RETHINKING AI LIABILITY IN INDIA: EVALUATING THE INFORMATION TECHNOLOGY ACT IN THE AGE OF AUTONOMOUS SYSTEMS

Ishita Rai, LL.B., Department of Law, New Delhi, Bharati Vidyapeeth (Deemed to be University)

ABSTRACT

The rapid integration of Artificial Intelligence (AI) into sectors such as healthcare, finance, governance, and digital commerce has transformed decision-making while simultaneously raising complex questions of legal responsibility. Existing liability frameworks under Indian law were developed with human actors in mind and are increasingly challenged by autonomous AI systems capable of making decisions with limited human intervention. This paper examines whether the Information Technology Act, 2000 adequately regulates civil and criminal liability arising from AI-related harms. Using a doctrinal research methodology, the study analyses relevant provisions of the Information Technology Act alongside judicial precedents, and allied legislation. It argues that while the Act addresses certain technology-enabled offences and intermediary responsibilities, it does not sufficiently resolve questions of liability where autonomous AI systems cause harm. The paper concludes by recommending targeted legislative reforms and a risk-based regulatory framework to ensure legal certainty, accountability, and responsible innovation in India's evolving AI ecosystem.

1. Introduction

Artificial Intelligence (AI) has rapidly evolved from a specialised branch of computer science into a transformative technology that influences almost every aspect of modern society. In India, AI-powered systems are increasingly deployed in healthcare, banking, e-commerce, education, law enforcement, and public administration to improve efficiency, automate decision-making, and enhance service delivery. Government initiatives such as the National Strategy for Artificial Intelligence and the IndiaAI Mission further reflect India's commitment to fostering innovation while positioning itself as a global leader in AI-driven development. As AI systems become more autonomous and capable of generating outputs with minimal human intervention, they also present unprecedented legal challenges concerning accountability and liability.

Traditional legal frameworks are primarily designed to regulate the actions of identifiable human actors. However, autonomous AI systems can independently analyse data, learn from experience, and make decisions that may result in financial loss, privacy violations, discriminatory outcomes, or even physical harm. In such situations, determining responsibility becomes increasingly complex. Questions arise as to whether liability should rest with the developer, the deployer, the user, or another stakeholder. These challenges expose the limitations of existing legal principles, particularly when legislation predates the emergence of advanced AI technologies.

The Information Technology Act, 2000, remains India's principal legislation governing cyber activities, electronic records, digital transactions, and certain cyber offences. Although several of its provisions address technology-related misconduct and intermediary obligations, the Act was enacted long before the widespread adoption of autonomous AI systems. Consequently, it does not expressly address liability arising from AI-generated decisions or autonomous conduct. This legislative gap raises important concerns regarding the adequacy of India's existing cyber law framework in addressing emerging AI-related harms.

This paper examines whether the Information Technology Act, 2000 provides an adequate legal framework for determining civil and criminal liability arising from autonomous AI systems. Employing a doctrinal research methodology, it analyses relevant statutory provisions, judicial precedents, and policy documents. The paper argues that while the Act continues to offer a foundational framework for regulating digital activities, it is insufficient to resolve the unique

legal challenges posed by autonomous AI. It concludes by advocating targeted legislative reforms and a coherent regulatory approach that balances technological innovation with legal accountability.

2. Understanding Artificial Intelligence and the Problem of Legal Liability

Artificial Intelligence (AI) refers to computer systems capable of performing tasks that ordinarily require human intelligence, including learning from data, recognising patterns, making predictions, and generating decisions. Unlike conventional software that operates according to predetermined instructions, AI systems employ algorithms that can adapt their outputs based on new information and experience. Machine learning and deep learning models, in particular, enable AI to improve its performance over time without explicit reprogramming, making its decision-making process increasingly complex and less predictable.

A distinction must be drawn between ordinary software and autonomous AI systems. Traditional software executes fixed commands designed by programmers and produces consistent outputs when provided with identical inputs. Autonomous AI, on the other hand, possesses the capacity to analyse dynamic data, learn continuously, and make decisions with limited or no real-time human intervention. While ordinary software functions as a passive tool under direct human control, autonomous AI demonstrates varying degrees of independence in carrying out assigned tasks. This distinction is significant because existing legal frameworks generally attribute liability to identifiable human actions rather than to systems capable of making autonomous decisions.

The legal implications of AI-generated harm can broadly be classified into civil and criminal liability. Civil liability arises where the deployment or operation of AI causes injury, financial loss, property damage, or violations of legal rights, giving rise to claims for compensation. For example, an autonomous vehicle involved in a traffic collision or a medical diagnostic AI that incorrectly recommends treatment may cause significant harm to individuals. In such situations, courts must determine whether responsibility lies with the developer, manufacturer, service provider, owner, or end user. Criminal liability, by contrast, concerns conduct that constitutes an offence punishable by law, requiring proof of elements such as intention, knowledge, or recklessness. AI-generated financial fraud, automated phishing attacks, or deepfake technology used for identity theft and extortion illustrate situations where criminal consequences may arise. However, AI itself cannot presently possess the mental state required

for criminal culpability under Indian law.

The central challenge is one of legal attribution. Existing liability principles are premised on the assumption that harmful acts originate from identifiable human actors exercising conscious control. Autonomous AI complicates this assumption because its decisions may emerge from complex computational processes that neither developers nor users can fully anticipate or explain. Similarly, algorithmic trading systems may independently execute transactions that disrupt financial markets without direct human instruction at the time of execution. As AI systems continue to acquire greater autonomy, determining responsibility for their actions becomes increasingly difficult, exposing significant gaps in traditional legal doctrines and highlighting the need for a more nuanced framework of accountability.

3. Existing Indian Legal Framework: Does the Information Technology Act, 2000 Regulate AI Liability?

The Information Technology Act, 2000 ("IT Act") is India's primary legislation governing electronic transactions, cyber offences, and intermediary liability. Enacted to facilitate electronic commerce and provide legal recognition to electronic records, the Act was drafted at a time when artificial intelligence was largely confined to academic research rather than commercial deployment. Consequently, although the Act establishes a comprehensive framework for regulating digital activities, it does not expressly contemplate autonomous AI systems or allocate liability for harms caused by algorithmic decision-making.

A. Civil Liability under Section 43

Section 43 of the IT Act provides for compensation where a person, without authorisation, accesses a computer system, downloads data, introduces computer contaminants or viruses, disrupts computer networks, or causes damage to digital resources. The provision primarily addresses unauthorised human conduct resulting in economic loss and serves as a civil remedy for victims of cyber-related damage.

While Section 43 may apply where an individual intentionally deploys an AI system to compromise a computer network, its application becomes uncertain when harm results from autonomous AI behaviour that was neither intended nor reasonably foreseeable. For instance, an AI-powered cybersecurity application that independently deletes critical organisational data

after misclassifying legitimate files as malicious would cause measurable economic harm. Yet the Act offers no guidance on whether liability should attach to the software developer, the organisation deploying the AI, the system operator, or another stakeholder. The provision therefore presumes direct human agency and provides little assistance in resolving disputes arising from autonomous decision-making.

B. Criminal Liability under Chapter XI

Chapter XI of the IT Act criminalises several forms of cyber misconduct, including dishonest or fraudulent access to computer resources (Section 66), identity theft (Section 66C), and cheating by personation using computer resources (Section 66D). These offences require proof of culpable human conduct, such as dishonest intention, fraudulent intent, or knowledge.

This requirement presents a significant challenge in the context of autonomous AI. Suppose a generative AI system creates convincing phishing emails or deepfake videos that facilitate financial fraud without the specific intent of its developer or user. Although the resulting harm may fall within the scope of existing cyber offences, attributing the requisite *mens rea* to any particular individual becomes legally difficult. Indian criminal law does not recognise AI systems as legal persons capable of forming criminal intent, leaving courts to rely on indirect theories of liability that may not adequately reflect the technology's autonomous capabilities.

C. Intermediary Liability under Section 79

Section 79 grants qualified immunity, or "safe harbour", to intermediaries for third-party content, provided they observe statutory due diligence and comply with lawful governmental or judicial directions. In *Shreya Singhal v. Union of India*, the Supreme Court clarified that intermediaries lose this protection only upon receiving actual knowledge through a court order or a notification issued by the appropriate government. This decision sought to balance freedom of expression with intermediary accountability in the digital environment.

However, the application of Section 79 to generative AI platforms remains uncertain. Unlike conventional intermediaries that merely host third-party content, many AI systems actively generate text, images, audio, or software code in response to user prompts. This raises an unresolved legal question: should developers of generative AI be treated as passive intermediaries entitled to safe harbour, or as active creators responsible for AI-generated

outputs? The IT Act provides no explicit answer, creating uncertainty for courts, technology companies, and users alike.

D. The Legislative Gap

The foregoing analysis demonstrates that the IT Act effectively regulates cyber offences committed by identifiable human actors but does not adequately address harms caused by increasingly autonomous AI systems. Its provisions assume that unlawful conduct can ultimately be traced to a natural or juristic person exercising meaningful control over the technology. As AI systems evolve beyond predictable, rule-based software into adaptive and self-learning models, this assumption becomes progressively weaker. The Act therefore remains reactive rather than anticipatory, highlighting the need for legislative clarification regarding AI-specific liability and accountability.

4. Judicial Responses and Comparative Perspectives on AI Liability

The rapid advancement of Artificial Intelligence has outpaced the development of legal doctrines governing accountability for technology-driven harms. Although Indian courts have not yet adjudicated a case directly concerning liability arising from autonomous AI systems, several judicial decisions establish principles that are relevant to understanding how existing law may respond to AI-generated harm. These decisions, when read alongside contemporary academic scholarship and comparative international developments, reveal both the strengths and limitations of India's current legal framework.

One of the most significant decisions in India's digital jurisprudence is *Shreya Singhal v. Union of India*, where the Supreme Court interpreted Section 79 of the Information Technology Act, 2000 and clarified that intermediaries enjoy safe harbour protection unless they fail to comply with lawful directions issued by a court or the appropriate government.[1] While the judgment concerned online intermediaries rather than AI systems, it reaffirmed the principle that liability under the IT Act is closely linked to human knowledge and control. This approach becomes difficult to apply where generative AI systems independently create harmful content, such as defamatory statements, deepfake videos, or fraudulent communications, without direct human supervision. The judgment therefore offers only limited guidance for determining

[1] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

responsibility in cases involving autonomous AI outputs.

Similarly, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a fundamental right under Article 21 of the Constitution and emphasised the importance of informational privacy in the digital age.[2] Although the decision predates the widespread deployment of generative AI, its constitutional reasoning assumes increasing significance as AI systems routinely process vast quantities of personal data. Algorithmic profiling, facial recognition technologies, and predictive analytics raise concerns regarding consent, transparency, and data minimisation. While *Puttaswamy* establishes a constitutional framework for protecting individual privacy, it does not resolve the question of liability where autonomous AI systems misuse or inadvertently expose personal information.

The decision in *Anvar P.V. v. P.K. Basheer* further demonstrates the judiciary's willingness to adapt traditional evidentiary principles to digital technologies by recognising the importance of authentic electronic evidence.[3] As AI-generated content becomes increasingly sophisticated, however, distinguishing genuine electronic records from manipulated outputs presents new evidentiary challenges. Hyper-realistic deepfakes and synthetic documents may satisfy conventional technical requirements while simultaneously undermining the reliability of digital evidence. Existing evidentiary rules therefore require continued judicial evolution to remain effective in an AI-driven environment.

The limitations of traditional liability doctrines have also attracted considerable scholarly attention. Ryan Abbott argues that legal systems should resist recognising AI as an independent legal person and should instead allocate responsibility to the humans involved in designing, deploying, or benefiting from AI technologies.[4] This approach preserves established principles of accountability while avoiding the conceptual difficulties associated with attributing legal personality to machines. Within the Indian context, Abbott's argument aligns with the existing structure of the Information Technology Act, which consistently imposes obligations upon natural or juristic persons rather than technological systems. However, the Act provides no clear criteria for determining which human actor should bear responsibility when multiple parties contribute to an autonomous AI's operation.

[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[3] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[4] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* 41–67 (Cambridge Univ. Press 2020).

Joanna Bryson similarly contends that AI should be regarded as a sophisticated tool rather than an autonomous legal entity capable of bearing rights or duties.[5] According to Bryson, assigning legal personality to AI risks allowing developers and corporations to evade responsibility by attributing blame to technology itself. This perspective reinforces the principle that accountability must ultimately remain with human actors. Nevertheless, as AI systems become increasingly adaptive and capable of generating unforeseen outcomes, identifying the appropriate liable party remains a significant practical challenge under existing Indian law.

Comparative developments provide useful guidance for addressing these shortcomings. The European Union's AI Act adopts a risk-based regulatory model that classifies AI systems according to the level of risk they pose and imposes corresponding obligations relating to transparency, human oversight, documentation, and compliance.[6] Rather than attempting to confer legal personality upon AI, the legislation focuses on regulating developers, providers, importers, and deployers according to their respective roles within the AI lifecycle. Likewise, the United Kingdom has favoured a principles-based approach centred on safety, transparency, fairness, accountability, and contestability, allowing existing sectoral regulators to oversee AI within their respective jurisdictions.[7] Singapore's Model AI Governance Framework similarly emphasises explainability, human-centric decision-making, and organisational accountability without creating an entirely separate legal regime for AI.[8]

These comparative approaches illustrate that effective AI governance does not necessarily require recognising AI as an independent legal subject. Instead, they emphasise clear allocation of human responsibility, proportionate regulation based on risk, and mandatory governance mechanisms capable of adapting to technological change. In contrast, India's Information Technology Act, 2000 remains primarily directed towards conventional cyber offences and intermediary liability, offering limited guidance on harms generated through autonomous AI decision-making. Consequently, while existing judicial principles provide a useful normative foundation, they are insufficient to resolve the novel attribution problems posed by increasingly autonomous AI systems. This gap underscores the need for a modern regulatory framework

[5] Joanna J. Bryson, Mihailis E. Diamantis & Thomas D. Grant, *Of, for, and by the People: The Legal Lacuna of Synthetic Persons*, 25 *Artificial Intelligence & Law* 273 (2017)
[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L).
[7] Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation* (U.K. Gov't, 2023).
[8] Infocomm Media Development Authority & Personal Data Protection Commission Singapore, *Model AI Governance Framework* (2d ed. 2020).

that complements, rather than replaces, India's existing cyber law architecture.

5. Recommendations

The preceding analysis demonstrates that while the Information Technology Act, 2000 provides a valuable foundation for regulating cyber activities, it does not adequately address liability arising from autonomous AI systems. Rather than replacing the existing framework, India should adopt targeted reforms that clarify responsibility while preserving technological innovation.

First, the Information Technology Act should be amended to expressly recognise AI-enabled harms. The Act currently regulates cyber offences and intermediary liability but remains silent on autonomous decision-making. Introducing AI-specific provisions would reduce legal uncertainty and enable courts to apply consistent principles when determining responsibility for AI-related harm.

Secondly, Parliament should incorporate a statutory definition of "autonomous AI system." The absence of a legal definition creates ambiguity regarding the scope of regulation and liability. A clear definition should distinguish adaptive AI systems capable of independent decision-making from conventional software operating solely on predetermined instructions. Such a distinction would ensure that liability rules are applied proportionately to technologies posing greater legal and societal risks.

Thirdly, mandatory human oversight should be required for AI deployed in high-risk sectors such as healthcare, financial services, transportation, law enforcement, and critical public infrastructure. Decisions involving diagnosis, criminal investigations, credit evaluation, or autonomous vehicles should not rely exclusively on algorithmic outputs. Human review should remain an essential safeguard where AI decisions may significantly affect individual rights or public safety.

India should also adopt a risk-based regulatory framework similar to international best practices. Instead of regulating every AI application uniformly, obligations should correspond to the level of risk posed by a particular system. High-risk AI should be subject to stricter requirements relating to transparency, documentation, safety testing, and post-deployment monitoring, while lower-risk applications may be governed through lighter compliance

obligations. Such an approach would encourage innovation without imposing unnecessary regulatory burdens.

Another important reform is the introduction of mandatory AI audits for high-risk systems. Independent technical and legal audits should evaluate algorithmic reliability, cybersecurity safeguards, data governance practices, and potential bias before deployment and at regular intervals thereafter. Periodic audits would promote transparency and enable organisations to identify and mitigate foreseeable risks before harm occurs.

Given the possibility of substantial financial losses resulting from autonomous AI failures, liability insurance should also be considered for operators and developers of high-risk AI systems. Similar to compulsory insurance in sectors involving significant public risk, such a mechanism would facilitate timely compensation for affected individuals while encouraging responsible deployment and risk management.

Finally, India should establish an independent AI regulatory authority responsible for developing technical standards, issuing compliance guidelines, monitoring high-risk AI systems, coordinating with sectoral regulators, and advising the government on emerging technological challenges. A specialised regulator would provide institutional expertise that existing regulatory bodies may currently lack and ensure that AI governance evolves alongside technological advancement.

6. Conclusion

Artificial Intelligence is reshaping the digital landscape at a pace that existing legal frameworks struggle to accommodate. Although the Information Technology Act, 2000 continues to serve as the cornerstone of India's cyber law regime, it was enacted in an era when autonomous AI systems were neither commercially viable nor legally foreseeable. Consequently, its provisions primarily regulate the conduct of identifiable human actors and provide limited guidance where AI independently contributes to harmful outcomes. As AI assumes increasingly autonomous roles in critical sectors, these traditional assumptions of legal responsibility become progressively inadequate. India's response should therefore focus on modernising its existing legal framework through targeted legislative amendments, risk-based regulation, institutional oversight, and clearer accountability mechanisms rather than abandoning established legal principles. A balanced approach that protects innovation while ensuring effective legal

responsibility will be essential for building public trust in AI and supporting its responsible integration into Indian society.

Bibliography

A. Statutes and Legislation

Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).

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

Digital Personal Data Protection Act, No. 22 of 2023 (India).

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

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L).

B. Cases

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

C. Books

Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge Univ. Press 2020).

D. Journal Articles

Joanna J. Bryson, Mihailis E. Diamantis & Thomas D. Grant, Of, for, and by the People: The Legal Lacuna of Synthetic Persons, 25 *Artificial Intelligence and Law* 273 (2017).

Philipp Hacker, The European AI Liability Directives—Critique of a Half-Hearted Approach and Lessons for the Future, 14 *Journal of European Consumer and Market Law* 5 (2023).

E. Government Reports and Policy Documents

Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation* (U.K. Gov't 2023).

Infocomm Media Development Authority & Personal Data Protection Commission Singapore, *Model AI Governance Framework* (2d ed. 2020).

NITI Aayog, *National Strategy for Artificial Intelligence: #AIForAll* (2018).

NITI Aayog, *Responsible AI for All: Approach Document for India, Part I—Principles for Responsible AI* (2021).

Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (2019).

UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).