International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Artificial Intelligence and Criminal Liability Challenges in Regulating AI-Driven Crimes

Dr. Sangeeta Masani

HOD & Assistant Professor School of Law and social Justice, Dr. B.R.Ambedkar University of Social Sciences, Dr. Ambedkar Nagar, MHOW (M.P.)

Abstract

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the twenty-first century. AI systems are now capable of autonomous decision-making, predictive analysis, facial recognition, natural language processing, and automated operations across multiple sectors including healthcare, finance, governance, transportation, and law enforcement. While AI has generated immense social and economic benefits, it has simultaneously created complex legal and criminal liability issues. AI-driven crimes, such as autonomous cyberattacks, deepfake frauds, algorithmic discrimination, automated financial manipulation, and autonomous weapon-related offences, challenge the traditional principles of criminal jurisprudence. Existing criminal laws are primarily designed around human intention, knowledge, negligence, and physical acts. However, AI systems often function autonomously, making it difficult to determine criminal responsibility. This paper examines the concept of AI-driven crimes, analyzes the limitations of existing criminal liability principles, and discusses the challenges in regulating AI-related offences. It further evaluates international approaches and proposes legal reforms for ensuring accountability in the age of intelligent machines.

Keywords: Artificial Intelligence, Criminal Liability, AI Crimes, Autonomous Systems, Cybercrime, Deepfake, Legal Regulation.

Introduction

Artificial Intelligence refers to the simulation of human intelligence in machines capable of performing tasks that traditionally require human cognition. Modern AI systems can learn from data, adapt to changing environments, and make decisions with minimal human intervention. Technologies such as machine learning, generative AI, robotics, and neural networks have revolutionized industries globally. However, alongside innovation, AI has also become a tool for sophisticated criminal activities. Criminals increasingly use AI to automate cybercrimes, create realistic deepfakes, manipulate financial markets, conduct identity theft, and spread misinformation. Autonomous AI systems may even independently perform harmful acts beyond the direct control of their programmers or users[1].

Traditional criminal law is founded upon two essential elements: *actus reus* (guilty act) and *mens rea* (guilty mind). The challenge with AI lies in the absence of human consciousness or intention. Since AI systems do not possess moral understanding or legal personality equivalent to humans, determining

[1] Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, Pearson Education.

liability becomes difficult. Questions arise regarding whether responsibility should fall upon programmers, developers, users, corporations, or the AI system itself[2].

The growing use of AI in autonomous vehicles, military systems, healthcare diagnostics, and financial decision-making has intensified concerns regarding accountability and regulation. Therefore, there is an urgent need to revisit criminal law principles to address AI-driven offences effectively.

Concept of AI-Driven Crimes

AI-driven crimes refer to offences committed using AI systems or crimes resulting from the autonomous functioning of AI technologies. Such crimes may either involve human misuse of AI tools or harmful acts performed by autonomous AI systems.

Types of AI-Driven Crimes[3]

1. **Cybercrimes:** AI is increasingly used for sophisticated cyberattacks, including automated hacking, phishing, malware generation, and password cracking. AI algorithms can identify vulnerabilities faster than human hackers.
2. **Deepfake and Identity Fraud:** Generative AI can create realistic fake audio, video, and images known as deepfakes. These are used for political misinformation, blackmail, impersonation, and financial fraud.
3. **Autonomous Vehicle Crimes:** Self-driving vehicles may cause accidents resulting in injury or death. Determining liability in such cases becomes complicated because the vehicle acts based on machine learning algorithms.
4. **Algorithmic Financial Crimes:** AI-based trading systems may manipulate stock markets, engage in insider trading, or create unfair financial advantages without direct human intervention.
5. **AI-Assisted Terrorism:** Terrorist organizations may use AI for surveillance, automated drone attacks, and propaganda dissemination through social media algorithms.
6. **Biased Decision-Making:** AI systems used in policing, hiring, or judicial sentencing may discriminate against individuals due to biased datasets, thereby violating fundamental rights.

Traditional Principles of Criminal Liability[4]

Criminal liability traditionally depends upon establishing the following elements:

1. **Actus Reus:** Actus reus refers to the physical element of a crime, meaning the commission of an unlawful act or omission prohibited by law. Criminal liability generally requires proof that the accused voluntarily performed the wrongful conduct. In traditional criminal law, only human beings are considered capable of committing such prohibited acts intentionally or negligently.
2. **Mens Rea:** Mens rea means the "guilty mind" or mental element required for criminal liability. It includes intention, knowledge, recklessness, or negligence while committing a criminal act. Courts examine the state of mind of the accused to determine criminal responsibility. This principle becomes difficult in AI cases because machines lack consciousness and moral understanding.
3. **Causation:** Causation establishes a direct link between the accused's conduct and the resulting harm or injury. Criminal law requires proof that the act of the accused substantially caused the prohibited

[2] Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer.
[3] Ugo Pagallo, *The Laws of Robots*, Springer Publications.
[4] Prof. S. N. Misra, *Bharatiya Nyaya Sanhita, 2023* (Central Law Publications, 24th ed., 2024).

consequence. In AI-related offences, identifying causation becomes challenging because autonomous systems may independently make decisions without immediate human intervention or control.

4. **Punishment and Deterrence:** Punishment and deterrence are major objectives of criminal law. Punishment seeks to impose penalties upon offenders for wrongful conduct, while deterrence aims to discourage future crimes by creating fear of legal consequences. Applying these principles to AI systems is problematic because machines cannot experience punishment, fear, guilt, or moral accountability.

Challenges in Regulating AI-Driven Crimes

1. **Absence of Legal Personality:** AI systems are not recognized as legal persons under most legal systems. Since AI cannot independently possess rights or duties, imposing criminal liability directly upon AI becomes difficult. Unlike corporations, which are recognized as artificial legal persons, AI systems currently lack separate legal identity. Therefore, punishment such as imprisonment or fines cannot meaningfully apply to AI itself.
2. **Difficulty in Determining Mens Rea:** Criminal law requires proof of guilty intention. AI systems operate based on algorithms and data processing rather than conscious intent. For example, if an autonomous vehicle causes a fatal accident due to flawed machine learning decisions, identifying the guilty mind becomes nearly impossible. The programmer may not have intended harm, while the AI itself lacks mental capacity.
3. **Multiple Stakeholders and Diffused Responsibility:** AI development involves several actors, including programmers, developers, manufacturers, corporations, data providers, and users. Harmful outcomes may result from collective actions rather than individual misconduct. This creates uncertainty regarding who should bear criminal responsibility:
   - The software developer?
   - The company deploying the AI?
   - The end-user?
   - The data trainer?
   - The maintenance operator?

   The distributed nature of AI systems complicates accountability.
4. **Autonomous Decision-Making:** Modern AI systems can learn and evolve independently through machine learning. Their actions may become unpredictable even to their creators. An AI chatbot, for instance, may generate harmful or defamatory content without explicit programming instructions. Such autonomous behavior challenges traditional legal assumptions that humans control machines.
5. **Lack of Transparency and Explainability:** Many AI systems function as "black boxes," meaning their internal decision-making processes are difficult to understand. Courts may struggle to determine why a particular AI system acted in a harmful manner. Without transparency, proving causation and negligence becomes extremely difficult.
6. **Jurisdictional Challenges:** AI crimes often transcend national borders. A cyberattack may originate in one country, target victims in another, and involve servers located elsewhere. Differences in national laws create obstacles in investigation, extradition, and prosecution. International cooperation is therefore essential.
7. **Inadequate Existing Laws:** Most criminal laws were drafted before the rise of AI technologies. Existing cyber laws may address computer misuse but fail to regulate autonomous AI conduct

comprehensively. For example, many legal systems do not specifically regulate deepfake technology or autonomous weapons.

Approaches to Criminal Liability in AI Cases

1. **Perpetration-by-Another Model:** Under this model, AI is treated as an innocent instrument used by humans to commit crimes. Liability is imposed upon the person controlling or programming the AI system. For example, if a person uses AI-generated deepfakes for extortion, the human operator remains criminally liable. But this model fails where AI acts unpredictably beyond human control.
2. **Natural-Probable-Consequence Model:** Under this approach, developers or users may be liable if harmful outcomes were foreseeable consequences of deploying AI systems. For example, if a company knowingly releases unsafe autonomous software likely to cause harm, criminal negligence may arise. But it is difficult to determine foreseeability in complex AI environments.
3. **Corporate Liability Model:** Corporations deploying AI systems may be held criminally liable for harms caused by their technologies. This model is particularly relevant where companies prioritize profit over safety standards. Corporations possess financial resources and institutional control necessary for compliance and compensation.
4. **Electronic Personhood Theory:** Some scholars propose granting limited legal personality to advanced AI systems, similar to corporations. Under this theory, AI could bear certain legal responsibilities independently. Critics argue that AI lacks morality, consciousness, and social accountability. Granting personhood may also allow corporations to evade liability.

International Regulatory Approaches

European Union: The European Union has adopted significant measures for AI regulation through the proposed AI Act. The Act classifies AI systems based on risk categories and imposes strict obligations upon high-risk AI developers. The EU emphasizes transparency, human oversight, and accountability.

United States: The United States primarily relies upon sector-specific regulation and existing tort and criminal laws. Federal agencies are increasingly issuing AI governance guidelines. However, there is no comprehensive federal AI criminal liability framework.

China: China has implemented strict regulations concerning generative AI, algorithmic recommendation systems, and deepfake technologies. The Chinese government emphasizes state control and cybersecurity.

India: India currently regulates AI indirectly through laws such as; Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023[5], Digital Personal Data Protection Act, 2023. India has not yet enacted a dedicated AI legislation. Nevertheless, policy discussions emphasize ethical AI, data protection, and responsible innovation[6].

Need for Legal Reforms: The rapid advancement of Artificial Intelligence has created an urgent need for comprehensive legal reforms capable of addressing the unique challenges posed by AI-driven crimes. Traditional legal systems were designed primarily to regulate human conduct and therefore struggle to effectively govern autonomous technologies that can make decisions independently. Existing criminal laws often fail to adequately address issues such as algorithmic accountability, autonomous decision-making, deepfake misuse, cyber manipulation, and harms caused by self-learning systems. Consequently,

[5] Bharatiya Nyaya Sanhita, 2023.
[6] Information Technology Act, 2000 (India).

countries across the world must enact dedicated AI legislation specifically dealing with criminal liability, accountability mechanisms, safety standards, and ethical obligations relating to AI technologies. Such laws should clearly define the responsibilities of developers, manufacturers, deployers, and users of AI systems while also establishing penalties for misuse or negligent deployment of harmful technologies. Without comprehensive legislation, legal uncertainty may increase and victims of AI-related harm may face difficulties in obtaining justice[7].

Another important reform is the establishment of mandatory human oversight over critical AI systems. AI technologies used in sectors such as healthcare, transportation, military operations, policing, and financial services should never operate entirely without meaningful human supervision. Human oversight is necessary to ensure that AI decisions remain subject to ethical and legal scrutiny and to prevent autonomous harmful conduct. For example, autonomous vehicles, medical diagnostic systems, and predictive policing tools can significantly impact human life and liberty. In such circumstances, human operators must retain the authority to monitor, intervene, or override AI decisions whenever necessary. This approach helps preserve accountability and reduces the risk of catastrophic errors caused by algorithmic failures.

Furthermore, governments should require explainable and transparent AI systems, especially in high-risk sectors. Many modern AI systems function as "black boxes," meaning that their internal reasoning processes are difficult to understand even for their developers. Lack of transparency creates major legal challenges in determining liability and proving negligence or causation in criminal proceedings. Therefore, legal reforms should mandate explainable AI requirements that enable regulators, courts, and affected individuals to understand how AI systems arrive at particular decisions. Transparency would not only enhance public trust but also facilitate effective investigation and judicial review in cases involving AI-related harm[8].

Corporate accountability also forms an essential aspect of AI regulation. Corporations developing or deploying AI systems must implement robust compliance mechanisms, safety audits, risk assessments, and ethical review procedures. Since companies often possess significant control over AI design and deployment, they should bear responsibility for ensuring that their systems operate safely and lawfully. Failure to adopt reasonable safeguards should attract civil as well as criminal liability where serious harm occurs. Regulatory authorities may also require periodic inspections and certification mechanisms to ensure compliance with safety standard[9]s.

In addition, international cooperation is crucial because AI-driven crimes frequently transcend national boundaries. Cyberattacks, data theft, online fraud, and deepfake dissemination often involve multiple jurisdictions, making enforcement difficult under isolated national laws. Therefore, international treaties and collaborative regulatory frameworks are necessary to facilitate information sharing, extradition, joint investigations, and harmonized standards for AI governance. Finally, governments and educational institutions should actively promote ethical AI development by encouraging research that emphasizes fairness, non-discrimination, transparency, privacy protection, and respect for human rights. Ethical AI governance is essential to ensure that technological innovation benefits society without undermining justice, equality, and human dignity.

[7] Andrew Selbst, "Disparate Impact in Big Data Policing," Georgia Law Review.
[8] UNESCO Recommendation on Ethics of Artificial Intelligence, 2021.
[9] OECD Principles on Artificial Intelligence, 2019.

Conclusion

Artificial Intelligence has transformed modern society and offers tremendous opportunities for economic growth, innovation, and efficiency. However, AI-driven crimes present serious challenges to traditional criminal law principles. The absence of human intention, autonomous decision-making, lack of transparency, and multiple stakeholder involvement complicate the determination of criminal liability.

Existing legal frameworks remain inadequate to address the complexities of AI-generated harms. While several approaches such as corporate liability and negligence-based accountability provide partial solutions, no universally accepted model currently exists.

The future of criminal law will require a balanced approach that encourages technological innovation while ensuring public safety and accountability. Governments must develop comprehensive AI regulatory frameworks incorporating transparency, human oversight, ethical standards, and international cooperation. Ultimately, the law must evolve alongside technology to ensure that justice remains effective in the era of intelligent machines.