INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY IN INDIA: LEGAL CHALLENGES AND THE NEED FOR A STRUCTURED ACCOUNTABILITY FRAMEWORK

AUTHORED BY - DR ASHISH PRATAP SINGH
Assistant Professor
Department of Law
ISBM University, Chhattisgarh

Abstract

Artificial Intelligence (AI) is rapidly transforming governance, commerce, healthcare, finance, and law enforcement in India. As AI systems become increasingly autonomous, the Indian criminal justice system faces unprecedented doctrinal and regulatory challenges. Criminal liability in India is traditionally grounded in the principles of *actus reus* and *mens rea*, codified primarily under the Indian Penal Code, 1860. Autonomous AI systems complicate the attribution of intent, foreseeability, and culpability. This paper critically examines whether AI can bear criminal liability under Indian law, analyses constitutional implications under Constitution of India, evaluates statutory gaps under the Information Technology Act, 2000, and considers the regulatory shift introduced by the Digital Personal Data Protection Act, 2023. The paper argues that AI cannot be directly criminally liable under existing Indian legal principles; instead, a hybrid framework emphasizing corporate criminal liability, regulatory compliance, and graded accountability is necessary to prevent accountability vacuums while preserving technological innovation.

1. Introduction

India has emerged as a major player in artificial intelligence development and deployment. AI applications are increasingly used in facial recognition systems, predictive policing tools, financial fraud detection, healthcare diagnostics, e-governance platforms, and autonomous mobility technologies. Government initiatives such as the National Strategy for Artificial Intelligence ("AI for All") demonstrate the state's commitment to integrating AI into governance.

However, AI deployment has outpaced legislative reform. When an AI-driven system causes

ISSN: 2582-6433

harm—such as wrongful arrest through facial recognition, algorithmic bias in welfare allocation, or fatal malfunction of autonomous vehicles—the question arises: who is criminally responsible under Indian law?

India's criminal justice system is historically human-centric. The Indian Penal Code, 1860 (IPC) presumes a human offender capable of intention, knowledge, or negligence. AI systems, by contrast, operate through algorithmic decision-making without consciousness or moral understanding.

This paper contends that while AI cannot satisfy the mental element required for criminal liability under Indian jurisprudence, accountability gaps must be addressed through structured regulatory and corporate liability reforms.

2. Foundations of Criminal Liability Under Indian Law

2.1 Actus Reus and Mens Rea in the IPC

Indian criminal law, largely codified in the IPC, is built upon two essential elements:

- **Actus Reus** – A voluntary act or illegal omission.
- **Mens Rea** – Guilty intention, knowledge, recklessness, or negligence.

The Supreme Court of India has repeatedly emphasized the importance of mens rea unless explicitly excluded by statute. In *State of Maharashtra v. Mohd. Yakub* (1980), the Court underscored the necessity of establishing intention or knowledge in criminal offenses.

AI systems present difficulty because:

- They perform physical acts (e.g., automated decision outputs).
- They lack intention or awareness.
- Their outcomes may be emergent rather than directly programmed.

Thus, attributing mens rea to AI under the IPC is conceptually incompatible with established doctrine.

3. Can AI Be a "Person" Under Indian Law?

3.1 Legal Personhood in India

Indian law recognizes both natural and juristic persons. Corporations are recognized as legal persons capable of prosecution. In *Standard Chartered Bank v. Directorate of Enforcement* (2005), the Supreme Court held that corporations can be prosecuted for criminal offenses.

However, corporations consist of human agents whose intent can be attributed to the company.

ISSN: 2582-6433

AI systems do not possess such human intermediaries once deployed autonomously.

Granting AI legal personhood would raise constitutional and philosophical issues. The Constitution of India guarantees fundamental rights to "persons," but these rights are grounded in human dignity and moral agency. Extending personhood to AI would distort constitutional principles.

Therefore, under current Indian jurisprudence, AI cannot be treated as a legal person capable of criminal prosecution.

4. Corporate Criminal Liability and AI Deployment

Indian courts recognize corporate criminal liability. Where AI is deployed by a company, liability may attach through:

- Vicarious liability
- Negligent supervision
- Failure to implement safeguards
- Fraudulent misrepresentation

If a company knowingly deploys unsafe AI systems, liability may arise under IPC provisions relating to negligence (e.g., Section 304A – causing death by negligence).

However, the challenge lies in proving:

- Foreseeability of harm
- Failure to exercise due care
- Direct nexus between human negligence and AI outcome

As AI systems become self-learning and adaptive, this nexus becomes harder to establish.

5. AI and the Information Technology Act, 2000

The Information Technology Act, 2000 governs cybercrimes, electronic records, and intermediary liability. While the Act addresses hacking, data theft, and cyber fraud, it does not directly regulate AI systems.

Section 79 of the IT Act provides safe harbor protection to intermediaries, subject to due diligence compliance. If AI platforms generate harmful content (e.g., misinformation, deepfakes), intermediary liability becomes relevant.

However, the IT Act was enacted before modern AI systems existed. It does not address:

- Autonomous decision-making
- Algorithmic bias

ISSN: 2582-6433

- AI-driven physical harm
- Accountability for machine learning errors

Thus, statutory reform is necessary.

6. Data Protection and AI Governance

The enactment of the Digital Personal Data Protection Act, 2023 marks a significant development in India's regulatory framework. AI systems rely heavily on personal data for training and deployment.

The DPDP Act imposes obligations on data fiduciaries, including:

- Lawful processing
- Purpose limitation
- Data minimization
- Security safeguards

While the Act does not directly impose criminal liability for AI harm, non-compliance may attract penalties. Improper data handling in AI systems could lead to criminal charges under other statutes if harm occurs.

7. Constitutional Implications of AI in India

AI deployment intersects with fundamental rights under the Constitution of India, particularly:

- Article 14 – Equality before law
- Article 19 – Freedom of speech and expression
- Article 21 – Right to life and personal liberty

In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognized privacy as a fundamental right. AI systems involving facial recognition or mass surveillance may infringe this right.

If AI-driven decisions result in deprivation of liberty (e.g., wrongful arrest through predictive policing), constitutional remedies may arise, even if criminal liability is unclear.

8. Autonomous Vehicles and Criminal Negligence in India

India currently regulates motor vehicles under the Motor Vehicles Act, 1988. Fully autonomous vehicles are not yet widely deployed, but the issue is imminent.

If an autonomous vehicle causes death:

ISSN: 2582-6433

- Section 304A IPC (causing death by negligence) may apply.
- Liability could fall on manufacturers or operators.

However, proving negligence in algorithmic design presents evidentiary challenges:

- Access to proprietary code
- Expert testimony requirements
- Determining foreseeability of algorithmic error

Indian courts may need to evolve standards of "algorithmic negligence."

9. Algorithmic Bias and Criminal Justice

AI tools used in law enforcement—such as facial recognition—raise concerns of bias and wrongful identification. If AI misidentifies an innocent person, resulting in arrest or detention, criminal liability may not attach directly to the AI.

Instead, liability may arise from:

- Police misuse
- Reckless reliance on unverified technology
- Violation of procedural safeguards

Judicial scrutiny under Articles 14 and 21 would likely be the primary remedy.

10. The Case Against AI Criminal Personhood in India

Granting AI criminal liability would be problematic because:

1. AI lacks consciousness.
2. AI cannot form mens rea.
3. Punishment (imprisonment/fine) lacks meaningful impact.
4. It may shield developers and corporations.

Indian criminal law is retributive and deterrent in nature. AI cannot be deterred or morally blamed.

11. Proposed Indian Hybrid Accountability Framework

To address accountability gaps, India should adopt a structured model:

11.1 Risk-Based Regulatory Classification

Inspired by global approaches, India should categorize AI systems by risk level:

- High-risk (law enforcement, healthcare, transport)
- Moderate-risk

ISSN: 2582-6433

- Low-risk

High-risk AI should require:

- Mandatory impact assessments
- Independent audits
- Government certification

11.2 Corporate Criminal Liability Expansion

Amend the IPC or introduce AI-specific legislation imposing liability where corporations:

- Fail to conduct due diligence
- Suppress known risks
- Deploy unsafe AI systems

11.3 Individual Liability for Gross Negligence

Engineers or executives should be liable only where:

- They intentionally override safety standards
- Engage in fraudulent concealment
- Act with reckless disregard for human life

11.4 Regulatory Authority for AI Oversight

India should establish a dedicated AI Regulatory Authority to:

- Set technical standards
- Conduct compliance audits
- Impose penalties
- Coordinate with data protection authorities

12. International Harmonization and India's Role

AI development is global. India must harmonize regulations with international frameworks to ensure competitiveness. However, regulation must be tailored to Indian realities, including:

- Digital divide
- Socioeconomic diversity
- Infrastructure disparities

ISSN: 2582-6433

13. Challenges to Implementation

- Balancing innovation with safety
- Preventing over-criminalization
- Ensuring judicial expertise in AI cases
- Avoiding regulatory capture
- Protecting startup ecosystems

14. Conclusion

Artificial Intelligence challenges the foundational assumptions of Indian criminal law. Under the Indian Penal Code, 1860, criminal liability depends on mens rea—an element AI systems cannot satisfy. The Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023 provide partial regulatory coverage but do not comprehensively address autonomous harm.

AI should not be granted criminal personhood under Indian law. Instead, accountability must focus on corporations, developers, and regulatory oversight. A hybrid model—combining risk-based classification, corporate criminal liability, and targeted individual responsibility—offers a balanced and constitutionally sound solution.

As India advances toward an AI-driven future, its legal system must evolve to ensure justice, fairness, and protection of fundamental rights without stifling innovation.