DIA is expected to address algorithmic accountability, consumer rights, and liability, signalling a potential transition from a purely policy-led approach to a more formalised regulatory regime.[53] This transition will be critical in determining how India balances its ambition for technological leadership with the necessity to safeguard its citizens from algorithmic harm.

Table 1: *A Comparison of AI Liability Frameworks in the EU, US, and India*

Characteristic	India	United States	European Union
Core Philosophy	Pro-Innovation, Developmental, "*Light-Touch*"	Market-Driven, Reactive, Sectoral	Rights-Based, Precautionary, Comprehensive
Primary Legal Instruments	IT Act of 2000, Digital Personal Data Protection Act of 2023, and the Proposed Digital India Act (DIA)	Common Law (tort, contract), Proposed Algorithmic Accountability Act (AAA)	The AI Act, Revised Product Liability Directive (PLD)
Liability Approach	Emerging/Undefined; Expected in DIA	Primarily Negligence/Product Liability; Varies by State	Tiered (Strict/Fault-Based); Product Liability for Software
Key Procedural Mechanisms	non-binding ethical guidelines, and advisories	post-deployment impact assessments (as proposed in AAA)	Pre-market conformity assessments,

[51] Lawful Legal, "India's Approach to AI Regulation: Navigating Innovation and Ethics", *available at*: https://lawfullegal.in/indias-approach-to-ai-regulation-navigating-innovation-and-ethics/ (last visited on: 27.06.2025).
[52] NM Law, "AI Regulation in India: A Dawn of Digital Governance", *available at*: https://nmlaw.co.in/ai-regulation-in-india-a-dawn-of-digital-governance/ (last visited on: 27.06.2025).
[53] *Ibid*.

			transparency obligations
Primary Enforcement Body	Ministry of Electronics and Information Technology (MeitY) and the Sectoral Regulators	State Attorneys General and the Federal Trade Commission (FTC)	The European AI Office and the National Authorities
Overall Status	Policy-Led; Key Legislation Developing	Fragmented; Key Legislation Proposed	Enacted and in force (phased implementation)

PUTTING THE "*DOWNTRODDEN*" AT THE CENTRE: SYSTEMIC HARM AND ALGORITHMIC BIAS

A liability risk analysis that is solely legal obscures the substantial human cost of algorithmic failure. In order to fulfil the imperative of addressing "*downtrodden concerns*," it is imperative to transition from abstract legal principles to the concrete, lived experiences of those harmed by biased AI systems.[54] These systems, which are frequently deployed in critical areas of life, do not merely replicate existing societal inequities; they amplify and entrench them on an unprecedented scale, concealed behind a façade of technological objectivity.

A. The Mechanism of Algorithmic Bias

The system's flaw, algorithmic bias, is not a negative thing; it is a result of the data society collects, and the decisions individuals make. It typically infiltrates systems through three primary methods:

- *Biased Training Data:* This is a major issue because an AI trained on decades of biased hiring or lending practices will replicate those patterns. This creates a feedback loop in which biased decisions generate new data that supports the bias, making results increasingly unjust.
- *Poor Algorithmic Design:* When developers unfairly evaluate factors or build models based on unconscious assumptions, bias can be introduced. Lack of diversity in

[54] *Supra* note 14 at 2316.

development teams can make people with similar backgrounds overlook discriminatory effects.

- *Proxies for Protected Attributes:* This is a highly problematic source of bias. Race may not be a factor that an algorithm can utilise; however, it can utilise related data, such as postal codes or credit history, which serve as effective substitutes for economic status and race. This may result in unjust outcomes.[55]

This feedback loop is detrimental due to the combination of inadequate data and inadequate design. An algorithm that is biassed makes a decision (such as declining a loan), which generates additional data that reinforces the original bias, resulting in increasingly unfair outcomes over time.[56]

B. Case Studies of Algorithmic Harm

This bias has tangible consequences. Creating new, concealed barriers to opportunity, they manifest as genuine harms that disproportionately affect marginalised and vulnerable communities.

- *Discrimination in Employment:* Automated hiring tools, which are currently employed by 99% of Fortune 500 companies, systematically eliminate qualified candidates.[57] Algorithms that are trained on data from a company's existing, non-diverse workforce may penalise applicants from different backgrounds. For instance, a system may learn to favour candidates who played certain sports or attended certain universities, effectively discriminating based on class and gender.[58] Additionally, these tools can penalise individuals with disabilities whose speech patterns or behaviours deviate from the algorithm's "*norm*."[59]

---

[55] IBM, "Algorithmic bias", *available at*: https://www.ibm.com/think/topics/algorithmic-bias (last visited on: 27.06.2025).

[56] Law vs., "Legal Implications of Algorithmic Bias in Decision-Making", *available at*: https://lawvs.com/articles/legal-implications-of-algorithmic-bias-in-decision-making (last visited on June 27, 2025).

[57] ACLU, "How Artificial Intelligence Might Prevent You from Getting Hired", *available at*: https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired (last visited on: 27.06.2025).

[58] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown, New York, 2016).

[59] E. P. Goodman and K. E. P. Levy, "New-School Discrimination by Data", 64 *Communications of the ACM* 40 (2021).

- *Bias in Finance and Lending:* In the financial sector, AI-driven systems are establishing a new form of "*digital redlining*."[60] Algorithms used for credit scoring and loan approvals can perpetuate historical discrimination by penalising applicants from minority neighbourhoods or those with non-traditional income patterns. A recent lawsuit alleged that a tenant screening system by SafeRent consistently gave lower scores to Black and Hispanic renters, in part because it failed to properly account for housing vouchers as a legal form of income.[61] This results in entire communities being excluded from housing and financial opportunities.

- *Healthcare and Insurance Inequities:* Healthcare has deadly consequences. A widely used commercial algorithm was found to reduce Black patient healthcare resources. This was because the algorithm used past healthcare spending as a proxy for need, which ignored the fact that Black patients spend less due to systemic barriers to access.[62] Pulse oximeters are less accurate on darker skin, and AI-powered diagnostic tools trained on white patients may misdiagnose and delay treatment for people of colour.[63]

- *Erosion of Consumer and Labour Rights:* In addition to discrete decisions, AI is employed to deploy manipulative "*dark patterns*" that deceive consumers, to implement discriminatory pricing, and to intensify worker surveillance, thereby eroding fundamental rights. The FTC's enforcement action against Rite Aid, which used a flawed and biased facial recognition system to falsely accuse customers, particularly women and people of colour, of shoplifting, highlights the real-world harm these systems can cause.[64]

The common thread in these cases is that algorithmic systems do not merely reflect societal bias; they magnify it at scale and obscure it from view. A single biased loan officer can cause

[60] UNT Dallas College of Law, "When Algorithms Judge Your Credit: Understanding AI Bias in Lending Decisions", *available at*: https://www.accessiblelaw.untdallas.edu/post/when-algorithms-judge-your-credit-understanding-ai-bias-in-lending-decisions (last visited on: 27.06.2025).

[61] AlgorithmWatch, "Racist Technology in Action: AI tenant screening fails the 'fairness' test", Bluesky, June 5, 2025.

[62] ACLU, "Algorithmic Bias in Health Care", (2022), *available at*: https://www.aclu.org/sites/default/files/field_document/algo_health_white_paper_draft_final_v4.pdf (last visited on: 27.06.2025).

[63] *Ibid*.

[64] FTC, "AI Risk and Consumer Harm", (January 2025), *available at*: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2025/01/ai-risk-consumer-harm (last visited on: 27.06.2025).

harm to dozens, while a single biased algorithm can cause harm to millions. This is all done while presenting an illusion of objective, data-driven neutrality. The combination of scale and obscurity renders algorithmic discrimination a uniquely potent and perilous force for the entrenchment of inequality.

THEORETICAL STANDARDS FOR RECONSTRUCTING LIABILITY FRAMEWORKS: INNOVATIVE APPROACHES

The reality of systemic harm and the doctrinal impasse necessitate more than incremental change. A deliberate effort must be made to establish a liability framework that is both fair and robust for AI-driven corporate governance. This necessitates a novel, two-pronged strategy that combines reformed substantive liability rules with mandatory procedural obligations. These two prongs are not independent solutions; they are symbiotic; procedural diligence is incentivised by the threat of substantive liability, and substantive claims are made possible by the evidence generated through procedural compliance.

A. Mandating a Corporate Accountability Toolkit: A Triad of Procedural Duties

In order to incorporate a new standard of technological diligence, the conventional corporate duty of care must be modernised. This entails the integration of a mandatory "*accountability toolkit*" into corporate governance for any high-risk AI system.

1. Algorithmic Impact Assessments (AIAs)

Before deploying any high-risk AI system that makes critical decisions about individuals, corporations must be legally obligated to conduct and publish an AIA.[65] This proactive process, which is based on established frameworks from the AI Now Institute and the Canadian government, compels a company to evaluate and disclose a system's purpose, functionality, and potential impacts on fairness, bias, and fundamental rights. This process must include:

- *Pre-acquisition Review:* An assessment of the system prior to the agency's adoption.
- *Public Disclosure:* Agencies are required to publicly disclose information regarding the system's purpose, reach, and internal use policies.

[65] F. Doshi-Velez and M. Kortz, "Accountability of AI under the Law: The Role of Explanation", arXiv preprint arXiv:1711.01134 (2017).

- *Self-Assessment:* A self-assessment of potential issues, such as bias and inaccuracy, and a plan for mitigation.
- *Public Comment and Challenge:* A significant opportunity for the public and external researchers to interact with, provide feedback on, and, if necessary, contest the agency's assessment.[66]

Companies such as Spotify, which have implemented internal AIAs for over a hundred of their systems, have demonstrated the feasibility and value of such assessments in identifying hotspots for harm and prioritising mitigation efforts.[67]

2. Independent "*Criterion*" Audits

Self-assessment is indispensable; however, it is inadequate. In order to guarantee objective verification and prevent "*ethics-washing*," the legal framework must require consistent audits conducted by independent, accredited third parties.[68] This proposal promotes the implementation of a "*criterion audit*" framework, which is based on the rigour and public trust that are associated with financial auditing.[69] A criterion audit consists of four primary characteristics:

- It is conducted in accordance with standardised, publicly accessible criteria that are derived from regulation.
- Its primary focus is on evaluating adherence to that regulation.
- Auditors are held to high ethical standards, accredited, and professionally trained.
- In order to guarantee transparency, the findings are published in a standardised report.

[66] D. Reisman, *et.al.,* "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability" (AI Now Institute, New York, April 2018). See also Treasury Board of Canada Secretariat, "Algorithmic Impact Assessment", OECD STIP Compass (2019).

[67] *See*, Spotify Engineering, "Lessons Learned from Algorithmic Impact Assessments in Practice", *available at*: https://engineering.atspotify.com/2022/09/lessons-learned-from-algorithmic-impact-assessments-in-practice (last visited on: 27.06.2025); J. Mökander, *et.al*., "Auditing and Assessing Algorithmic Systems: A Case Study at Spotify", 1 *Journal of Online Trust and Safety* 1 (2024).

[68] *Supra* note 66.

[69] M. C. Elish, *et.al*., "The Criterion Audit: A Novel Framework for AI Auditing", in Proceedings of the 2024 AAAI/ACM Conference on AI, Ethics, and Society 250 (AAAI Press, 2024).

- This establishes a system of external accountability that transitions from voluntary principles to enforceable standards, granting regulators the authority to inspect companies for noncompliance.[70]

3. Legal Requirement for Explainable AI (XAI)

Transparency is not an afterthought; it is a fundamental design principle. XAI techniques, which render the decision-making process of an AI model transparent and auditable, are indispensable for numerous legal purposes.[71] The legal requirement for high-risk systems should be to elevate explainable AI (XAI) from a desirable technical feature to a legal requirement.

- *Fulfilling the Right to Explanation:* They are essential for the "*right to explanation*" of affected individuals, as acknowledged in regulations such as the GDPR.
- *Facilitating Audits and Assessments:* They are essential for the meaningful audits and impact assessments detailed above.
- *Evidence for Redress:* They furnish the essential evidence required for individuals to pursue redress when they are injured.[72]

The practical application of XAI in high-stakes industries such as finance (explaining loan denials), healthcare (justifying diagnoses), and manufacturing (ensuring quality control) demonstrates its necessity and viability.[73]

B. Reforming Substantive Liability: From Legal Fictions to Tangible Responsibility

A clear and effective path to liability must exist when procedural duties fail, despite their potential to prevent harm. In order to address the accountability gaps that were identified in Part II, it is necessary to reform substantive law.

---

[70] Ada Lovelace Institute, "A code of conduct for AI? Algorithm audits and the law" (2023), *available at*: https://www.adalovelaceinstitute.org/report/code-conduct-ai/ (last visited on: 27.06.2025).

[71] Milvus, "How does Explainable AI impact regulatory and compliance processes?", *available at*: https://milvus.io/ai-quick-reference/how-does-explainable-ai-impact-regulatory-and-compliance-processes (last visited on: 27.06.2025).

[72] S. Wachter, B. Mittelstadt, and C. Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", 31 *Harvard Journal of Law & Technology* 841 (2018).

[73] *See*, Viso.ai, "Explainable AI (XAI) – The Complete Guide"; Meegle, "Explainable AI in Manufacturing"; Smythos, "Explainable AI Examples: Real-World Applications & Use Cases", available at the respective company websites (last visited on: 27.06.2025).

1. A Tiered Liability Regime

A traditional fault-based negligence standard can be maintained for standard, low-risk AI. The law should adopt a tiered approach to liability that aligns with the risk-based framework of the AI. Nevertheless, the liability standard must be adjusted for AI systems that are specifically designated as "*high-risk*" (e.g., in the areas of credit, hiring, and justice). The corporate deployer would be required to demonstrate that they exercised all due care or that the harm was not caused by their system in the event that a high-risk system causes harm. Alternatively, the framework could impose strict liability or, at the very least, a rebuttable presumption of fault or causality. This directly addresses the evidentiary imbalance that currently renders victims powerless, thereby transferring the responsibility to the party with the most information and control.

2. Extending Product Liability to Software

In order to establish a clear path for redress, legislatures and courts must definitively determine that AI systems and software are "*products*" under product liability law.[74] This reform would permit claims based on design defects and failure to warn. An algorithm that is trained on biassed data or designed with discriminatory proxies could be considered to have a design defect. A corporation that deploys a powerful AI tool without adequately disclosing its limitations, potential for error, or biased outputs could be liable for failure to warn. Emerging case law, such as *Garcia v. Character Technologies, Inc.*, in which a court allowed a product liability suit to proceed treating an AI chatbot as a "*product*," signals a judicial willingness to adapt doctrine to technological reality, a trend that should be codified into law.[75]

3. Redefining Fiduciary Duties for the Algorithmic Age

Competent algorithmic oversight must be added to the duty of care. This doctrinal evolution should be accompanied by corporate governance reforms that establish human responsibility. This includes creating roles like an AI Oversight Officer or board committee to understand, monitor, and account for the corporation's AI systems.[76] This measure eliminates the

[74] *Supra* note 25.

[75] Garcia v. Character Technologies, Inc., Case No. 24-cv-01586-PCP (N.D. Cal. May 20, 2025). See also Verisk, "GenAI Product Liability Cases to Watch", *available at*: https://core.verisk.com/Insights/Emerging-Issues/Articles/2025/May/Week-4/GenAI-Product-Liability-Cases (last visited on: 27.06.2025).

[76] *Supra* note 14 at 2330.

accountability gap by holding a specific, identifiable human actor in the corporate hierarchy accountable for the deployment and consequences of automated systems.

Reconstructed framework creates virtuous cycle. The threat of substantive liability motivates corporations to invest in and follow AIAs, audits, and XAI procedures. These procedures provide evidence that helps victims and regulators enforce substantive law. We reject the false dichotomy between innovation and regulation. A clear, predictable, and robust liability regime steers innovation towards trustworthy and responsible ends, building public confidence for AI's widespread and equitable adoption.

SUGGESTIONS AND RECOMMENDATIONS

In order to implement the reconstructed liability framework, it is imperative that key stakeholders collaborate and implement practical measures. The subsequent recommendations demonstrate how to enhance the fairness, utility, and accountability of AI governance.

1. **For Policymakers and Lawmakers:**

- *Adopt Phased and Interoperable Laws:* Rather than attempting to enact a single, comprehensive law, divide it into smaller components. Begin by establishing a body of evidence by enacting laws that mandate AIAs and public registries for high-risk systems, as outlined in the US Algorithmic Accountability Act.[77] Subsequently, modify liability laws to align with significant international frameworks, such as the EU AI Act. For instance, adhering to the EU's high-risk regulations could establish a "*rebuttable presumption of compliance*" with local law, which would facilitate the compliance with both sets of regulations.

- *Establishing Clear Regulatory Jurisdiction & Funding:* Increase the authority of a nodal agency, such as the proposed Digital India Authority, while ensuring that sectoral regulators (such as SEBI for financial AI and IRDAI for insurance) are aware of their specific responsibilities. This will prevent any potential overlap and ensure that all parties are aware of what to anticipate.[78] Ensure that regulators have sufficient

[77] *See*, The Algorithmic Accountability Act of 2023, supra note 44. See also Danielle Keats Citron, "Technological Due Process", 85 *Washington University Law Review* 1249 (2008).
[78] NITI Aayog, "Responsible AI for All: Adopting the Framework" (NITI Aayog, Government of India, New Delhi, 2021).

funding to perform their duties by levying a nominal fee on the revenue of organisations that implement high-risk AI. This will provide them with the necessary funds to employ technical experts and enforce the regulations.

- *"Safe Harbour" Provisions:* In order to motivate individuals to implement optimal practices in good faith, laws should include safe harbour provisions. In the event that companies can demonstrate that they are adhering to mandatory procedures such as AIAs and independent audits in good faith and with strong evidence, they will be shielded from certain punitive damages, even if harm still occurs. This renders it more appealing to adhere to the regulations than to circumvent them.[79]

2. For Industry Leaders and Business Owners:

- *Operationalize AI Ethics through Internal Governance:* Establish internal AI review boards or ethics committees that include representatives from various departments, including legal, technical, business, and ethics. These organisations should be granted the authority to supervise and authorise AIAs, evaluate audit findings, and discontinue the implementation of systems that present unacceptable risks.[80]

- *Establish a Mandate and maintain a record of Responsible AI Training:* Stop providing individuals with general ethics training. Establish mandatory training and certification programs for each position that pertains to the management of data, the mitigation of bias, and the development of responsible AI. Ensure that the completion of these programs and the attainment of DEI objectives in technical teams are associated with the compensation and performance evaluations of executives.

- *Creating Sector-Specific Codes of Conduct:* Collaborating with industry associations to establish comprehensive, legally binding regulations for particular sectors, such as AI in healthcare or AI in hiring. These codes, which were developed with the assistance of civil society and regulators, have the capacity to provide more detailed

[79] Daniel B. Schwarcz, "Regulating AI in Insurance", 2023 *University of Illinois Law Review* 1335 (2023) (discussing the role of safe harbors in promoting responsible innovation).

[80] *See*, Timnit Gebru, *et.al*., "Roles for Computing in Social Change", in Proceedings of the 2016 ACM Conference on Computers and Society 251 (ACM, 2016); World Economic Forum, "AI Governance: A Holistic Approach to Implement Responsible AI" (WEF, Geneva, 2021).

and practical guidance than a general law, thereby establishing a benchmark for the "*state of the art*."[81]

3. **For the Courts:**

- *Develop specialised curricula and bench books:* Collaborate with the National Judicial Academies and the most prestigious law and technology schools to develop a standardised curriculum and bench book on AI. This resource should address the fundamentals of machine learning, the origins of bias, and emerging issues in evidence law that are related to algorithmic systems.[82]

- *Apply Known Rules to New Facts:* Rather than referring to it as "*dynamic interpretation*," consider judicial reasoning as the application of enduring legal principles (such as procedural fairness or foreseeability in tort) to novel technological facts. One method of accomplishing this is to substantiate decisions with established case law by utilising examples from existing complex liability systems, such as those for drugs or aeroplanes.

- *Establish a neutral panel of technical experts:* In order to halt the "*battle of the experts,*" courts could be permitted to utilise a pre-vetted, neutral panel of technical experts that is maintained by a national organisation, such as the Ministry of Electronics and Information Technology. These experts could serve as special masters or provide the court with independent reports, thereby enhancing the credibility of the evidentiary process.[83]

4. **For Academia and Civil Society:**

[81] OECD, "Artificial Intelligence in Society" 145 (OECD Publishing, Paris, 2019) (discussing sector-specific guidance).

[82] *See*, David Freeman Engstrom, "The New Civil Procedure: From Class Actions to Private Regulatory Process", 96 *New York University Law Review* 1645 (2021) (discussing the need for judicial education in complex litigation).

[83] Federal Judicial Center, Reference Manual on Scientific Evidence (The National Academies Press, Washington, D.C., 3rd edn., 2011).

- *Establish secure whistleblower platforms:* Establish secure, legally protected locations where technologists and other corporate employees can report concerns regarding AI systems that are unethical or harmful without fear of losing their jobs.[84]

- *Enhance "Bias Bounty" Programs:* Advocate for and assist in the establishment of standardised "bias bounty" programs, which are analogous to cybersecurity bug bounties. These programs would provide independent researchers with financial compensation and public recognition for identifying and responsibly disclosing discriminatory vulnerabilities in artificial intelligence systems that are employed in the business sector.[85]

- *Establish Interdisciplinary Legal-Technical Clinics:* Colleges and universities should establish clinical programs that allow law and computer science students to collaborate to evaluate the compliance, bias, and fairness of real-world algorithms utilised in the public and private sectors. This would simultaneously provide them with practical training and benefit the public.[86]

CONCLUSION

AI and corporate governance are currently at a critical juncture in their integration. In the past, doctrinal frameworks that were intended for human actors have failed to consider automated decisions. The most vulnerable members of society are disproportionately affected by this failure, which results in tangible harm, systemic discrimination, and the erosion of fundamental rights. Unsustainable and unjust are the legal uncertainty and patchwork of inadequate responses.

Deliberate liability reconstruction is required, as per this article. This proposal suggests a novel framework that combines robust substantive legal reforms with proactive procedural obligations. Corporate duty of care would shift from reactive to proactive through the implementation of legally mandated Explainable AI, independent "*criterion*" audits, and

[84] *See*, The Signals Network, "Our Mission", *available at*: https://thesignals.org/ (last visited on: 27.06.2025); *See also*, Frances Haugen, *The Power of One* (Little, Brown and Company, New York, 2023).
[85] Rumman Chowdhury, "Get Loud: A Call to Action for Responsible Tech", Harvard Business Review, Nov. 15, 2022, *available at*: https://hbr.org/2022/11/get-loud-a-call-to-action-for-responsible-tech (last visited on: 27.06.2025).
[86] *See*, e.g., Stanford Law School, "RegLab: Law, Technology, and Policy Clinic", *available at*: https://law.stanford.edu/reglab/ (last visited on: 27.06.2025).

mandatory Algorithmic Impact Assessments. A procedural backbone that is supported by reformed substantive law-a tiered liability regime that shifts the burden of proof for high-risk systems, an expanded product liability doctrine that treats AI as a product, and redefined fiduciary duties that ensure clear human oversight-must be implemented.

This decision is of a normative nature. The cost of progress is inequality, which we can accept by allowing technology to evolve without accountability. Our legal and corporate governance structures can be modified to enable us to master our tools, rather than being mastered by them. We can guarantee responsible corporate innovation by ensuring that liability is in alignment with control and profit. This will guarantee that the many advantages of AI are distributed, and its negative effects are rectified in a fair and effective manner, thereby maintaining corporate accountability and algorithmic age fairness.