DOI: *https://doij.org/10.10000/IJLSI.112726*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 2

2025

AI and Legal Liability: Who is Responsible for Decisions Made by Algorithms?

LAXMI[1] AND DR. SUNIL KUMAR[2]

ABSTRACT

The proliferation of Artificial Intelligence (AI) in decision-making across critical sectors such as healthcare, criminal justice, finance, and employment has raised pressing questions regarding legal liability and accountability. This article explores the multifaceted challenge of determining who is responsible when algorithmic decisions lead to harm or injustice. It begins by examining the structure and functioning of AI systems, particularly machine learning models, and identifies how the "black box" nature of these systems complicates legal scrutiny. Through real-world case studies, including Amazon's biased hiring algorithm and the use of COMPAS in criminal sentencing, the article illustrates the tangible consequences of unregulated AI. It critically evaluates emerging legal responses, such as the EU's proposed AI Act and suggestions for AI personhood, and considers alternative models like assigned liability, mandatory insurance, and human-in-the-loop oversight. The article argues that a coherent and proactive legal framework tailored to AI's unique characteristics is necessary to ensure accountability, fairness, and redress. Furthermore, it advocates for embedding normative legal principles into AI governance and stresses the importance of international harmonization to prevent regulatory arbitrage. The overarching conclusion is that legal systems must evolve in tandem with technological innovation to safeguard human rights and societal trust. The liability question is not merely a legal dilemma but a fundamental test of democratic institutions in the digital age.

Keywords: *Artificial Intelligence Liability, Algorithmic Harm, Legal Accountability, AI Personhood, Regulatory Reform*

I. INTRODUCTION

From futuristic conjecture, artificial intelligence (AI) has evolved into a pervasive force influencing decision-making in a wide range of industries, including healthcare, finance, transportation, criminal justice, education and employment. These days, algorithms decide who gets hired, what medical care they receive, how long they stay in jail and even whether they are eligible for loans. These tools promise efficiency, consistency and data-driven insight, but

[1] Author is an Advocate at Bahadurgarh Bar Association, Bahadurgarh, India.
[2] Advocate at Assistant Professor at Jagannath University, Bahadurgarh, India

they also create a new kind of legal complexity: who is responsible for decisions made by AI systems that result in injustice or harm?

The emergence of algorithmic decision-making calls into question fundamental legal concepts of liability. Traditionally, human behaviour, intent and predictability are used to determine who is responsible. Algorithms, particularly those driven by machine learning, can function in ways that are autonomous, opaque and challenging for even their designers to completely comprehend[3]. This phenomenon, which is sometimes called the "black box" problem, poses important queries: Can lines of code be used to track down accountability? Is it the fault of the machine, the data, the developers, or the deployers if an AI system behaves erratically or discriminates against groups?

High-profile disputes have made the legal void surrounding AI-generated results more noticeable. Autonomous vehicles have been implicated in fatal accidents, facial recognition software has misidentified people in criminal investigations and predictive policing tools have been found to disproportionately target minority communities. Legal systems around the world are still mainly ill-prepared to place blame or apply penalties to non-human agents in spite of these harms. AI cannot be sued or punished in many jurisdictions because it is not regarded as a legal person[4].

The complexity is increased by the allocation of liability among various participants in the AI lifecycle, including end users, data scientists, software engineers and corporate entities. This division of responsibilities frequently leads to a regulatory gray area where companies evade serious repercussions and victims of algorithmic harm find it difficult to access remedies.

This article examines the developing controversy surrounding algorithmic decision-making liability. It looks at how current legal frameworks try and frequently fail to address this issue, examines actual case studies where AI has harmed people and assesses possible reform models. The main question still stands: how can the law guarantee justice, accountability and transparency in a time when machines are increasingly making decisions that impact people's lives? Answering this question is a societal necessity as the use of AI grows, not just a legal theory issue.

[3] Mikhail Mikhailovich Turkin, Evgeny Sergeevich Kuchenin, Renata Romanovna Lenkovskaya, and Georgyi Nickolaevich Kuleshov, “Liability of artificial intelligence as a subject of legal relations” 14(2) EurAsian Journal of BioSciences (2020).

[4] Georg Borges, “Liability for AI systems under current and future law: An overview of the key changes envisioned by the proposal of an EU-directive on liability for AI” 24(1) Computer Law Review International 1–8 (2023).

II. Understanding algorithmic decision-making

The question of how algorithms make decisions lies at the core of the discussion surrounding AI liability. Modern artificial intelligence (AI), particularly machine learning (ML), depends on data-driven training to "learn" patterns, make predictions and even adapt over time, in contrast to traditional software systems that adhere to set rules that are preset by humans. Legal responsibility is made more difficult by this evolutionary design, especially when the decisions that are made are discriminatory, ambiguous or unpredictable[5].

AI systems work using a variety of learning models[6]:

Supervised learning: A labelled dataset is used to train the algorithm. A loan approval system might, for instance, learn from thousands of previously submitted applications that have been marked as "approved" or "rejected." It forecasts results for new applicants using this data.

Unsupervised Learning: Without human-labelled outputs, these systems find hidden patterns or groupings in data. They are frequently employed in fraud detection and market segmentation.

Reinforcement Learning: Algorithms optimize their actions based on reward systems by learning by trial and error from feedback from the environment. Autonomous vehicles and robotics frequently use this.

The Black Box Problem

The so-called "black box" problem, the inability to completely comprehend or track how an algorithm comes to a specific conclusion is one of the most concerning features of contemporary AI. Decisions are made using thousands or even millions of internal parameters, which are difficult for developers to understand, particularly in deep learning systems. This lack of transparency significantly reduces oversight and makes it more difficult to prove intent, fault, or causation are three essential components of legal accountability[7].

Was it based on income, credit history or an ingrained prejudice against a particular zip code associated with race, for instance, if an AI system rejected a loan application? Without explainability, the decision's legality and ethics cannot be ascertained by the impacted party or a regulator.

[5] DG, EPRS, “Understanding algorithmic decision-making: Opportunities and challenges” (2019).

[6] Christoph F. Breidbach, “Responsible algorithmic decision-making” 53(2) Organizational Dynamics 101031 (2024).

[7] David Goad and Uri Gal, “Understanding the impact of transparency on algorithmic decision-making legitimacy”, in Matthew Sharp, Lukasz Wojdanowski, et.al. (eds.), Working Conference on Information Systems and Organizations 64–79 (Springer International Publishing, 2018).

III. Current legal frameworks and their gaps

The swift implementation of artificial intelligence has revealed significant shortcomings in current legal frameworks, which were never intended to handle the intricacies of algorithmic decision-making. Human agency, foreseeability and the idea of deliberate or careless behaviour are all fundamental components of legal systems, whether they are founded on civil codes or common law[8]. However, artificial intelligence (AI) challenges these presumptions by introducing agents that have the potential to act independently, change over time and produce results that are difficult to attribute to a single actor.

Tort and Product Liability

Using tort law, especially the doctrines of negligence and product liability, is one way to address harm brought on by AI. Usually, courts look at whether a party's failure to use reasonable care resulted in predictable harm to other people. Manufacturers may face strict liability in product liability cases if a defective product results in harm. Nevertheless, there are several difficulties when implementing these doctrines in AI systems.

First, it can be challenging to identify whether an AI-based choice is a "defect." Can developers be held accountable if an algorithm works as intended but still yields a biased or harmful result? Conventional product liability presupposes a distinct division between usage, manufacturing, and design. When it comes to AI, the final product may be influenced by developers, data trainers, system integrators, and users. Assigning responsibility is challenging because of this fragmentation[9].

Because AI is adaptive, the strict liability doctrine, which holds manufacturers accountable regardless of fault might not apply to it. In contrast to a broken toaster, an AI system might produce a dangerous result depending on learning patterns or dynamic inputs that weren't considered during design.

Contractual Limitations and Disclaimers

Terms of service, end-user license agreements, or disclaimers that aim to restrict liability are found in many AI platforms and products. These provisions might require that the software be used "as is," or they might put the onus of supervision on the user. When used in high-stakes AI applications like healthcare, criminal justice, or autonomous vehicles, these terms raise

[8] David Goad and Uri Gal, "Understanding the impact of transparency on algorithmic decision-making legitimacy", in Matti Rossi, Mikko Siponen, et.al. (eds.), Working Conference on Information Systems and Organizations 64–79 (Springer International Publishing, Cham, 2018).

[9] Billups P. Percy, "Products Liability—Tort or Contract or What" 40 *Tulane Law Review* 715 (1965).

serious concerns even though they are legally enforceable in many jurisdictions[10].

Contractual disclaimers might not be enough to release parties from liability in situations where life, liberty, or rights are at risk. When such clauses clash with the public interest or fundamental rights, courts are starting to examine them more closely.

Criminal Liability and Intent

The concepts of actus reus (guilty act) and mens rea (guilty mind) form the foundation of criminal law. AI cannot create the mental state required for criminal liability because it lacks consciousness and intent. The possibility of imposing derivative criminal liability on human actors who create or implement AI systems carelessly or with egregious negligence has been raised by this[11].

For example, should the creators of an autonomous car face manslaughter charges if a fatal collision results from software defects? In situations like these, where human control is limited or indirect, it would be necessary to reconsider the concepts of causation, foreseeability, and duty of care.

International Regulatory Developments

European Union: The proposed EU AI Act places stringent requirements on high-risk applications, like credit scoring or biometric surveillance and categorizes AI systems according to risk. It requires risk assessments, human oversight and transparency but does not establish new liability regimes[12].

United States: No comprehensive federal AI law exists in the United States. Most of the regulation is state-driven and sector-specific (for example, healthcare or finance). Instead of legal requirements, the emphasis is still on voluntary guidelines like the NIST AI Risk Management Framework.

India: Laws pertaining to AI have not yet been put into effect in India. AI-related issues are indirectly covered by the current legal framework, which includes the Consumer Protection Act of 2019 and the Information Technology Act of 2000. Although the need for "responsible AI" was highlighted in a 2023 NITI Aayog report, legal enforceability is still lacking.

[10] Michael G. Pratt, "Disclaimers of Contractual Liability and Voluntary Obligations" 51 *Osgoode Hall Law Journal* 767 (2013).

[11] Roman Veresha, "Criminal and Legal Characteristics of Criminal Intent" 24 *Journal of Financial Crime* 118-128 (2017).

[12] Tatevik Davtyan, "An Overview of Global Efforts Towards AI Regulation" 15 *Bulletin of Yerevan University C: Jurisprudence* 158-174 (2024).

Why Traditional Law Falls Short

When it comes to artificial intelligence, traditional legal doctrines have significant limitations. The problem of causation, which is frequently diffuse and indirect in AI systems, is one of the biggest obstacles. AI results are often the result of intricate interactions between code, data, learning algorithms, and environmental inputs, in contrast to traditional liability scenarios where a particular action directly causes harm. It becomes very challenging to follow a direct line of cause and effect as a result. Although AI systems function without consciousness or volition, legal responsibility usually depends on the existence of intent or knowledge of potential harm. The application of concepts like negligence or recklessness is made more difficult by algorithmic decisions that lack human intent[13].

The delayed nature of harm in AI use presents another challenge. In contrast to a flawed product that results in harm right away, algorithmic harm can appear only after extended or iterative use, as in the case of predictive policing tools or biased recruitment algorithms. The repercussions might not be immediately apparent until discriminatory or mistaken patterns are discovered over time, at which point it becomes more difficult to seek legal remedies. The fact that accountability for AI systems is frequently split among several parties, including developers, data providers, vendors and end users, who may be based in different countries, further complicates matters. In addition to obscuring legal responsibility, this accountability fragmentation makes it difficult to enforce laws in cross-border situations.

Given these difficulties, it is becoming increasingly obvious that conventional legal frameworks are inadequate for handling the dangers presented by autonomous systems. If current doctrines were all that were used, the results would probably be inconsistent, reactive, and insufficient. Instead, a forward-thinking legal framework that is especially adapted to the special features of AI technologies and upholds the values of accountability, transparency and fairness is desperately needed.

IV. IDENTIFYING LIABILITY: WHO CAN BE HELD RESPONSIBLE?

It is necessary to carefully examine the different actors involved in the development, application, and use of AI systems to decide who should be responsible for any harm they cause. AI systems are rarely the product of a single manufacturer or entity, in contrast to conventional tools or products. Rather, they are created by a complex ecosystem that includes end users, corporate entities, data scientists, software developers, and third-party service

[13] Steven Feldstein, "Evaluating Europe's Push to Enact AI Regulations: How Will This Influence Global Norms?" 31 *Democratization* 1049-1066 (2024).

providers. The assignment of legal responsibility is a complex problem because each of these actors may have a different impact on the algorithm's behaviour and results[14].

The decision-making logic of an AI system is frequently shaped in large part by developers and designers. They choose the performance goals, training parameters, and algorithms to be used. There is a compelling case for holding the developers of the AI liable if the harm is caused by defective code, inadequate testing, or predictable outcomes that were disregarded during development. However, a lot of developers are employed by corporations, which may protect people by virtue of the corporate liability principle. In these situations, the business that owns and sells the AI product is a better target for legal action. This is in line with the more general legal precept that the people who benefit from a technology should also be responsible for the risks it presents[15].

Businesses that implement AI systems in real-world environments play an equally important role. The final say over how the technology is used is retained by companies that incorporate AI tools into their decision-making processes, such as insurance companies using predictive models or hospitals using diagnostic AI. These organizations risk being held accountable for negligence or failing to exercise due care if they employ AI systems without being aware of their limitations, neglect to provide sufficient human oversight, or disregard early warnings about bias or inaccuracy. Even if the harm was indirectly brought about by AI, the idea of "vicarious liability" may also be applicable in situations where a company is held accountable for the deeds of its personnel or tools[16].

There is also some accountability on the part of data providers and those who train AI systems. Biased or unrepresentative datasets can produce unsafe or discriminatory results because machine learning results heavily rely on the quality of the training data. Those in charge of data curation and preprocessing may be held partially liable if harm is caused by predictable errors in the data, such as the use of arrest records that exhibit systemic racial bias. However, it can be difficult to demonstrate a connection between data bias and personal injury, particularly when the AI system has changed because of new inputs or interactions[17].

End users, such as judges, employers, consumers, and government representatives, may also be held partially accountable, especially if they use AI as a "black box" without exercising

[14] Jean-Sébastien Borghetti, "Civil Liability for Artificial Intelligence: What Should Its Basis Be?" 17 *La Revue des Juristes de Sciences Po* 94-102 (2019).

[15] W. Nicholson Price II, Sara Gerke, and I. Glenn Cohen, "Liability for Use of Artificial Intelligence in Medicine," in *Research Handbook on Health, AI and the Law* 150–166 (2024).

[16] Mark A. Geistfeld, Ernst Karner, Bernhard A. Koch, and Christiane Wendehorst (Eds.), *Civil Liability for Artificial Intelligence and Software*, vol. 37 (Walter de Gruyter GmbH & Co KG, 2022).

[17] Chaudhary, Gyandeep. "Artificial Intelligence: The Liability Paradox." *ILI Law Review* (2020).

critical judgment. The role of the human intermediary in permitting or exacerbating harm must be carefully examined, for instance, if a judge makes sentencing decisions based only on automated resume filters without review, or if an HR manager bases hiring decisions entirely on these criteria. Courts can assess whether users exercised reasonable caution, questioned dubious outputs, or heedlessly followed unsubstantiated AI recommendations[18].

Some academics and decision-makers have suggested shared or tiered models of liability because of the multiple parties involved. Under this approach, responsibility could be distributed proportionally based on the level of control, foreseeability of harm, and the capacity of each actor to mitigate risk. Another proposal is the use of "strict liability" in high-risk situations, where specific actors usually corporations would be held liable regardless of fault just for using the AI. Stronger incentives for safety, transparency and oversight would result from this, which would resemble product liability regimes.

In the end, determining culpability in AI cases requires more than just assigning blame. It calls for a systems-level viewpoint that acknowledges the interconnectedness of technological and human actors. By creating distinct lines of accountability, requiring mandatory audit trails, and mandating documentation of development choices, legal reform should take this complexity into account. Only then will the law be able to keep up with the changing risks posed by AI and guarantee that individuals impacted by algorithmic decisions have significant channels for legal recourse.

V. CASE STUDIES: WHEN ALGORITHMS GO WRONG

Examining real-world instances where algorithmic systems have resulted in actual harm is crucial to comprehending the ramifications of AI-driven decisions and the difficulties in determining legal liability. These case studies highlight the institutional and regulatory shortcomings that have permitted such harms to continue unchecked, in addition to the technological complexity of AI. They also draw attention to the pressing need for more transparent accountability frameworks that can handle both personal complaints and systemic issues.

The application of the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) tool in the American criminal justice system is among the most frequently cited instances of algorithmic failure. Judges have used COMPAS, which was created to evaluate the likelihood of recidivism among defendants, when determining bail and sentencing. But

[18] Wagner, Gerhard. "Liability for Artificial Intelligence: A Proposal of the European Parliament." *Available at SSRN 3886294* (2021).

according to a 2016 ProPublica investigative report, the algorithm had serious racial bias and incorrectly flagged Black defendants as high-risk at a rate that was almost twice as high as that of white defendants. Despite these discoveries, the COMPAS developer refused to reveal the inner workings of the algorithm, citing proprietary protection. The courts maintained its use, ruling that defendants lacked the authority to investigate the inner workings of the instrument[19].

Another warning in the private sector comes from Amazon's experimental AI hiring tool. Ten years' worth of resumes submitted to the company were used to train the system, which was created in 2014 to expedite the hiring process. With time, the AI started penalizing resumes from graduates of all-female colleges and downgrading applications that contained the word "women's," such as "women's chess club captain." This gender bias was not intentionally coded; rather, it developed from historical data showing hiring trends that were dominated by men. Amazon dropped the project after learning of the bias. This case raises issues regarding data governance, employer liability, and the boundaries of automated decision-making in delicate human resource contexts by demonstrating how machine learning systems can inadvertently reproduce discriminatory practices that are ingrained in historical data[20].

The 2018 Tempe, Arizona, fatal accident involving an autonomous Uber car is another noteworthy instance. At night, the self-driving car killed a pedestrian who was crossing the street. According to investigations, the pedestrian was detected by the car's software, but it was unable to appropriately identify her as a hazard and initiate evasive action. At the crucial moment, the safety driver behind the wheel was not paying attention. Despite apparent shortcomings in system design and corporate oversight, Uber was not sued, even though the driver was ultimately charged with negligent homicide. The case brought up challenging issues regarding shared accountability between AI systems, corporate developers, and human operators. It revealed how inadequate current criminal and traffic laws are to handle autonomous technologies[21].

Algorithmic trading systems have also caused market instability in the financial services industry. Due in large part to the interactions of high-frequency trading algorithms, the Dow Jones Industrial Average fell by almost 1,000 points in a matter of minutes during the 2010

[19] Brennan, Tim, Bill Dieterich, Markus Breitenbach, and Brian Mattson. "A Response to 'Assessment of Evidence on the Quality of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)'." *Traverse City, MI: Northpointe Institute for Public Management*, 2009.

[20] Tripuraneni, Subhashini, and Charles Song. Hands-On Artificial Intelligence on Amazon Web Services: Decrease the Time to Market for AI and ML Applications with the Power of AWS. Packt Publishing Ltd, 2019.

[21] Arrowsmith, J. Ramon. "Structural Geology and Tectonics Forum at Arizona State University, Tempe, AZ, January 4-9, 2018." *NSF Award Number 1743564. Directorate for Geosciences* 17, no. 1743564 (2017): 43564.
Ask ChatGPT

"Flash Crash." The incident demonstrated how intricate, self-reinforcing algorithmic behaviours can result in systemic risks, even though it was challenging to determine the precise liability. Regulators found it difficult to place blame or put preventative measures in place, which made it clear that algorithmic financial instruments needed more stringent oversight[22].

AI's application in medical diagnostics is a more recent example. According to a 2020 study, even when Black patients were just as ill as white patients, an AI system that is frequently used in American hospitals to distribute healthcare resources was less likely to refer them for further care. The algorithm unintentionally underestimated the severity of illness among Black patients, who traditionally spend less on healthcare due to systemic inequities, by using healthcare costs as a proxy for health needs. Indirect discrimination, the suitability of proxies in medical AI and hospitals' and vendors' obligations to verify algorithmic fairness were among the ethical and legal issues this brought up.

These case studies each highlight a distinct aspect of the liability conundrum. The ramifications of poor AI decisions are extensive and profound, ranging from bias and opacity to systemic risk and bodily harm. However, current legal systems have almost always failed to deliver prompt remedies or unambiguous accountability. Due to a combination of jurisdictional fragmentation, contractual shielding and legal ambiguity, victims frequently have no recourse while developers and deployers avoid repercussions. These illustrations highlight the necessity of proactive, legally binding frameworks that guarantee AI technologies are developed, implemented, and overseen with accountability at their centre.

VI. The debate on AI personhood and autonomous liability

Legal scholars and policymakers are starting to investigate whether AI systems should be given some sort of legal personhood as they grow more independent and able to make complicated decisions without direct human intervention. Similar to how corporations are regarded by the law, the idea of AI personhood aims to acknowledge some AI systems as autonomous beings with the capacity to have rights and obligations. Though contentious, this concept has drawn interest as a potential remedy for the widening accountability gap in AI-related harms, especially in situations where it is impossible to pinpoint a single human actor as being at fault[23].

AI personhood proponents contend that existing legal frameworks are essentially insufficient

[22] Akansu, Ali N. (2017). The flash crash: A review. *Journal of Capital Markets Studies, 1*(1), 89–100.

[23] Sen, Arghya. (2023). Artificial intelligence and autonomous systems: A legal perspective on granting personhood and implications of such a decision. *DME Journal of Law, 4*(01), 15–26.

to handle sophisticated autonomous systems. These systems frequently take decisions based on real-time data, behave in unpredictable ways, and change over time because of machine learning. In these situations, conventional theories that depend on human carelessness or intent fall short of describing the type of harm that AI causes. Theoretically, legal personhood for AI might enable liability to be directly attributed to the system, like how a corporation can be sued or fined without the involvement of its executives or shareholders. In addition to encouraging developers to include fail-safes and ethical safeguards in AI design, this would make it easier for victims to get compensation[24].

In a 2017 resolution, the European Parliament raised the possibility of giving the most advanced AI systems "electronic personhood." The goal was to hold these organizations legally responsible for any harm they inflict, possibly with the help of mandated insurance plans or compensation funds. Despite not becoming law, the proposal sparked debates around the world regarding the legality and philosophy of giving non-human entities rights or obligations. Without implying that AI systems have moral agency, feelings, or consciousness, some academics contend that electronic personhood could function as a legal fiction a practical means of filling legal voids[25].

Critics of AI personhood, however, bring up several moral, legal and pragmatic concerns. One significant worry is that establishing a legal barrier between AI developers and systems could shield human actors from accountability. Companies may use legal personhood to shift accountability to machines, undermining human accountability, if AI entities turn into "fall guys." Moral agency and the capacity to comprehend and abide by legal norms qualities that modern AI systems do not and possibly cannot possess have historically been associated with legal personhood. AI lacks consciousness, free will and the ability to discriminate between right and wrong. Therefore, giving such systems legal responsibility could weaken the moral underpinnings of the law and dilute the meaning of liability[26].

There are major obstacles to practical implementation as well. An AI system needs to be able to own assets, have legal counsel, and have a way to compensate victims to be regarded as a legal entity. This brings up difficult issues regarding financing, authority, and legal status. Who would represent the AI? Who would supply its resources? What happens if it stops operating

[24] Lovell, Jasmine. (2023). Legal aspects of artificial intelligence personhood: Exploring the possibility of granting legal personhood to advanced AI systems and the implications for liability, rights and responsibilities. *Rights and Responsibilities*, (May 10, 2023).

[25] Braun, Tomasz. (2025). Liability for artificial intelligence reasoning technologies–a cognitive autonomy that does not help. *Corporate Governance: The International Journal of Business in Society*.

[26] Novelli, Claudio. (2023). Legal personhood for the integration of AI systems in the social context: a study hypothesis. *AI & Society, 38*(4), 1347–1359. https://doi.org/10.1007/s00146-022-01537-5

or goes "bankrupt"? The model of AI personhood runs the risk of becoming less of a workable legal solution and more of a theoretical curiosity in the absence of definitive answers.

The creation of quasi-personal liability models, which acknowledge that AI systems function somewhat independently but still impose legal accountability on their human creators or operators, is an alternative to full personhood. This includes the idea of "assigned liability," in which accountability is given according to who has the greatest influence, knowledge, or advantage over the actions of the AI system. To guarantee that victims receive compensation regardless of fault, some advocate for the introduction of mandatory insurance programs that require developers and deployers of high-risk AI systems to maintain liability coverage, akin to auto insurance.

"AI trusteeship models," in which AI systems function under the legal supervision of a responsible person or organization, are also gaining popularity. This arrangement is based on legal parallels in guardianship and trust law, where a legally responsible agent acts on behalf of an entity that lacks legal capacity, like a minor or someone with a disability. Such a model, when applied to AI, could recognize the system's functional autonomy while upholding human accountability[27].

VII. Proposals for reform and future directions

The demand for strong legal reform is intensifying as artificial intelligence becomes more pervasive in important decision-making procedures. Policymakers and academics are proposing specific changes that consider the realities of algorithmic governance because traditional liability doctrines are finding it difficult to keep up. By balancing innovation and societal protection, these proposals seek to close the accountability gap. In this changing legal environment, several important reform recommendations have emerged as leaders.

AI-Specific Liability Laws

Creating legal frameworks specifically for AI is one of the most urgent needs. The intricacy of algorithmic decision-making is frequently overlooked by generic tort or product liability laws. By establishing a risk-based framework for regulating AI systems and lowering the burden of proof for claimants, the European Union has taken the lead with its proposed AI Liability Directive and AI Act. These frameworks can be used as templates by other jurisdictions, assisting regulators and courts in assessing responsibility, harm, and foreseeability in AI-

[27] Brown, Lloyd A. (2025). Artificial intelligence & Trusts and Trustees: A new dawn of investment opportunities and risks? Trusts & Trustees, 31(5), 210–215. https://doi.org/10.1093/tandt/ttae017

related incidents.

Transparency and Auditability Requirements

Enforcing transparency in the creation and application of AI systems is a second crucial reform. This entails keeping thorough audit trails that record the sources of data, model training procedures, performance reviews, and reasoning behind decisions. Legal liability would now be based on both the documented diligence used in design and testing as well as the results. Even in cases where the system is a "black box," accountability would be made possible by these audit logs, which would be essential evidence in court. In high-stakes situations like healthcare, finance and criminal justice, explainability the ability of AI decisions to be comprehended by humans should be a legal requirement.

Mandatory AI Insurance Schemes

Many experts advocate for mandatory insurance for AI systems to guarantee compensation for victims, regardless of how difficult it may be to prove fault. Such programs would require AI developers and implementers, especially those working in high-risk fields, to maintain coverage, much like auto insurance does. The system's risk profile and potential for damage would determine premiums. This strategy lowers financial risk, shields victims from drawn-out legal proceedings and motivates businesses to put in place more robust security measures to control insurance premiums.

Human-in-the-Loop Oversight

Legally requiring human oversight in AI decision-making is another widely supported reform, especially in fields where mistakes can have serious consequences. Laws could require "human-in-the-loop" (HITL) protocols, in which human agents actively participate in approving or vetoing algorithmic decisions. However, genuine authority and critical analysis not just formality are required for such oversight to have any significance. The idea that humans must always be ultimately accountable should be reinforced by extending legal liability to users who rely on AI but fail to use appropriate judgment.

Creation of AI Regulatory Authorities

The intricacy and scope of AI implementation outside of courtrooms necessitate constant regulatory oversight. Many advocates for the creation of national and regional commissions or bodies specifically tasked with overseeing AI. These organizations would be able to issue interpretive guidelines, impose sanctions, investigate harm and certify systems. They would help standardize compliance, facilitate public scrutiny and maintain centralized registries of AI systems. Under the GDPR, these organizations would operate similarly to data protection authorities, providing much-needed institutional support for law enforcement.

International Harmonization of Liability Standards

The necessity of cross-border uniformity in legal standards is becoming increasingly apparent given the worldwide scope of AI development and application. International organizations like the Global Partnership on AI, UNESCO and the OECD have started to develop model policies and common principles. Multinational firms would gain from harmonizing liability laws, which would also allow for fair competition and guarantee that people are protected no matter where harm occurs. Regulatory arbitrage, in which businesses relocate their operations to less restrictive jurisdictions, could also be avoided with concerted efforts.

Embedding Normative Legal Principles

Any reform initiative needs to be based on moral and legal principles that endure. All future AI laws must be based on the values of accountability, openness, human dignity, equity and redress. These standards ought to be operationalized through enforceable laws in addition to being aspirational. Legislators and courts need to strike a balance between allowing AI developers unbridled freedom and preventing innovation by being overly cautious. Rather, the law needs to develop into a flexible, adaptable framework that protects rights and advances technology.

VIII. Conclusion

The problem of determining who is responsible for algorithmic decisions is becoming more pressing and intricate as artificial intelligence becomes more integrated into our legal, economic and social structures. The harms caused by autonomous, data-driven systems are beyond the scope of traditional legal frameworks, which are based on presumptions of human intent, control and foreseeability. AI has shown both its enormous potential and its ability to have unexpected, unclear and occasionally negative effects in a variety of fields, including content moderation, healthcare diagnostics, predictive policing and financial decision-making. The issue of "who is responsible" is no longer merely theoretical in these situations; it has practical implications for accountability, justice and public confidence.

The different facets of liability related to AI have been examined in this article, starting with the shortcomings of traditional theories like strict liability, product liability and negligence. When the actor is non-human, the harm is diffuse and the causal chain is obscured by intricate algorithmic procedures, these legal classifications find it difficult to adjust. When AI systems learn and develop in ways that even their designers cannot completely predict, it becomes challenging to apply the conventional concepts of intent and foreseeability. Because of this, people who are harmed by algorithms frequently have few legal options, and those who create and implement AI systems are subject to unclear legal obligations.

There have been several attempts to close this gap. While some advocate for more radical solutions, like giving AI systems a limited form of legal personhood, others suggest revisiting current doctrines and extending them to accommodate AI. Given that AI systems lack consciousness, moral agency and autonomy, the latter is still controversial from an ethical and practical standpoint. Promising avenues for improvement are provided by more practical models like assigned liability, required insurance and human-in-the-loop supervision. These methods recognize the unique operational nature of AI while maintaining the importance of human accountability.

There is increasing agreement that a reactive or piecemeal approach is insufficient. A comprehensive, forward-thinking legal framework that can adjust to the difficulties presented by AI technologies is what is required. The fundamental tenets of such a framework must be normative: accountability, transparency, fairness, and redress. Clarifying the responsibilities and liabilities of different players in the AI development lifecycle, offering victims practical and effective remedies, and establishing incentives for moral design and implementation are all important goals. After all, the public as well as investors and innovators looking to create reliable systems gain from legal certainty.

International cooperation will be crucial. AI transcends national borders; its creation and application frequently take place in different jurisdictions. Uneven protections, regulatory arbitrage, and legal fragmentation are possible in the absence of coordinated standards. A fairer and more predictable legal environment may be achieved in large part through mutual recognition of AI accountability frameworks, interoperability in certification and shared global standards.

It is a test of our collective ability to regulate emerging technologies in ways that uphold democratic values and human dignity, not just a legal technicality. The law must change along with AI. To make sure that technological advancement doesn't come at the price of justice and accountability, a proactive, moral, and flexible legal response will be necessary.

*****

IX. References

1. Rizkia, Nanda Dwi et al., "Legal Protection of Consumers in Electronic Transactions: Challenges and Future Prospects," (2024) 4(2) Journal Equity of Law and Governance 307.
2. Swandari, Selly, Swadia Gandhi Mahardika & Tengku Andrias Prayudha, "Legal Protection for Consumers in E-Commerce Transactions: Challenges and Solutions in the Digital Era," (2025) 2(1) Journal of Mujaddid Nusantara 23.
3. Kumalasari, Indra & Hengki Syahyunan, "Uncovering Legal Gaps in Digital Banking: Customer Protection and Bank Accountability in Indonesia," (2024) 25(2) LITIGASI 301.
4. Nedumaran, G., D. Mehala & M. Baldevi, "Consumer Protection Act 2019 – An Overview," (2022) 9(9) Mukh Shabd Journal.
5. Misra, Adrita, "The Consumer Protection Act, 2019 – A Comparative Analysis," (2022) 4(3) Indian J.L. & Legal Rsch. 1.
6. Consumer Protection (E-Commerce) Rules, 2020, Ministry of Consumer Affairs, Government of India.
7. Information Technology Act, 2000, No. 21 of 2000, India Code.
8. Silfiah, Rossa Ilma, Kristina Sulatri & Yudhia Ismail, "Legal Protection of Consumers with Online Transactions," (2024) 4(6) Journal of Law, Politic and Humanities 2584.
9. Kaur, Ravinder & Chinmay Sahu, "Cryptography in Industry: Safeguarding Digital Assets and Transactions," in Next Generation Mechanisms for Data Encryption (CRC Press, 2025) 146.
10. Pandey, Siddharth Kumar, "Legal Safeguards for Consumers in E-Commerce Transactions: An Analytical Study."
11. Seritti, Laura, "Online Shopping and Quality Problems: What Safeguards for Platform Users Under the EU Consumer Protection Regime?," (2021) 10(5) Journal of European Consumer and Market Law.
12. Information Technology (Reasonable Security Practices and Procedures) Rules, 2011, G.S.R. 313(E), Ministry of Electronics and IT.
13. Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code.

14. Puri, K., "Protection Against Monopolistic and Unfair Trade Practices in India," (1992) 34(3) Journal of the Indian Law Institute 443.
15. Cox, James R., "State Consumer Protection or Deceptive Trade Practices Statutes: Their Application to Extensions of Credit and Other Banking Activities," (1988) 105 Banking L.J. 214.
16. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E).
17. Glöckner, Jochen, "Unfair Trading Practices in the Supply Chain and the Co-ordination of European Contract, Competition and Unfair Competition Law in Their Reaction to Disparities in Bargaining Power," (2017) 12(5) J. of Intellectual Property Law & Practice 416.
18. Hockstad, Trayce et al., "A Regulatory Gap Analysis in Transportation Cybersecurity and Data Privacy," (2025) 64(1) Transportation Journal e12036.
19. Dean, James B., "The Foreign Unauthorized Insurer: A State Regulatory Gap," (1965) 32 Ins. Counsel J. 432.
20. Sharma, Vivek et al., "Regulatory Framework Around Data Governance and External Benchmarking," (2022) 14(2) J. of Legal Affairs and Dispute Resolution in Engineering and Construction 04522006.
21. Seth, Swati Bajaj, "Reviewing the Anticompetitive Practices in Indian Digital Market: Probable Gaps in Existing Competition Law and Need for Digital Competition Act," in Intellectual Property Rights and Competition Law in India (Routledge, 2024) 42.
22. Bhagotra, Arushi & Rounak Doshi, "Bridging the Gap Between SEBI's Investigation Procedure and Principles of Natural Justice – Identifying the Loophole in the Law," (2022) 5 J. on Governance 164.
23. Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises, (2019) Delhi High Court.
24. Prachi Agarwal v. Swiggy, (2021) National Consumer Disputes Redressal Commission (NCDRC).
25. Passos de Freitas, Vladimir, "The Role of Regulatory Agencies," (2014) 44 Envtl. Pol'y & L. 552.

26. Berry, William D., "Theories of Regulatory Impact: The Roles of the Regulator, the Regulated, and the Public," (1982) 1(3) Review of Policy Research 436.

27. Osman, Magda, "Psychological Harm: What is It and How Does It Apply to Consumer Products with Internet Connectivity?," (2025) J. of Risk Research 1.

28. Heath, Amanda J., "Commentary on 'Psychological Harm: What is It and How Does It Apply to Consumer Products with Internet Connectivity?' by Magda Osman," (2025) 28(2) J. of Risk Research 154.

29. Panjaitan, Hulman & Nindyo Pramono, "Legal Protection of Consumers in Digital Transactions," (2023) 11(3) Russian Law Journal 1431.

30. Tan, Qingyue, "Research on International Consumer Protection Mechanisms in Cross-Border E-Commerce Transaction Security," in 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024) (Atlantis Press, 2024) 359.

31. Verico, Kiki, The ASEAN Economic Integration Principles: Open, Convergence, Inclusive, and Green (Institute for Economic and Social Research, Universitas Indonesia, 2022).

32. Bradley, Christopher G., "The Consumer Protection Ecosystem: Law, Norms, and Technology," (2019) 97 Denver L. Rev. 35.

33. Ballaji, Nima, "Consumer Protection in the Era of Digital Payments: Legal Challenges and Solutions," (2024) 15 Beijing L. Rev. 1268.

34. Pandey, Aishwarya, "Consumer Protection in the Era of E-Commerce: Issues and Challenges," (2022) 4(1) International Journal of Legal Science and Innovation.

35. Shreya, G., "Technological Advancements in Enforcement of Consumer Rights: Online Dispute Resolution," in ADR Strategies: Navigating Conflict Resolution in the Modern Legal World (2022) 247.

*****