# AI MAY SPEAK, BUT HUMANS MUST ANSWER: REAFFIRMING HUMAN RESPONSIBILITY IN THE AGE OF ALGORITHMIC GOVERNANCE

S.K. Deshmukh, Student of Law, Maharashtra National Law University, Nagpur

## ABSTRACT

The rapid integration of Artificial Intelligence (AI) into advisory and decision-making processes across sectors such as law, banking, healthcare, and governance has generated complex legal questions concerning liability for unlawful or erroneous advice. This article argues that Indian law must resist the temptation to anthropomorphise AI and instead reaffirm a human-centred architecture of liability grounded in control, foreseeability, and constitutional accountability. Drawing upon doctrines of vicarious liability, consumer protection, constitutional law, and criminal jurisprudence, the article demonstrates that responsibility must rest with the natural or juristic persons who design, deploy, and rely upon AI systems. Judicial precedents such as Indian Medical Association v. V.P. Shantha, State of Rajasthan v. Vidyawati, Justice K.S. Puttaswamy v. Union of India, and Anuradha Bhasin v. Union of India reveal a consistent judicial commitment to accountability over technological delegation. Rejecting criminal liability for AI due to the absence of mens rea and statutory recognition, the article proposes a structured model of distributed and enterprise liability capable of preserving deterrence, compensatory justice, and democratic oversight. It concludes that while AI may "speak" through automated advice, the normative architecture of Indian law mandates that humans must ultimately answer for its consequences.

***Key Words:*** *- AI Liability, Human-Centric Accountability, Indian Jurisprudence, Automated Decision-Making, Enterprise Responsibility.*

## INTRODUCTION

Artificial Intelligence increasingly participates in decisions affecting legal rights, financial stability, medical treatment, and access to public welfare. Algorithmic tools recommend legal strategies, assess creditworthiness, and assist administrative governance. As institutional reliance deepens, a foundational question emerges: who bears responsibility when AI provides unlawful advice?

This article advances the claim that Indian law should reject artificial personhood for AI and instead develop a framework of distributed responsibility. Liability presupposes intention, negligence, or the capacity to understand legal norms, attributes absent in algorithmic systems. Treating AI as a juridical actor would therefore diffuse accountability.

Indian courts have historically resisted attempts by institutions to evade liability through delegation. Whether harm arises from employees, administrative machinery, or technological tools, the law looks beyond the instrument to the controlling authority. AI must be treated similarly: as a sophisticated tool rather than a bearer of legal responsibility.

## THE JURISPRUDENTIAL ERROR OF ARTIFICIAL PERSONHOOD

Some scholars advocate granting limited legal personality to advanced AI. While administratively attractive, this approach confuses instrumental autonomy with moral agency.

Legal personhood has historically been extended only when it advances normative goals. Corporations were recognised as juristic persons to facilitate economic organisation while preserving human accountability behind the corporate veil.[1]Extending similar status to AI risks creating liability shields rather than responsibility structures.

Punishment presupposes blameworthiness. AI lacks consciousness, cannot internalise sanctions, and is incapable of moral judgment. Sanctioning an algorithm would therefore fail both retributive and deterrent purposes.

[1]*Salomon v. Salomon & Co. Ltd.*, [1897] AC 22 (HL).

More concerningly, artificial personhood may enable corporations and public authorities to externalise risk by attributing harm to computational error. Indian constitutional culture, deeply anchored in accountability, should resist such diffusion.

The coherent approach is not artificial personhood but enhanced human responsibility for automated power.

## ALGORITHMIC POWER AND THE RULE OF LAW

AI represents a structural shift in how power is exercised. Decisions once made by identifiable officials increasingly emerge from opaque computational processes. This raises a rule-of-law concern: can authority remain legitimate when reasoning becomes unintelligible?

The Supreme Court has equated arbitrariness with inequality.[2] Algorithmic opacity risks producing such arbitrariness by preventing affected individuals from understanding decision-making bases.

Scholars warn against the emergence of a "black box society," wherein automated systems evade scrutiny.[3] European frameworks have responded by recognising protections against purely automated decision-making.[4] Indian constitutionalism, with its commitment to reasoned state action, is unlikely to tolerate governance by inscrutable machines.Opacity is therefore not merely technical, it is constitutional.

## VICARIOUS LIABILITY AND TORTIOUS RESPONSIBILITY

Indian tort law provides a persuasive analogy through vicarious liability, under which employers are responsible for wrongful acts committed during employment.[5] The justification lies in control, benefit, and risk allocation.

If a bank deploys an AI system that misrepresents lending eligibility, the algorithm functions as an operational extension of the institution. Allowing the bank to attribute fault to software would undermine consumer protection.In Indian Medical Association v. V.P. Shantha, the Supreme

[2]*E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.
[3]Frank Pasquale, The Black Box Society (Harvard University Press, 2015).
[4]General Data Protection Regulation, art. 22, Regulation (EU) 2016/679.
[5]*PushpabaiPurshottamUdeshi v. Ranjit Ginning & Pressing Co*., (1977) 2 SCC 745.

Court recognised liability for deficiencies in service.[6] An AI advisory platform dispensing incorrect legal or medical guidance falls squarely within this doctrine.The AI cannot be sued; the provider must answer.

Traditional vicarious liability may be insufficient for AI harms given complex production chains involving developers, deployers, and data suppliers. A more suitable evolution lies in enterprise liability, which allocates risk to the entity best positioned to prevent harm and absorb loss.

Indian courts have embraced analogous reasoning. In M.C. Mehta v. Union of India, the Supreme Court articulated absolute liability for hazardous enterprises.[7] While AI is not industrially hazardous, its capacity to scale harm instantaneously justifies similar logic.

When technology multiplies risk, the law must intensify responsibility. This represents doctrinal continuity rather than innovation.

## STATE LIABILITY AND CONSTITUTIONAL ACCOUNTABILITY

Courts have refused to allow the State to disclaim responsibility for harms caused by internal mechanisms. In State of Rajasthan v. Vidyawati, the government was held liable for employee negligence.[8]

If a government deploys an AI-based system that unlawfully denies welfare benefits, it cannot argue that "the machine made the mistake." Administrative discretion cannot be outsourced without retaining responsibility.Algorithmic governance must remain constitutionally disciplined.The constitutional implications of AI are particularly significant when automated systems affect fundamental rights.

In Justice K.S. Puttaswamy v. Union of India, privacy was recognised as intrinsic to Article 21, accompanied by warnings against unaccountable data-driven governance.[9]Similarly, Anuradha Bhasin v. Union of India reaffirmed that restrictions on liberty must satisfy legality, necessity,

[6]*Indian Medical Association v. V.P. Shantha*, (1995) 6 SCC 651.
[7]*M.C. Mehta v. Union of India*, (1987) 1 SCC 395.
[8]*State of Rajasthan v. Vidyawati*, AIR 1962 SC 933.
[9]*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

and proportionality.[10]Automated decisions lacking transparency struggle to meet these requirements.

Article 14 prohibits arbitrariness. In E.P. Royappa v. State of Tamil Nadu, arbitrariness was equated with inequality.[11] Algorithmic bias may therefore become constitutionally suspect.Technology cannot dilute fundamental rights.

India lacks a comprehensive statute governing AI liability. The Information Technology Act, 2000 was designed for electronic commerce rather than autonomous decision-making.Section 79 grants intermediaries conditional safe harbour, but negligent deployment of AI cannot hide behind intermediary protection.[12]

Globally, regulators are converging on proactive governance. The European Union's Artificial Intelligence Act adopts a risk-tiered model imposing strict obligations on high-risk systems.[13]Comparative experience reveals a critical lesson: legal systems that delay regulatory clarity risk adjudicating technological crises rather than preventing them.

## DUTY OF CARE IN ALGORITHMIC ECOSYSTEMS

Negligence law hinges upon foreseeability and reasonableness. Organisations adopting AI capable of influencing legal entitlements or medical outcomes face heightened foreseeability of harm.The neighbour principle in Donoghue v. Stevenson established that manufacturers owe duties to ultimate consumers.[14] Developers of AI resemble modern manufacturers of algorithmic advice; defective models or biased datasets should attract liability.

The Consumer Protection Act, 2019 reinforces this through statutory product liability.[15] Failure to warn users about system limitations may constitute negligence.Complexity is not a defence.

[10]*Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[11]*E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.
[12]Information Technology Act, 2000, s. 79.
[13]European Commission, Proposal for an Artificial Intelligence Act, COM/2021/206 final (2021).
[14]*Donoghue v. Stevenson*, [1932] AC 562 (HL).
[15]Consumer Protection Act, 2019, ss. 82–87.

Professionals integrating AI must exercise independent judgment. In Jacob Mathew v. State of Punjab, negligence was defined as conduct falling below expected professional standards.[16] A doctor blindly following AI diagnosis risks breaching this standard.

Lawyers and financial advisors remain similarly bound by duties of competence.AI must assist not replace human reasoning. Delegation has never absolved responsibility in law.

## THE IMPOSSIBILITY OF CRIMINAL LIABILITY

Criminal law presupposes mens rea. AI lacks intention, consciousness, and moral blameworthiness. Indian statutes addressing corporate offences impose liability on persons in charge rather than abstract entities.[17]There exists no conceptual foundation to prosecute an algorithm. Responsibility must trace back to humans.

Given the layered architecture of AI ecosystems, liability should be distributed across the technological chain:

| | |
|---|---|
| Developers negligent design or biased training data | Negligent design or biased training data |
| Deployers | Oversight failures |
| Data controllers | Dataset integrity |
| Professionals | Uncritical reliance |

Such a framework prevents diffusion of accountability while fostering public trust.Innovation requires responsibility, not deregulation.The AI liability debate ultimately concerns constitutional morality. Technologies deployed by the State must remain subordinate to dignity, liberty, and equality.

Unchecked automation risks normalising bureaucratic distancing, where responsibility dissolves into systems architecture. Constitutional democracy demands identifiable decision-makers where power exists, accountability must follow.

[16]*Jacob Mathew v. State of Punjab*, (2005) 6 SCC 1.
[17]Negotiable Instruments Act, 1881, s. 141.

## CONCLUSION

Artificial Intelligence is transforming governance, commerce, and professional practice, yet its integration must not destabilise foundational legal principles. The temptation to attribute liability directly to AI reflects regulatory anxiety, but jurisprudential shortcuts rarely produce durable solutions.Indian law should reject artificial personhood and refine doctrines capable of preserving accountability within technologically mediated environments. A structured model of distributed and enterprise liability offers the most coherent path forward.

The future of law is not a contest between humans and machines; it is a test of whether legal systems can adapt without surrendering their normative core.AI may optimise decisions but legitimacy requires responsibility and responsibility, in law, remains irreducibly human.