THE INVISIBLE DEFENDANT: WHO IS RESPONSIBLE WHEN ARTIFICIAL INTELLIGENCE CAUSES HARM IN INDIA?

Ayush Kumar Upadhyay, LLM, Tata Institute of Social Sciences, Hyderabad

When a machine makes a mistake, the courtroom falls silent - not from shock, but from uncertainty. India's legal framework, built entirely around human accountability, has no answer for the age of artificial intelligence.

Artificial intelligence (AI) is no longer a fictional concept. Nowadays, AI is diagnosing our diseases, giving or denying us loans, and driving self-driving cars on the streets. But what would the issue be if an AI system injured someone? To whom is the law legally accountable? In India, the truthful response is that we don't know. The laws we have today were designed in a world in which a human being made all significant decisions. They are not designed to handle a self-operating machine. This article examines the inadequacy of existing legal instruments in India and the actions of other nations. It offers a concise, viable, easy-out, and a new statute that will, at last, determine who pays when AI goes bad.

Take three actual Indian incidents. In 2024, an AI system produced a deepfake video, a digitally manipulated video that was totally convincing and realistic, of a well-known Indian journalist promoting fake medicines. The Delhi High Court was forced to intervene and make the government act. The same year, an AI bot was employed to duplicate a renowned Bollywood singer without his consent. The Bombay High Court halted it. And the first in India, a major news agency, in its initial litigation against an AI company, alleged that the company had used the agency's published articles to train its AI without permission.

In both instances, AI injured a real person. And in both instances, the Indian courts were wrestling with a fundamental question: who are we to blame?

This is not a far-off or minor issue. By 2027, the AI market in India will reach USD 17 billion. Hospitals, banks, courts, and government offices use AI. Human beings are influenced by AI daily, often without realizing it. Now, however, when an AI system harms you, the Indian law

does not give a clear answer on who is liable to pay damages. This article addresses that gap.

Here are the reasons our pre-AI law tools are unsuitable.

The way to see the problem is first to examine how Indian law would allocate responsibility when a person is injured.

Negligence is the most used legal instrument. Under this rule, as in the well-known English case of *Donoghue v Stevenson of 1932*, if you are careless and your carelessness causes injury to someone, you must compensate for the injury. To demonstrate negligence, you must demonstrate the following: (1) the person owed a duty of care, (2) the person did not exercise the care, (3) the person's negligence led to the damage, and (4) you were injured.

Considering this as applied to AI now. Who was "careless"? The two-year-old software engineer, who wrote the code? The company where the AI was admitted to a hospital? This physician who trusted the AI? If an AI system makes a faulty diagnosis, there is hardly any way to tell an individual it is their fault. The AI decided for itself and tended to act in ways its developers do not even fully understand. This has been referred to as the black-box problem: the decision-making process of AI is unclear, even to professionals.

There is also a more potent tool, namely absolute liability, which India has, which was developed by the Supreme Court in the landmark case of *MC Mehta* in 1987. Under this rule, which was better than the older rule in *Rylands v Fletcher*, if a company creates a dangerous situation and something goes wrong, it should compensate, even if it was not careless. No excuses. This is promising news regarding AI. However, this rule was intended to apply to physical disasters (such as gas leaks or factory explosions). Courts have not yet applied it to an AI that provides bad medical advice or unjustly refuses a loan.

Next is the Consumer Protection Act 2019, under which consumers can sue for a faulty product or substandard service. A machine that hurts you will, in theory, be called a malfunctioning service. But the law requires you to indicate a specific defect. When a machine-based loan system learns to be biased against women or rural residents unobtrusively, not due to a coding error, but as perceiving the trends of the historical data it was trained on, what constitutes the defect? There is no good answer to the law.

Lastly, the new criminal code, Bhartiya Nyaya Sanhita 2023, in India still requires proof of a

guilty mind (mens rea) to convict a person of a crime involving harm. There is no mind in an AI machine, no intention in an AI machine, no guilt. The responsibility for the crime is always placed on a human being, but our law provides no specifications on what kind of human being should be held responsible.

Why do we already have the Laws, and why aren't they enough?

Three basic laws in India occasionally apply in AI-related conflicts: the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, and the Consumer Protection Act 2019. None of them were developed using AI, and none adequately addresses the gap.

The IT Act was codified in response to hacks and data theft, not to address a situation in which an AI makes a bad decision on its own, one that negatively affects you. The Data Protection Act protects your personal data. It provides you with the right to demand that it be deleted, but nothing if an AI system destroys your life by refusing you a job or even a medical procedure. The nearest match is the Consumer Protection Act; however, as explained above, it cannot cover the peculiarities of AI system failures.

Our Constitution provides an element of hope. The historic Puttaswamy ruling of 2017 by the Supreme Court determined that the right to privacy is essential. This has been cited to object to AI-led monitoring and deepfakes. The constitutional remedies, including appeals to the High Court or the Supreme Court, are costly and time-consuming and do not serve the purpose of putting money into the hands of ordinary people who have suffered.

The government has not taken a back seat. In November 2025, the government released the India AI Governance Guidelines, and NITI Aayog released a National AI Strategy in 2018, making AI companies responsible and ethical. This is the kind of sign. However, they are not compulsory; no one has a legal obligation to observe them, and any breach of them does not attract a legal penalty. Any victim of AI will not be able to appear in court and tell, "The corporation violated the rules, pay me. Willing regulations are not sufficient.

What to Learn?

The most extensive AI legislation ever in the world is the EU AI Act 2024. Its main concept is straightforward and logical: the more dangerous the AI system is, the stricter the rules are. It

categorizes AI systems into four types:

(1) Banned AI: AI that is an unacceptable threat to the rights of people: AI that manipulates your behavior by not disclosing it to you. These are completely prohibited.

(2) High-Risk AI: AI applications in healthcare services, employment, credit ratings, law enforcement, and related fields. Before deployment, these should meet stringent safety and transparency standards.

(3) Limited-Risk AI: e.g., chatbots, which, at any rate, should inform you that you are interacting with the machine.

(4) Minimal Risk AI: AI tools used daily can be subjected to simple demands. At the same time, the EU is drafting an AI Liability Directive to simplify compensation for victims. Normally, in court, the victim must prove exactly how the AI caused the harm, which is almost impossible with a black-box system. The Directive reverses this by stating that, should the AI firm violate the regulations, the court will presume that the AI is the cause of the harm and that the firm must demonstrate to the contrary.

In the United States, there has been a more unstructured process, with various regulations across sectors and the judiciary making up the remainder. Criminal cases such as Lee v Tesla have attempted to extend extant product liability laws to apply to self-driving vehicles, with varying degrees of success. This piecemeal method confuses and leaves numerous victims unredressed.

In January 2026, the Indian government think tank, the Office of the Principal Scientific Adviser, published a white paper proposing a techno-legal strategy that involves the direct development of legal safeguards into AI platforms. It is an up-and-coming concept that India should start implementing quickly.

What India Must Do! An Easy, Equitable Compromise.

Going by all this, this is what India requires: a new law, a clear, fair, easy-to-use law for the ordinary people. The legislation ought to operate in 4 simple steps.

Step 1: AI/risk level - Like the EU, India ought to categories AI systems based on their

perceived threat. Artificial intelligence in hospitals, banks, courts, and self-driving cars poses a significant threat. Recommendations and other simple customer services delivered by AI are less risky. There are varying levels and rules for different risks.

Step 2: AI high-risk responsibility is made automatic. In the case of dangerous, at-risk AI systems, the company that developed it and the company that implements it should automatically pay damages (if the AI causes harm) without the victim having to prove they were careless. This is akin to the doctrine of absolute liability. If an AI medical system provides you with the wrong diagnosis and you get hurt, the hospital and the software developer pay up, full and simple.

Step 3: Collective responsibility up and down the chain. One cannot make AI alone. The design company, the utility company, and, in many cases, even the individual who used it all contribute. Determinations of who is liable and to what extent should be defined by the law: designers compensate for faulty or unfair systems; deploying companies compensate for using the AI irresponsibly; common users compensate simply by being intentional and careless users of the AI.

Step 4: Forced safety (checks). Companies should undergo a formal review of the likelihood of risks and the means to mitigate them before deploying any high-risk AI, which is required to be an AI Impact Assessment. This not only compels the harm to be minimized in the first place but also creates a paper trail that victims can use in court if something goes awry.

Political momentum towards this already exists. The Artificial Intelligence (Ethics and Accountability) Bill 2025 was proposed in Parliament in December 2025 as a private member's bill. It suggests the creation of a national AI ethics committee, which will be mandatory for conducting bias audits, and other penalties will range between Rs. 5 crore and Rs. It has been pending in Parliament, but at least it demonstrates Parliament's willingness to act. The government ought to incorporate these concepts and the liability regime suggested here into the next Digital India Act.

The Victim Cannot Wait.

The responsibility question regarding the harm caused by AI is not a philosophical issue. This is a practical question that is real and is being faced by real people - the patient whose cancer

was not detected due to the false flag of AI in a hospital. The young graduate was denied all jobs since a job-seeking algorithm was discriminatory towards individuals in her district. A machine that does not understand how it was planned wrongly declined the family a home loan. These individuals should be answered and compensated.

The current laws of India were developed in a world where human beings made all the critical decisions. The world is becoming fast-changing. The bright side is the fact that we do not need to begin with a blank sheet: the principle of absolute liability as developed by the Supreme Court, the pro-victim orientation of the Consumer Protection Act, and the provision of the basic rights by the Constitution all have a wonderful basis upon which we can create something.

The last ingredient is missing: a clear, contemporary law on who will pay when AI malfunctions. The EU has already constructed it. India possesses the instrumentation, the jurisprudential culture and the necessity. It is now only a matter of having the political goodwill to do it and to do it before a larger number of people are subjected to the machinery that no longer reports to anyone.