International Journal of Professional Development
ISSN: 2277-517X (Print), 2279-0659 (Online) Vol.13, No.2, July-Dec.2024
Impact Factor: 3.986(IFSIJ)

Artificial Intelligence and Criminal Liability: A Study of the Legal Framework in India

Rupender
Designation - Advocate
Email- advocaterupenderchoudhary@gmail.com
Mob. No. 7988153788

Abstract
The rapid advancement of artificial intelligence (AI) technologies has presented unprecedented challenges to traditional legal frameworks, particularly in the realm of criminal liability. As AI systems become increasingly autonomous and capable of making decisions that can result in harm, questions arise regarding who should be held accountable when these systems cause injury, death, or other criminal consequences. This paper examines the current legal framework in India concerning AI and criminal liability, analyzes the gaps in existing legislation, and proposes potential approaches to address these emerging challenges. Through an examination of the Indian Penal Code, Information Technology Act, and relevant case law, this research identifies the need for comprehensive legal reform to accommodate the unique characteristics of AI systems while ensuring accountability and justice

Keywords: Artificial Intelligence, Criminal Liability and Legal Framework in India

Introduction

Artificial Intelligence has transitioned from a theoretical concept to a practical reality that permeates various aspects of modern life. From autonomous vehicles and medical diagnostic systems to algorithmic trading platforms and predictive policing tools, AI systems are increasingly making decisions that were traditionally reserved for human judgment. This technological evolution raises fundamental questions about legal responsibility, particularly in criminal law where the principles of mens rea (guilty mind) and actus reus (guilty act) have long been foundational.

The Indian legal system, rooted in colonial-era legislation and common law principles, faces significant challenges in addressing AI-related criminal liability. The Indian Penal Code, 1860 (IPC), was drafted in an era when the concept of non-human decision-making entities was inconceivable. Similarly, the Information Technology Act, 2000 (IT Act), while more contemporary, primarily addresses cybercrime and electronic commerce rather than AI-specific concerns. This paper examines whether India's current legal framework adequately addresses criminal liability involving AI systems and explores potential pathways for legal reform.

Understanding AI and Its Classification

Before examining legal liability, it is essential to understand the different categories of AI systems. AI can be broadly classified into three types:

Narrow AI (Weak AI): These systems are designed to perform specific tasks, such as facial recognition, spam filtering, or recommendation algorithms. Most contemporary AI applications fall into this category.

General AI (Strong AI): Hypothetical systems that would possess human-like cognitive abilities and could perform any intellectual task that a human can perform. Such systems do not currently exist.

Super AI: Theoretical systems that would surpass human intelligence across all domains. This remains entirely speculative.

For legal purposes, the distinction between these categories is crucial. Current discussions of AI liability primarily concern Narrow AI systems, which operate within defined parameters but may

exhibit unexpected behavior due to machine learning algorithms. The degree of autonomy, predictability, and human oversight varies significantly across different AI applications, necessitating nuanced legal approaches.

Traditional Principles of Criminal Liability in India

The Indian criminal justice system is predicated upon several fundamental principles that pose challenges when applied to AI systems:

Mens Rea and Actus Reus: The IPC requires both a guilty mind (mens rea) and a guilty act (actus reus) for most criminal offenses. Section 39 of the IPC defines "voluntarily" as causing an effect by an act done with the intention of causing that effect, or with knowledge that such effect is likely to be caused. AI systems, lacking consciousness and intent, cannot possess mens rea in the traditional sense. This creates a fundamental incompatibility between AI decision-making and criminal liability.

Legal Personhood: Under Indian law, only natural persons and certain legal entities (corporations, companies) can be held criminally liable. The IPC does not recognize AI systems as legal persons. While corporate criminal liability has been established through vicarious liability principles, extending this framework to AI presents unique challenges.

Causation: Establishing causation—linking the accused's actions to the criminal outcome—is essential for criminal liability. In AI cases, causation becomes complex due to multiple actors involved in designing, programming, deploying, and maintaining AI systems. Determining which actor's conduct was the proximate cause of harm is often difficult.

Current Legal Framework in India

The Indian Penal Code, 1860: The IPC remains the primary source of criminal law in India but contains no provisions specifically addressing AI. Several sections could potentially apply to AI-related harms:

Section 304A (Death by Negligence): Could apply when AI systems cause death through negligent design or deployment. However, proving negligence requires establishing a duty of care and breach, which is complicated when multiple parties are involved in AI development and deployment.

Section 336 (Endangering Life or Personal Safety): This provision addresses acts that endanger human life, potentially applicable to reckless AI deployment.

Section 66 (Computer Related Offenses): While part of the IPC, this section has been largely superseded by the IT Act.

The Information Technology Act, 2000

The IT Act, amended in 2008, addresses cybercrimes and electronic governance but does not specifically tackle AI liability. Relevant provisions include:

Section 43 (Penalty for Damage to Computer Systems): Imposes civil liability for unauthorized access or damage to computer systems, potentially applicable when AI systems are compromised.

Section 66 (Computer Related Offenses): Addresses fraudulent computer-related activities but lacks specificity regarding autonomous AI decision-making.

Section 72 (Breach of Confidentiality and Privacy): Could apply to AI systems that mishandle personal data, though not specifically designed for AI contexts.

The Motor Vehicles Act, 1988: With the advent of autonomous vehicles, the Motor Vehicles Act becomes relevant. However, the Act presumes human drivers and lacks provisions for fully autonomous systems. The 2019 amendments did not adequately address liability in autonomous vehicle accidents.

Emerging Regulations: The Digital Personal Data Protection Act, 2023, represents India's effort to regulate data processing, including by AI systems. While primarily focused on privacy and data protection, it establishes principles that could influence AI liability frameworks. The Act mandates accountability and transparency in data processing, potentially creating a foundation for AI-specific regulations.

Judicial Approach and Case Law: Indian courts have not yet extensively addressed AI-

specific criminal liability. However, several cases provide insights into how existing legal principles might apply:

Justice K.S. Puttaswamy v. Union of India (2017): While not directly about AI, this landmark privacy judgment established that technology must be compatible with constitutional rights. The Court recognized that technological advancement must be balanced with fundamental rights protection, providing a constitutional foundation for regulating AI systems.

Shreya Singhal v. Union of India (2015): This case struck down Section 66A of the IT Act, emphasizing the importance of precisely drafted legislation in technology-related matters. The judgment suggests that vague or overly broad AI regulations could face constitutional challenges.

Evolving Jurisprudence on Corporate Criminal Liability: Indian courts have increasingly recognized corporate criminal liability through the doctrine of vicarious liability and the identification theory. In Standard Chartered Bank v. Directorate of Enforcement (2005), the Supreme Court held that corporations could be prosecuted for criminal offenses. This jurisprudence could potentially extend to AI systems deployed by corporations.

Theoretical Approaches to AI Criminal Liability

Legal scholars and policymakers have proposed various approaches to address AI criminal liability:

Direct Liability of AI Systems: This approach would grant legal personhood to AI systems, making them directly liable for criminal acts. The European Parliament has considered creating a legal status of "electronic persons" for sophisticated AI systems. However, this raises philosophical and practical questions: Can punishment deter AI behavior? How would sanctions be enforced against non-human entities?

Liability of Developers and Manufacturers: Under this model, criminal liability would attach to those who design, develop, and manufacture AI systems. This approach aligns with traditional product liability principles but may be problematic for open-source AI or systems that learn and evolve post-deployment.

Liability of Users and Deployers: Organizations or individuals deploying AI systems could bear criminal liability for harms caused. This approach incentivizes careful selection and monitoring of AI systems but may discourage innovation and AI adoption.

Strict Liability: Given the difficulty of establishing mens rea, some scholars advocate for strict liability offenses for AI-related harms. This would eliminate the intent requirement for certain AI-caused injuries, though it raises concerns about fairness and proportionality.

Shared or Distributed Liability: This approach recognizes that AI systems result from contributions by multiple actors—developers, data providers, deployers, and users. Liability would be apportioned based on each party's contribution to the harmful outcome.

Challenges in Establishing AI Criminal Liability in India

Several obstacles complicate the establishment of AI criminal liability in India:

The Black Box Problem: Many AI systems, particularly those using deep learning, operate as "black boxes" where decision-making processes are opaque even to their creators. This opacity makes it difficult to establish causation and assign blame.

Autonomy and Unpredictability: As AI systems become more autonomous and capable of learning, their behavior may diverge from their original programming. When an AI system acts in unexpected ways, determining liability becomes problematic.

Rapid Technological Evolution: Legal systems are inherently conservative and slow to change, while AI technology evolves rapidly. Legislation risks becoming obsolete before enactment.

Evidentiary Issues: Proving criminal liability requires evidence of intent, knowledge, or negligence. In AI cases, technical complexity may make it difficult for prosecutors, judges, and

juries to understand how systems function and where responsibility lies.

Cross-Border Complications: AI systems often involve international supply chains, with development, data storage, and deployment occurring across multiple jurisdictions. This creates challenges for Indian law enforcement and courts.

Comparative Perspectives: International Approaches

Examining how other jurisdictions address AI liability provides valuable insights for India:

European Union: The EU has been proactive in AI regulation. The proposed AI Act categorizes AI systems by risk level and imposes varying obligations. The EU's approach emphasizes transparency, accountability, and human oversight. The Product Liability Directive is being revised to address AI-specific challenges.

United States: The US has adopted a sector-specific approach, with different agencies regulating AI in their domains. There is no comprehensive federal AI liability framework, though states like California have enacted AI-related legislation. The focus has been on algorithmic transparency and anti-discrimination.

United Kingdom: The UK has proposed a principles-based approach to AI regulation, emphasizing safety, transparency, fairness, accountability, and contestability. This flexible framework allows adaptation to technological changes.

China: China has enacted several AI-related regulations, including algorithmic recommendation regulations and deep synthesis regulations. The approach emphasizes state control, security, and social stability alongside innovation.

Proposed Framework for India

Based on the analysis above, India should consider a comprehensive approach to AI criminal liability:

Legislative Reform

Specialized AI Legislation: India needs dedicated AI legislation that addresses liability, governance, and ethical principles. This legislation should complement rather than replace existing criminal law.

Amendments to the IPC: Specific provisions should address AI-related harms, including negligent AI deployment, failure to supervise AI systems, and reckless disregard for AI-related risks.

Clarification of Liability Standards: Legislation should specify when developers, deployers, and users bear criminal liability for AI-caused harms.

Risk-Based Classification: Adopting a risk-based approach similar to the EU's AI Act would categorize AI systems based on potential harm. High-risk systems (autonomous vehicles, medical AI, criminal justice AI) would face stricter regulatory requirements and clearer liability frameworks.

Mandatory Impact Assessments: Organizations deploying high-risk AI systems should conduct mandatory impact assessments examining potential harms, risks, and mitigation measures. Failure to conduct adequate assessments could constitute criminal negligence.

Human Oversight Requirements: For high-risk applications, meaningful human oversight should be mandatory. The "human-in-the-loop" approach ensures human decision-makers can intervene in AI processes, establishing clearer lines of accountability.

Transparency and Explainability: AI systems in sensitive domains should meet transparency and explainability standards. The ability to explain AI decision-making is crucial for establishing causation and liability.

Establishment of Regulatory Bodies: India should establish specialized regulatory bodies with technical expertise to oversee AI development and deployment. These bodies could investigate AI-related incidents, much like aviation accident investigation boards.

Vicarious Liability Framework: Corporate entities deploying AI systems should bear vicarious liability for AI-caused harms. This

incentivizes careful AI selection, monitoring, and governance.

Conclusion

The intersection of artificial intelligence and criminal liability presents profound challenges to India's legal system. The current framework, developed for human actors, inadequately addresses the unique characteristics of AI systems—their autonomy, opacity, and distributed development process. While the IPC and IT Act provide some foundation, they are insufficient for the AI era.

India stands at a critical juncture. The country has the opportunity to develop a comprehensive, forward-looking legal framework that balances innovation with accountability, technological advancement with fundamental rights protection. This framework must address key questions: When should AI-related harms constitute criminal offenses? Who bears responsibility—developers, deployers, or users? What standards of care should apply?

The proposed approach—combining legislative reform, risk-based classification, mandatory oversight, and specialized regulatory bodies—offers a pathway forward. This framework would establish clear liability principles while remaining flexible enough to adapt to technological evolution.

As AI becomes increasingly embedded in Indian society, from healthcare and transportation to finance and governance, the need for legal clarity becomes urgent. Without adequate legal frameworks, there is a risk of either stifling beneficial innovation through legal uncertainty or failing to hold responsible parties accountable for AI-caused harms.

The development of AI liability law in India will require collaboration among legislators, judiciary, technologists, ethicists, and civil society. International cooperation and learning from comparative approaches will be valuable. Ultimately, the goal must be to create a legal framework that serves justice, protects rights, encourages responsible innovation, and maintains public trust in both technology and law.

References

1. Basu, S. (2020). "Artificial Intelligence and Criminal Liability: Need for a Legal Framework in India." *Journal of Indian Law Institute*, 62(3), 345-368.
2. Chopra, S., & White, L. (2011). *A Legal Theory for Autonomous Artificial Agents*. University of Michigan Press.
3. Council of Europe. (2022). "Artificial Intelligence and Criminal Law." *European Committee on Crime Problems*, Report No. PC-OC (2022) 03.
4. Digital Personal Data Protection Act, 2023. Act No. 22 of 2023. Government of India.
5. European Commission. (2021). "Proposal for a Regulation on Artificial Intelligence (AI Act)." COM(2021) 206 final.
6. Hallevy, G. (2015). *Liability for Crimes Involving Artificial Intelligence Systems*. Springer International Publishing.
7. Information Technology Act, 2000. Act No. 21 of 2000. Government of India.
8. Information Technology (Amendment) Act, 2008. Act No. 10 of 2009. Government of India.
9. Indian Penal Code, 1860. Act No. 45 of 1860. Government of India.
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
11. Kumar, A., & Singh, R. (2022). "Autonomous Systems and Criminal Liability: Indian Perspective." *Indian Journal of Law and Technology*, 18(1), 89-112.
12. Law Commission of India. (2018). "Report on Electronic Evidence and Related Issues." Report No. 271.
13. Matthias, A. (2004). "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata." *Ethics and Information Technology*, 6(3), 175-183.
14. Motor Vehicles (Amendment) Act, 2019. Act No. 32 of 2019. Government of India.
15. NITI Aayog. (2021). "Responsible AI: Principles for AI." Government of India.

16. Pagallo, U. (2013). *The Laws of Robots: Crimes, Contracts, and Torts*. Springer.
17. Raja, D. K. (2019). "Artificial Intelligence and the Indian Legal System: Emerging Challenges." *Socio-Legal Review*, 15(2), 234-259.
18. Ratcliffe, S. (2020). "Product Liability and Artificial Intelligence: An Update." *Computer Law & Security Review*, 39, 105471.
19. Scherer, M. U. (2016). "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies." *Harvard Journal of Law & Technology*, 29(2), 353-400.
20. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
21. Standard Chartered Bank v. Directorate of Enforcement, (2005) 4 SCC 530.
22. Turner, J. (2019). *Robot Rules: Regulating Artificial Intelligence*. Palgrave Macmillan.
23. UK House of Lords Select Committee on Artificial Intelligence. (2018). "AI in the UK: Ready, Willing and Able?" HL Paper 100.
24. Vladeck, D. C. (2014). "Machines Without Principals: Liability Rules and Artificial Intelligence." *Washington Law Review*, 89(1), 117-150.
25. Wadhwa, V., & Salkever, A. (2017). *The Driver in the Driverless Car: How Our Technology Choices Will Create the Future*. Berrett-Koehler Publishers.
26. Wischmeyer, T., & Rademacher, T. (Eds.). (2020). *Regulating Artificial Intelligence*. Springer International Publishing.