ISSN: 3048-4782

VOL. III ISSUE I

BEYOND BRIEFS LAW REVIEW

VOLUME III ISSUE I

DATE OF PUBLICATION: 31.12.2025

FREQUENCY: BI-ANNUAL

PUBLICATION CYCLE: (JULY - DECEMBER) 2025

ISSN: 3048-4782

VOL. III ISSUE I

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of the Publishing Editor of Beyond Briefs Law Review. The Editorial Team of Beyond Briefs Law Review and the Author holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of Beyond Briefs Law Review. Though all efforts are made to ensure the accuracy and correctness of the information published, Beyond Briefs Law Review shall not be responsible for any errors caused due to oversight or otherwise.

AI-GENERATED DECISIONS AND LEGAL RESPONSIBILITY: WHO SHOULD HAVE THE RESPONSIBILITY?

~ *Mahashweta Mitra* [1]

Abstract

The integration of artificial intelligence (AI) into various sectors such as governance, healthcare, and law enforcement is reshaping legal responsibility frameworks. As AI systems operate with less human oversight, traditional liability concepts struggle to adapt. The paper analyzes accountability for harm caused by AI decisions and explores responsible parties—developers, deployers, or the AI itself—using comparative legal research across the UK, EU, and US. Challenges include transparency issues within machine learning, data contamination, and responsibility distribution in AI supply chains. In India, existing laws like the IT Act and Consumer Protection Act are inadequate for addressing autonomous AI harms. The study recommends establishing a layered liability system to address industry-specific risks, advocating for strict liability in high-risk applications and thorough pre-deployment audits. Ultimately, it asserts that AI's autonomy cannot exempt human or corporate accountability, urging a legal reassessment to clarify responsibilities of those involved with intelligent systems.

Keyworks

Algorithmic Accountability, AI Liability Frameworks, Strict Product Liability, Risk Based Regulation, Autonomous Systems Governance

[1] You may contact the author at the following email address: mahashweta.mitra25@outlook.com

INTRODUCTION:

Artificial intelligence has come a long way beyond suggesting a film or creating a playlist in the world where our decisions are made unknowingly by technology. It can now decide whether an individual gets a loan or not, whether someone is suspicious in a bank account or whether an investor can manage his finances or not. Its pace and precision will be efficient, but there is also a new form of risk that is bound to emerge with this ever-increasing dependency which cannot be easily traced back to a single act, individual or machine[2].

This is not the first time that this tension has been experienced. Patients decades ago, imagined intelligent systems that were able to think, act and even defy human commands, just like the cases of 2001: A Space Odyssey. When Bowman threatens HAL, "Unless you follow my order I will have to disconnect you," the war was an expression of anxiety over machines that are not ready to relinquish power. The thing which previously existed only in fiction, has returned to real life, particularly with the emergence of generative AI. The moral dilemmas that amused the audience are now real issues that need to be addressed by legislators, companies, and society.

What we had expected much less though, is the challenge of grasping how AI comes up with its decisions and, more to the point, who should be held accountable when the decisions are wrong. In the absence of understanding how these systems work, or even any real comprehension of the dangers that they present, the consequences of AI involvement can become unjust, unreasonable, and detrimental, and the blame will be shifted to the wrong hands[3].

With the advent of AI, fast turning into a futuristic dream into a daily companion, appearing in the homes, the workplaces, and the markets, the question of responsibility has become a problem that cannot be disregarded anymore. In cases where an AI system makes an action or a judgment, who is responsible? Current liability frameworks are unable to keep up with AI especially when it acts unpredictably or when it exhibits some level of autonomy that erases the distinction between creator, user and machine. The disease becomes more difficult to prove the error or causation in

[2] Erica Stanford, *Autonomous AI: Who is Responsible When AI Acts Autonomously and Things Go Wrong?*, Global Legal Insights (Nov. 2025) https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/autonomous-ai-who-is-responsible-when-ai-acts-autonomously-and-things-go-wrong/

[3] OAL Law, *Understanding AI Liability: Who's Responsible When Algorithms Err?*, OAL Law, https://oal.law/understanding-ai-liability-whos-responsible-when-algorithms-err/

bearing in mind that the models are complex and cannot be fully predicted or traced by producers or users[4].

Such challenges have led to further economic and legal considerations on how rules can be most apt at reducing harm and yet promote innovation[5]. Here, emerging proposals like the revised Product Liability Directive and AI Liability Directive by the EU are trying to fill the gaps, which are the first significant steps to a more consistent and future-oriented accountability regime.

KNOWING AUTONOMOUS AI AND THE ORIGINS OF RESPONSIBILITY:

At a time when automated systems silently decide who is creditworthy, a transaction is suspicious or even how a car should react in a split second, artificial intelligence has long since left the realm of science-fiction fantasy. Such systems are now affecting the choices which were previously only subject to human decisions.

Autonomous AI can be defined as the systems that are able to decide or to perform actions without human supervision. Autonomous AI learns with huge amounts of data, updates internal parameters, and develops over time unlike traditional software that runs a pre-written, rule-based script that the programmer writes line-by-line. This learning process is also facilitated by machine learning models like artificial neural networks that facilitate the system to make classifications, predictions, or judgments that the developers may not always understand in detail. When AI is presented with new information or changes in the conditions of its operation, it can act in a way that is not consistent with the original training, producing the results that seem opaque or even counterintuitive. This complex interaction of size, complexity, and lack of transparency makes attributing legal responsibility upon harm a difficult task.

These difficulties are not on paper. In 2018, one of the Uber self-driving tests in Arizona hit and killed a pedestrian. Even though the sensors in the car did identify the woman, the system did not identify her as a danger that needed to be braked upon. There was human safety driver who was distracted. The tragedy has revealed the unpleasant truth that the decision made by the AI was at the center of the accident, but it is the safety driver who has been targeted by the legal system rather than the corporation that created, implemented, and promoted autonomous technology. Other controversies include Tesla Autopilot whereby fatal crashes beg some hard questions; is it

[4] HFW, *Legal Liability for AI-Driven Decisions: When AI Gets It Wrong, Who Can You Turn To?*, HFW Insights, https://www.hfw.com/insights/legal-liability-for-ai-driven-decisions-when-ai-gets-it-wrong-who-can-you-turn-to/c

[5] RiskInfo.AI, *Who Is Responsible When AI Makes a Mistake?*, RiskInfo.AI Blog, https://www.riskinfo.ai/post/who-is-responsible-when-ai-makes-a-mistake

the drivers who are responsible because they put too much trust in a semi-autonomous system or is it the company that created and promoted the same dependency with the choice of design and promotion[6]?

Autonomous AI may have severe real-world effects even without causing physical damage. The Microsoft chatbot Tay went viral with offensive text after adversarial manipulation; the Amazon[7] job search application filtered out female applications since the system learnt through biased historical data; and the 2010 Flash Crash demonstrated that even in the case of interacting trading algorithms, a collective destabilization of financial markets can be made by any individual without the intention or foresight to cause it. These examples demonstrate one similarity: the activity of AI systems cannot be explained only by a human error of an individual person, as their behavior is frequently the product of semi-autonomous learning, the complexity of models and non-deterministic procedures.

Machine learning systems operate under the features that essentially redefine the concept of responsibility. Their semi-autonomy implies that engineers do not directly decide what correlations the system will recognize and what features it will deem the most crucial. They are extremely challenging to trace causation because of their complexity: their enormous datasets, millions of internal parameters, etc. Their non-determinism implies that a similar input may at times yield different outputs, which invalidates the traditional liability models, which depend on predictability. Together, these characteristics contemplate the belief that the developer, the deployer or the user can always be the one identified as the culprit when something bad happens.

The ethical and legal question of how much to place responsibility on the individuals who design, train, deploy, regulate, and depend upon autonomous AI systems is not whether such systems can act autonomously, but how such systems should share such responsibility among those involved in creating these systems, training them, deploying them, controlling them, and depending on them. This is an oversimplification of a highly complicated socio-technical ecosystem by placing the blame on one side. Rather, comprehending the emergence of autonomy into AI- and how its opaque decision-making proceeds is the pivotal basis of building equitable, practical, and contemporary structures of legal responsibility.

[6] VinciWorks, *AI in the Dock: Who Is Liable When Machines Get It Wrong?*, VinciWorks Blog, https://vinciworks.com/blog/ai-in-the-dock-who-is-liable-when-machines-get-it-wrong/am

[7] Emerge Digital, *AI Accountability: Who's Responsible When AI Goes Wrong?*, Emerge Digital, https://emerge.digital/resources/ai-accountability-whos-responsible-when-ai-goes-wrong/

MAKING OUR WAY IN AN AGE OF AUTONOMOUS AIS:

Since artificial intelligence systems are taking on the role of acting with a certain level of autonomy that can only be used by humans in the past, the question of who should bear responsibility when such systems malfunction has been at the forefront in current technology law. Self-driven AIs-machines that can make decisions and adjust to new events and operate without direct human control have ceased to be a subject of fantastical fiction and become a part of reality. Such systems move cars, filter loan applications, handle insurance claims, monitor the public areas, and even give advice to physicians. There is a new form of legal uncertainty that comes with this autonomy, however, as an AI can take a harmful or erroneous decision, who is to be held responsible?

The old model of liability which was developed on a premise that products are fixed and predictable fails to hold[8] in the fluid and data-driven behavior presented by AI. Classical software is executed on deterministic algorithms which are coded by humans; errors can frequently be reported to an apparent language programming mistake or hardware fault. Machine learning systems on the other hand regarding these systems, they learn, just by looking at huge amounts of data, they update their internal parameters, and they act in manners that even the creators of these systems can never fully predict. Their logic is usually non-transparent, not always deterministic and regularly changes post-deployment.

Even when a self-driving car wrongly classifies a pedestrian, or a recruitment algorithm targets women, or a financial model causes market instability, the law still demands that a human or an organization should compensate the damage. The machine can never be sued, punished or morally responsible. However, it is not often easy to decide who in the human or the organization should take the responsibility. The new AI entails a stacked ecosystem: data providers, model creators, platform providers, integrators, auditors, regulators and end users. All of them play a role in the functioning of the system yet none of them might directly cause the detrimental output.

The first traditional time-tested doctrines used by the victims are negligence or product liability in which the developers did not test adequately, were aware of the risks yet chose to ignore them or were able to sell the system more than it could perform. However, AI is making these doctrines strained[9]. It may be stated by developers that they could not reasonably anticipate that the harmful

[8] SMS Law College, *Laws for AI: Who Is Liable When a Machine Makes a Mistake?*, SMS Law College Blog, https://blog.smslawcollege.com/laws-for-ai-who-is-liable-when-a-machine-makes-a-mistake/

[9] Legacy Law Offices, *AI on Trial: Rethinking Liability in India's Current Legal Framework*, Legacy Law Offices, https://www.legacylawoffices.com/ai-on-trial-rethinking-liability-in-indias-current-legal-framework/

outcome will occur, or that the problem is caused by the misuse of the user, change of the environment, malicious data poisoning. The concept of a defect, which was previously related to the implication of a faulty product, is only more difficult to pinpoint as the system is constantly modified in a manner that no one has complete authority over.

This uncertainty is manifested by regulatory responses all over the world[10]. The policy of the European Union is based on high-risk AI strict liability, where the deployers and developers are considered guilty without any fault. The US is using a system of disjointed, industry-specific regulation. India, which is yet to have a specific AI liability regime, has thus far been using analogies to product liability, IT Act negligence, and constitutional values. The policy dilemma is obvious, either should the law focus on the protection of the consumer with a strict liability or focus on innovation by a fault-based approach?

Contemporary systems of governance are increasingly appreciating the fact that the issue of AI harm can only be preempted through more than the simple attribution of blame. The control of risks, ongoing surveillance, real-time validation of a model, the need to be transparent, and the control of AI by humans in the loop are rapidly becoming an essential expectation of any participant in the AI value chain. An emerging industry standard in the EU, under the AI Act, the NIST AI Risk Management Framework, and other emerging industry standards around the world focus on documentation, explainability, safety testing, red-teaming and continuous performance reviews. These process-driven tasks recognize an empirical fact: AI malfunctions do not occur overnight but because of a chain of minor glitches that build up due to the common belief that the system is operating normally.

Clinicians who may be using diagnostic AI as professional users will also be expected to practice better care. Although they might not be the root cause of the underlying algorithmic mistakes, they should be aware of the system constraints, be aware of any of the associated training, and not become blind followers to the non-transparent results. Meanwhile, downstream deployers should have in place systems of feedback, pointing out bad things that are happening, and intercession in case of trends of silent failure.

[10] A&O Shearman, *Legal Liability of AI: Dealing with Minds Immeasurably Superior to Ours*, A&O Shearman Insights, https://www.aoshearman.com/en/insights/future-disputes-risks/legal-liability-of-ai-dealing-with-minds-immeasurably-superior-to-ours

The issue of split responsibility cannot be eliminated by the finest risk-management constructs, however. The data providers, model creators, and application developers tend to work in silos where they only have a partial perspective of the risks. There is haphazard coordination within this chain, and there are little to no binding duties within this chain that mandate upstream developers to share safety tools, supply model cards in detail, or place significant obligations on downstream deployers. The risks when it is seen that everybody is at fault include the fact that no one feels responsible.

The point is that the main obstacle at that is to build a legal and regulatory framework that considers the complexity of AI without letting organizations get away with the pretense of machine autonomy. The legislation must make sure that human controls, corporate controls and regulatory controls should keep up with the technologies that they are meant to control. The essential problem with the assignment of responsibility to AI which works autonomously.

The current state of AI systems presents a certain degree of autonomy that breaks the traditional assumptions of law and responsibility. These technologies are trained on gigantic data sets, they optimize their internal structure and they generate decisions that are not even understandable to their creators. On the one hand, such autonomy allows efficiency, speed, and unprecedented analytical capability, on the other hand, it creates profound uncertainty in the distribution of legal responsibility in the event of something going wrong. Conventional civil and criminal systems assume that there is a human agent with the capability to act intentionally, negligently or carelessly; AI has no such qualities. A machine is incapable of creating mens rea, unable to be punished, and able to make a sensible compensation to a victim. Simultaneously, these systems are the result of a one huge human ecosystem: data collectors, coders, designers, corporate management, compliance teams, end-users, and all of them affect the system at various levels. Such unfair datasets, model design, inadequate supervision, unforeseen model drift, unsafe deployment conditions, or willful adversarial manipulation may cause harm. With all these actors responsible, it becomes extremely hard to tie liability to one point of failure.

Another challenge that courts encounter is that the modern deep-learning systems are opaque. Neural networks do not always give answers on why they arrived at a given decision and the judges and regulators find it hard to use doctrines like foreseeability, duty of care, proximate causation and product defect[11]. This situation is even worse as soon as the system goes into actual use. The AI models do not stop and do not stand still after a sale, they evolve, update themselves, as well as learn new behavioral patterns as time passes. A system can perform well at its initial rollout and be dangerous months after and then one would wonder who would be blamed when the malfunctioning is found out after continuing to learn.

To achieve a liability allocation in this setting, it is necessary to study all the participants of the AI lifecycle. Individuals who create algorithms, the models, and choose the training data, developers and programmers, can be liable to the Indian laws, including the Consumer Protection Act, the IT Act, and the principles of negligence or the failure to warn. They are held accountable in cases of injuries caused by prejudiced contributions, unsafe designing, or inappropriate testing. Their main defense though is the natural variability of machine-learning systems, through this, they can claim that no rational developer could have expected the detrimental result.

Closest to real-world consequences are usually the deployers and users of AI, e.g. hospitals applying AI to diagnostic services, banks applying credit-scoring systems or law-enforcement agencies using facial-recognition systems. They regulate the environment where AI is used, define the degree of human supervision, and have a contractual or a public law duty to approach responsible use. According to Indian law on vicarious liability and administrative responsibility, these actors may be liable in case of the harm, a failure to oversee the behavior of the system, or due to the application of the tool in the wrong context.

The limited responsibility may also be imposed on the end-users, e.g., doctors, HR managers, teachers, or loan officers, especially when those blindly accept the results of AI because they are supposed to exercise their professional judgment. They are less likely to be held responsible though, their liability is usually limited to negligence or abuse; it would be quite unreasonable to expect them to take responsibility for flaws within the system itself.

Arguments supporting or opposing the idea of the legal personhood of AI sometimes appear, using comparisons to corporations or other juristic persons. But this is a conceptually unsound and in India it is impractical. AI systems are not conscious, intentional, possessing assets, and acting morally. Indian law embraces natural and juristic persons only, and even the courts have

[11] Harshita Saharavat, *AI Liability in India* (2025), available at https://theacademic.in/wp-content/uploads/2025/08/169.pdf

traditionally been wary of efforts to give personhood even to non-human symbolic persons. Soon, AI will not be able to be sued or punished directly.

Since the AI ecosystems are complex in nature, it is most realistic to use a combined or hybrid model of liability. In this kind of model, the blame of flaws in the design would be spread over among the developers, the deployers, the users, and the regulators. Aronic safe-harbour might be applied to those actors that adhere to sound risk-management procedures and more severe liability would be placed on high-stakes applications, like policing, healthcare, and financial decision-making.

Hallucination, wherein a system makes an output confident but false, is one of the unique issues of the modern AI, particularly generative models. Hallucinations do not legally make the distinction between reasonable statistical error and defect to action. The model applies the exact processes in both correct and inaccurate responses and it is difficult to classify the error as being a malfunction. In the case of outputs concerned with subjective or uncertain domains, e.g. medical prediction, scientific inference or creative reasoning, then the boundaries between innovation and error are even more difficult to judge. The further AI addresses the issues that are beyond the cognitive abilities of humans, the less chance the users, courts, or regulators will be able to test the rightness of the AI decision, and this introduces an evaluation gap, which makes the question of liability even more problematic.

This sophistication contributes to an increasing compliance cost to organizations. The current AI governance demands that model behavior, performance-drift tracking, data provenance documentation, model outputs validation, and regular audits of third-party systems be continuously monitored. Failure to perform these roles fast emerging as a known kind of organizational negligence. Most of the vendors will seek to protect their interests by disclaiming the use of their own risk clauses in the contract, but this does not hold when AI tools are tailored or made specific towards a particular client. In very networked AI supply chains, where data suppliers, cloud providers, integrators, and corporate consumers are all involved, several actors partially control the situation, and blame-shifting is the order of the day, as well as the identification of one responsible party is hardly possible.

AI LIABILITY AND INDIAN LEGAL FRAMEWORK:

In India, the legal landscape regarding Airbnb is as follows:

Even though rapid AI implementation is observed in India in various industries and fintech and healthcare are among them, the country does not have a special legal framework concerning AI. The existing legislation is developed regarding the human-controllable technologies, and courts or regulatory bodies are now trying to extend these models to the algorithmic behavior, which usually causes ambiguity.

INFORMATION TECHNOLOGY ACT, 2000 [12]

The IT Act continues to be the foundation of Indian digital governance system in matters of cybercrimes, intermediary liability and data protection obligations. It however does not take into consideration harms by autonomous decision-making systems. Although the liability in case of negligent treatment of personal data is stipulated in Sections 43A and 72A, these sections lack coherence with respect to the issue of loss or injury in the case of an algorithmic act or machine-generated result. The Act assumes human supervision, which is becoming less consistent with modern AI systems.

CONSUMER PROTECTION ACT, 2019 [13]

The Consumer Protection Act acts as a protection to people against faulty services and unjust business. Hypothetically, automated platforms or AI-based services can be included in its scope. However, the law does not provide any directions in cases of algorithm-based bias or faulty automated decisions[14], which are especially important to the e-commerce recommendation setting, automated lending or telemedicine. In the cases when the ill act is the result of the opaque nature of a self-learning model, it is difficult to distribute responsibility based on the consumer law framework.

INDIAN CONTRACT ACT, 1872 [15]

Naturally, transactions with the use of AI are becoming more based on algorithmic tools, smart contracts, or automated negotiations. Nonetheless, the Contract Act assumes that the use of human intent is present, free will and legal competence, which AI systems cannot have as their inherent nature. There are questions that cannot be answered, such as Can an AI agent sign a binding

[12] Information Technology Act, 2000, No. 21 of 2000 (India).

[13] Consumer Protection Act, 2019, No. 35 of 2019 (India).

[14] SMS Law College, *Laws for AI: Who Is Liable When a Machine Makes a Mistake?*, SMS Law College Blog, https://blog.smslawcollege.com/laws-for-ai-who-is-liable-when-a-machine-makes-a-mistake/

[15] Indian Contract Act, 1872, No. 9 of 1872 (India).

contract? Who is liable when there is an error in a contract that has been written or signed by an autonomous system? Currently, the law of India does not offer explicit solutions.

PROBLEMS WITH APPLICATION OF EXISTING LAWS TO AI:

ABSENCE OF LEGAL PERSONHOOD:

According to the Indian law, a liable entity must be a natural or a juristic person. In a case where no identifiable direct human wrongdoer can be discovered, AI systems can neither be sued nor punished.

CHALLENGES IN TRACING FAULT:

The autonomous systems will be able to learn new information or adjust on the field after implementation, so it will be challenging to determine who between a developer, deployer, user or data provider may have caused the harm.

OPAQUE DECISION-MAKING:

Most developed AI models are not explainable. The legal principles based on foreseeability, accountability or reasonable justification are challenging to execute when the inner logic of the system is not available.

NONE OF THE MECHANISMS OF RISK CLASSIFICATION:

India is yet to categorize AI systems and classify them according to risk as the EU does. The lack complicates the targeted regulation or the responsibility allocation.

REGULATORY FRAGMENTATION:

Various sectoral regulators control the use of AI, but none of them has a single standard in terms of accountability, leaving developers and consumers uncertain.

COMPARATIVE APPROACHES TO AI LIABILITY:

To see how India can devise its own model of addressing AI-related harm, it can be helpful to look at how other major jurisdictions combat it[16].

EU ARTIFICIAL INTELLIGENCE ACT [17]

Introduced in 2024, AI Act is the first general regulatory framework on artificial intelligence in the world[18]. It sorts the AI systems into four groups including unacceptable, high-risk, limited-risk

[16] Tae Wan Kim, *Accountability for Autonomous Systems: Ethical and Legal Challenges*, *AI & Society* (2023), https://link.springer.com/article/10.1007/s00146-023-01640-1.

[17] Regulation (EU) 2024/XXX of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act).

[18] Ginger Stober et al., *AI Liability and Governance: Emerging Risks and Legal Responses*, 18 *Journal of Law, Innovation & Technology* (2025), https://www.tandfonline.com/doi/full/10.1080/17579961.2025.2469345.

and minimal-risk. Systems that are considered high-risk (typically medical diagnostics, employment screening, law enforcement tools, etc.) should be of high-quality regarding transparency, data management, human control, and constant monitoring. Even though the Act does not per se establish liability, it influences circumstances under which developers and deployers can be subjected to responsibility under other legislations.

GDPR is a collection of rules and guidelines that guarantee the protection of the personal data of all individuals involved in the study.

GENERAL DATA PROTECTION REGULATION (GDPR)

The automated decision-making is explicitly regulated by GDPR. Article 22 provides people with the right not to be guided by algorithms only but ask humans to revise the decisions. This offers valuable procedural security on the opaque or unjust AI-driven results.[19]

PRODUCT LIABILITY DIRECTIVE (2024 REVISION) [20]

Europe has changed its strict liability regime to cover AI systems including software-as-a-service. The victims of the AI-induced harm will no longer be required to demonstrate negligence; there will be strict liability against developers and providers of systems that will cause harm, which will be necessary due to the obfuscatory nature of machine learning models.

UNITED STATES: TORT-DRIVEN AND SECTOR-SPECIFIC.

The US is based on tort and disorganized sectoral regulations, as opposed to the integrated system of the whole of Europe.

TORT AND PRODUCT LIABILITY

The AI disputes are subjected to traditional negligence and product liability doctrines by courts. The plaintiff must prove duty, breach and causation, which is not always easy in the case of AI systems developing or acting unpredictably. Cases of self-driving cars, computerized credit rating or medical AI point out these challenges.

SECTORAL OVERSIGHT

Examples of regulators include the FDA (healthcare AI), FTC (algorithmic fairness) and NHTSA (autonomous vehicles), although there exists no federal AI liability law. The Blueprint of AI Bill of Rights defines the ethical principles but does not establish any binding.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).

[20] Directive (EU) 2024/XXX of the European Parliament and of the Council on Liability for Defective Products (Recast).

POLICY ROADMAP OF AI LIABILITY REGIME IN INDIA:

India needs a proactive, right-focused, and technology-sensitive[21] law due to the high pace of AI technologies spread throughout the Indian industries and the uncertainty related to the questions of accountability of the technologies used to conduct automatic decisions. The initial priority would be the adoption of specific AI laws. An all-encompassing law must specifically define the AI systems, categorize them based on the risk and has the liability that will be based on the factors of control, intent and reasonable foreseeability. Such laws must also comply with the current laws such as the IT Act, Consumer Protection Act and the IPC in addition to enhancing constitutional principles of equality, privacy and due process. The existence of distinct responsibilities of developers, deployers and end-users would serve to address the existing gaps created by ad hoc interpretations of older statutes.

Another way that India would gain is by establishing a specialized regulatory body to govern AI in the same way that the EU has its AI Office or individual regulators like the SEBI and TRAI in the country. Such an agency is tasked with the responsibility of policymaking, norm setting, certifying AI systems, overseeing compliance, investigating harm, and collaborating with regulators in sector-specific regulators, which include healthcare, finance, transportation, and law enforcement. Such an authority needs to be empowered with the law, technologically informed, ethically based and institutionally independent to be effective002E

Another reform that is necessary is the mandatory audits of high-risk AI systems. Independent audits of algorithmic principles conducted by an independent auditing body should be imposed on technologies in areas like diagnostic healthcare, predictive policing, credit scoring, staffing and other critical services provided to the population, which can detect bias, discrimination or error. They should also be subjected to regular impact assessments whereby the impact on privacy issues, implications on fairness, and accuracy of the system have to be assessed and statutory penalties imposed should they not do so. The audits would assist in creating transparency in the operation of AI systems and making sure that the decisions they make are also accountable.

Together with auditing, India ought to establish happenable AI liability insurance like the present day professional indemnity schemes among doctors or lawyers. This insurance would guarantee that damages due to algorithmic mistakes, biased forecasts or unforeseen failures end in

[21] Kirsten Martin, *Artificial Intelligence and Liability*, 61 *Computer Law & Security Review* 105726 (2023), https://www.sciencedirect.com/science/article/pii/S0267364923000055.

compensations to the people who have fallen victims. It would also help companies invest in solid safety practices, documentation and explainability since risk-reduction practices are usually requested by insurers. This system would minimize litigation costs and maintain transparency on the issue of financial accountability.

Regulatory or legal frameworks that handle AI should also be founded on the key pillars that include transparency, accountability, and fairness. It should be constructed in such a way that it generates explanations in ways comprehensible to the people it relates to; the accountability of each phase of the AI systems lifecycle should be assigned to identifiable individuals in the system; and barriers must be in place to ensure that the processes in an algorithm do not reinforce social disparity, caste prejudice, or economic disadvantage. These values may be impressed into the law, purchasing standards, industry regulations, and industry standards.

Finally, AI liability regime in India should be strata-based, interwoven, and made in line with constitutional promises. In the absence of a clear system of accountability determination, AI systems can destroy legal certainty, access to justice and trust. The reforms will help establish a moderate structure that will allow technological advancement but will also hold anyone seriously liable to injury.

CONCLUSION:

Since artificial intelligence will gradually assume the functions of decision making that were previously performed solely by human judgement, the issue of legal responsibility will emerge as one of the most pressing problems of modern governance. Current AI systems are more independent than they have ever been, learning, adapting, and producing results that even its developers themselves might be unable to comprehend. This technological change reveals the profound fractures in the classical theories of liabilities, and all of them were created on the premise of the existence of a human agent with the capacity to knowingly, carelessly, or predictably act. According to the principle of harm, once AI systems make decisions that harm, it shatters the core of the present civil, criminal, and regulatory systems.

As is shown in this study, there is no one actor that would realistically be accountable to the outcomes of AI. Rather, it is shared throughout a highly networked system of developers of algorithms and training data; deployers and operators who apply AI to the real world; end-users who consume automated outputs; and regulators who either establish or do not establish sufficient standards of oversight. Meanwhile, the fact that AI systems cannot legally and philosophically be considered independent entities that have rights or responsibilities makes it difficult to significantly alter the situation. Therefore, the machine itself should not be blamed of the blame regardless of its autonomous or unpredictable behaviors.

Finally, an effective AI liability framework should appreciate the fact that accountability is not lost in autonomy. The fact that artificial intelligence can learn, evolving, and making opaque errors further increases the demand of strict, obvious, responsibility frameworks. The most balanced way to go is a multi-layered and hybrid model of liability, backed up by transparency requirements, strong oversight responsibilities, and process-oriented risk management. This type of framework provides that the innovation will keep going on but not at the cost of justice, safety, or social confidence.

Legally speaking, as India is going through the potentially transformative power of AI, its legal framework must become equally sophisticated. Devoid of intentional reform, AI systems might exist within a vacuum of liability, where victims have no one to turn to and that AI governance will become ineffective and stir no confidence. Thoughtful and future-oriented regulation can enable responsible utilization of AI, however, that promises technological advancement without losing the key principles of accountability and the rule of law.