AI and Criminal Law: Assessing the Adequacy of Existing Legal Frameworks

ABSTRACT

The rapid development of Artificial Intelligence (AI) in areas like healthcare, business, government, and digital communication has created many advantages, but also new legal and regulatory issues. Autonomous decision-making, large data processing, content creation, and complex task execution are all areas where AI systems are capable. These can be used in wrongful ways, such as committing fraud, stealing identities, making deepfakes, privacy abuse, spreading false information, and cyberattacks. These issues highlight the shortcomings of most legal systems. They have been created with the idea of trying to keep control over people's behaviour, as opposed to technologies that operate on their own. This paper analyses, the legal constructs of AI-related crimes with specific emphasis to India. It attempts to study the scope of coverage of the Indian Penal Code 1860, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 in relation to crimes involving AI Systems. It also considers the different positions of the European Union, the United States of America, the United Kingdom, and the relevant case law and writings. The study attempts to conclude that the existing laws are partly sufficient and that with respect to AI, legislative reform is necessary in order to clarify the thresholds of liability and accountability for AI-related injuries.

Keywords: Artificial Intelligence, AI-related Crimes, Cybercrime, Data Protection, Privacy Rights, Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, AI Regulation, Deepfakes, Identity Theft, Criminal Liability, Global AI Governance

INTRODUCTION

One of the most disruptive technologies in history is Artificial Intelligence (AI). AI has impacted many areas, including healthcare, finance, administration, transport, education and communication. Through automation, predictive analysis and machine learning, AI has enabled increased efficiency and innovation and improved decision-making throughout the public and private sectors.

However, AI also brings with it new kinds of legal risks and criminal misuse, such as automated fraud; identity theft; the production of manipulated media; algorithmic discrimination; intrusive surveillance and increasingly sophisticated cyber-attacks. Unlike traditional crime, AI-related crime often includes the involvement of autonomous/semi-autonomous systems, multiple participants, indirect control and complicated causal chains, which create significant challenges for traditional criminal law that is based on human intent, behaviour and individual culpability.

This study looks at whether the existing legal structures adequately address crimes associated with artificial intelligence (AI). It also reviews international systems and developments in court and explores potential methods for improving criminal laws pertaining to AI.

1. LEGAL FRAMEWORK GOVERNING AI-RELATED CRIMES

The legal framework governing AI-related crimes is still in a developing stage, as most existing laws were drafted long before the emergence of advanced Artificial Intelligence systems. Traditional criminal laws were designed to address human conduct and intentional wrongdoing, whereas AI-generated crimes involve complex interactions between algorithms, data systems, and varying levels of human supervision. As a result, there exists a significant gap between technological advancement and legal regulation, making it difficult to effectively address offences committed through or by AI systems within the current legal structure. [1]

In India, as well as in many other jurisdictions, AI-related criminal liability is indirectly governed through existing laws such as the Indian Penal Code, 1860 and the Information Technology Act, 2000. However, these statutes do not specifically define or regulate Artificial Intelligence as an independent source of liability. Instead, they rely on traditional legal principles such as intention, knowledge, and negligence to determine criminal responsibility.

[1] *Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2021) 27–30.*

This creates challenges in applying these provisions to [2] AI-generated acts, particularly in situations where harm is caused autonomously without direct human intent or real-time control. [2]

The Information Technology Act plays a particularly important role in addressing cyber-related offences that may involve AI systems, such as hacking, identity theft, data breaches, and online fraud. Nevertheless, the Act primarily focuses on human actors and intermediaries, rather than autonomous systems capable of independent decision-making. Similarly, emerging concerns related to deepfakes, algorithmic manipulation, and automated cyberattacks highlight the limitations of existing legal provisions in dealing with technologically advanced forms of criminal activity.[3]

Another significant aspect of the legal framework is the growing importance of data protection and privacy laws in regulating AI systems. Since AI relies heavily on large datasets for training and functioning, issues of consent, data misuse, and privacy violations become central to legal analysis. Although India's Digital Personal Data Protection Act, 2023 provides a framework for safeguarding personal data, it does not comprehensively address criminal liability arising specifically from AI-generated harm. [4]

At the international level, different jurisdictions have adopted varied approaches to regulating AI-related crimes. The European Union has introduced risk-based regulatory frameworks, while other countries rely on sector-specific guidelines or ethical AI principles. However, there is no uniform global standard for assigning criminal liability in cases involving AI systems, which creates additional complexity in cross-border digital offences. [5]

Judicial interpretation also plays a crucial role in shaping the legal understanding of AI-related crimes, as courts attempt to apply existing legal doctrines to new technological realities. However, in the absence of specific legislation, judicial responses remain largely interpretative and case-specific. This highlights the urgent need for comprehensive legal reform to establish a clear and consistent framework for addressing AI-generated crimes effectively. [6]

1.1 Applicability of Indian Penal Code to AI-Generated Crimes

The Indian Penal Code, 1860 remains the core criminal statute in India and governs a wide range of offences based on the principles of human intention, action, and culpability. However, since the IPC was enacted in a pre-digital era, it does not explicitly recognise Artificial

[2] *Indian Penal Code, 1860; Information Technology Act, 2000; Andrew Murray, Information Technology Law (4th edn, OUP 2019) 412.*

[3] *Information Technology Act, 2000, ss 43, 66, 66C, 66D, 67.*

[4] *Digital Personal Data Protection Act, 2023 (India); Daniel J Solove, Understanding Privacy (Harvard University Press 2008) 101.*

[5] *European Union, Artificial Intelligence Act (EU Regulation, 2024); OECD, OECD Principles on Artificial Intelligence (2019).*

[6] Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar 2018) 233–240.

Intelligence as a subject of criminal liability. As a result, its application to AI-generated crimes is indirect and interpretative in nature. Courts and law enforcement agencies must rely on

traditional provisions and extend them to modern technological contexts, which often creates conceptual and practical difficulties in cases involving autonomous systems.

Most IPC provisions can only be applied to AI-related offences when a human actor behind the AI system can be clearly identified. For example, offences such as cheating, forgery, defamation, and criminal intimidation may be invoked when AI is used as a tool to commit harm. However, this approach assumes that a human being has full control over the system, which is not always the case in advanced AI applications. In situations where AI systems independently generate harmful outputs, the direct application of IPC provisions becomes legally uncertain and challenging.

A major limitation of the IPC in the context of AI is its strong reliance on the doctrine of *mens rea*. Criminal liability under the IPC generally requires intention, knowledge, or at least negligence on the part of the accused. However, AI systems do not possess mental intent in the legal sense, and their outputs are based on data-driven algorithms rather than conscious decision-making. This creates a legal gap when harm is caused without any identifiable human intention, making it difficult to satisfy the essential ingredients of many IPC offences. The doctrines of abetment and criminal conspiracy under the IPC are sometimes used to extend liability to individuals involved in the creation or deployment of AI systems. If it can be proven that a developer or user knowingly facilitated the misuse of AI technology for illegal purposes, liability may be established. However, in many AI-generated crime scenarios, the connection between human conduct and the final harmful outcome is indirect or unclear, which limits the effectiveness of these provisions in ensuring accountability.

Another challenge arises in establishing causation under the IPC when AI systems are involved. Criminal law requires a clear link between the accused's conduct and the resulting harm. In AI related cases, especially those involving machine learning and autonomous decision-making, the causal chain is often complex and multi-layered. The system's behaviour may evolve over time based on training data, making it difficult to trace a specific human action as the direct cause of the offence. This weakens the traditional framework of liability under the IPC.

Overall, while the Indian Penal Code provides a broad foundation for criminal prosecution, its effectiveness in addressing AI-generated crimes remains limited. The statute was not designed to deal with autonomous technologies, and its reliance on human intention and control creates significant gaps in applicability. As AI systems become more advanced and independent, there is a growing need for legal reforms or supplementary legislation to ensure that criminal liability can be effectively assigned in cases involving Artificial Intelligence.

1.2 Information Technology Act and Cyber Offences

The Information Technology Act, 2000 serves as the primary legislation in India for addressing cybercrimes and regulating electronic commerce and digital activities. It provides a legal framework for offences such as hacking, identity theft, data theft, cyber fraud, and publication of obscene or offensive material online. Since Artificial Intelligence systems often operate within digital environments, many AI-generated crimes fall indirectly under the ambit of the IT Act. However, the Act was enacted before the widespread adoption of AI technologies, and

therefore it does not specifically address issues related to autonomous systems or algorithmic decision-making.

The IT Act primarily assumes human intervention behind cyber activities, meaning that liability is generally attributed to individuals or organisations rather than autonomous systems. Sections dealing with unauthorised access, data damage, and cyber fraud are based on the assumption of intentional human conduct. In cases where AI systems independently execute harmful actions, such as automated hacking tools or self-learning malware, identifying the responsible human actor becomes extremely difficult. This creates a significant enforcement challenge for investigative agencies and courts.

The role of intermediaries under the IT Act is particularly important in the context of AIgenerated content. Platforms that host or transmit AI-generated material may be held liable under Section 79, but only if they fail to observe due diligence requirements. However, with the rise of generative AI systems that automatically produce text, images, and videos, determining intermediary responsibility becomes increasingly complex. It is often unclear whether the platform is merely hosting content or actively contributing to its generation through AI tools.

Another limitation of the IT Act is its lack of provisions addressing algorithmic accountability and transparency. AI systems can generate harmful outcomes such as deepfakes, misinformation, and automated fraud without direct human input at the time of offence. The Act does not provide a clear mechanism to regulate or penalise such autonomous outputs, leading to ambiguity in enforcement. This gap becomes more pronounced in cases involving large-scale AI-driven cyberattacks or coordinated digital manipulation campaigns.

The evidentiary challenges under the IT Act also complicate AI-related prosecutions. Digital evidence must be traced back to a specific device, user, or account, but AI systems often operate across distributed networks and cloud-based infrastructures. This makes it difficult to establish ownership or control over the offending action. As a result, even when harm is clearly caused, linking it to a legally responsible entity under the IT Act becomes problematic.

Overall, while the Information Technology Act provides an essential framework for combating cybercrime in India, it is not adequately equipped to handle the complexities introduced by Artificial Intelligence. The absence of AI-specific provisions, combined with challenges of attribution, transparency, and causation, highlights the urgent need for legislative updates. Strengthening the IT Act or introducing dedicated AI regulation would be necessary to ensure effective legal control over emerging forms of cyber and AI-generated crimes.

1.3 Data Protection and Privacy Laws

Data protection and privacy laws play a crucial role in regulating Artificial Intelligence systems because AI fundamentally depends on large volumes of personal and non-personal data for training, learning, and decision-making. In India, the Digital Personal Data Protection Act, 2023 represents a significant step toward establishing a structured framework for safeguarding personal data.

However, while the Act addresses issues of consent, data processing, and data fiduciary responsibilities, it does not explicitly deal with criminal liability arising from AI-generated harm. This creates a gap between data governance and criminal accountability in cases where misuse of data by AI systems leads to unlawful outcomes.

Artificial Intelligence systems often process sensitive personal data, including biometric information, behavioural patterns, financial records, and location data. The misuse or unauthorised processing of such data can result in serious violations of privacy rights. However, when such violations occur through autonomous AI systems, determining liability becomes complex. It is often unclear whether responsibility lies with the data fiduciary, the AI developer, the deploying organisation, or the end user, especially when the system operates independently based on learned data patterns.

A major concern in AI-driven data processing is the issue of informed consent. Traditional data protection frameworks assume that individuals provide clear and informed consent for the use of their data. However, in AI systems, data is often collected indirectly, aggregated from multiple sources, and used for purposes beyond the original scope of consent. This raises legal and ethical concerns, particularly when AI systems generate outputs that harm individuals, such as profiling-based discrimination or identity misuse.

Another important aspect is data bias and algorithmic discrimination, which can lead to harmful consequences even without direct human intent. AI systems trained on biased datasets may produce discriminatory results affecting employment, credit scoring, law enforcement profiling, and access to services. While such outcomes may violate principles of fairness and equality, existing data protection laws do not clearly assign criminal liability for algorithmic bias, making enforcement difficult.

Cross-border data flows further complicate the application of privacy laws in AI-related contexts. Many AI systems operate on global cloud infrastructure, where data is processed in multiple jurisdictions. This raises questions about which legal system applies when a data breach or AI-generated harm occurs. The absence of harmonised international data protection standards increases uncertainty in assigning liability and enforcing legal remedies.

Overall, while data protection and privacy laws provide an essential regulatory foundation for safeguarding individual rights in the digital age, they are not sufficient to address the complexities of AI-generated crimes. The intersection of AI autonomy, large-scale data processing, and algorithmic decision-making requires more comprehensive legal mechanisms that integrate privacy protection with clear standards of criminal accountability.

1.4 International Legal Approaches to AI Liability

Internationally, there is no uniform legal framework specifically governing criminal liability for Artificial Intelligence, but several jurisdictions and regulatory bodies have developed different approaches to address AI-related risks. The European Union has taken a leading role through its proposed Artificial Intelligence Act, which adopts a risk-based classification system for AI applications. High-risk AI systems are subject to strict compliance requirements, including transparency, accountability, and human oversight. However, even in the EU framework, criminal liability is still largely dependent on national laws rather than a unified supranational criminal code.

The United States follows a sector-specific and innovation-driven approach, relying on existing legal frameworks such as tort law, consumer protection laws, and cybersecurity regulations to address AI-related harms. There is no comprehensive federal AI legislation that directly defines criminal liability for AI systems. Instead, liability is generally imposed on developers, companies, or users based on negligence, product liability, or intentional misuse. This

fragmented approach creates flexibility but also leads to inconsistency in enforcement across different states and sectors.

In the United Kingdom, regulatory efforts focus on principles such as fairness, accountability, and transparency, with regulatory guidance issued by agencies rather than strict legislative provisions. The UK approach emphasises adaptive regulation, allowing existing laws to be interpreted in the context of AI technologies. However, like other jurisdictions, it still relies on human-centric liability models and does not recognise AI as an independent legal subject for criminal responsibility.

International organisations such as the OECD and the United Nations have also contributed to the development of ethical guidelines and policy frameworks for Artificial Intelligence. These frameworks emphasise human rights protection, safety, transparency, and accountability in AI development and deployment. However, they remain non-binding in nature and do not establish enforceable criminal liability standards. As a result, their impact is limited to policy guidance rather than legal enforcement.

A common feature across most international approaches is the rejection of direct criminal liability for AI systems themselves. Instead, responsibility is consistently traced back to human actors such as developers, operators, or organizations deploying the technology. This reflects the global consensus that AI, at least in its current form, should not be treated as a legal person capable of bearing criminal responsibility. However, this approach also highlights the difficulty of addressing autonomous decision-making systems within traditional legal structures.

Overall, international legal approaches to AI liability reveal a fragmented and evolving regulatory landscape. While significant progress has been made in establishing ethical and riskbased guidelines, there remains a lack of uniformity in addressing criminal liability for AIgenerated harm. This reinforces the need for coordinated international legal standards that can effectively bridge the gap between technological advancement and criminal accountability.

1.5 Judicial Trends and Case Laws

The judicial approach toward Artificial Intelligence and AI-generated crimes is still evolving, as courts across jurisdictions are increasingly confronted with technological disputes that challenge traditional legal principles. Although there are limited direct judicial precedents specifically addressing AI-generated crimes, courts have played a significant role in interpreting existing legal doctrines in the context of emerging digital technologies. The judiciary generally relies on established principles of criminal liability, such as intention, causation, and foreseeability, to extend existing laws to new technological situations involving Artificial Intelligence systems.[7]

In India, courts have consistently adopted an interpretative and expansive approach when dealing with technology-driven disputes. In cases such as **Shreya Singhal v. Union of India (2015)**, the Supreme Court emphasized the importance of protecting fundamental rights in the digital space while also clarifying the limits of intermediary liability.

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

Although not an AI-specific case, it is relevant in understanding how courts deal with online platforms that may host algorithmically generated or user-driven content. Similarly, in **K.S. Puttaswamy v. Union of India (2017)**, the recognition of the right to privacy laid a strong foundation for regulating data-driven technologies, including AI systems that rely heavily on personal data processing. [8]

The principle of liability for hazardous or high-risk activities has also been judicially developed in cases such as **M.C. Mehta v. Union of India (Oleum Gas Leak Case, 1987)**, where the Supreme Court introduced the doctrine of absolute liability. This principle is particularly relevant in AI-related contexts, as it suggests that entities engaged in inherently risky technological activities may be held strictly responsible for harm caused, regardless of intent or negligence. This judicial reasoning provides a potential framework for addressing AI generated harm in the absence of specific legislation. [9]

Courts have also dealt with issues of causation and foreseeability in criminal law, which are central to AI liability debates. In **Jacob Mathew v. State of Punjab (2005)**, the Supreme Court clarified the standards for criminal negligence, emphasizing the need for a gross deviation f[2]rom reasonable care. This becomes relevant in AI cases where developers or operators may be held liable if they fail to exercise adequate caution in designing or deploying AI systems. However, applying these standards to autonomous systems remains challenging due to the unpredictable nature of AI decision-making. [10]

2. Critical Analysis on academic literature on Ai Criminal liability

Criminal liability in terms of Artificial Intelligence has also attracted considerable academic attention as far as the limitations of traditional approaches towards addressing issues associated with autonomous decision-making systems are concerned. The classical criminal law theory of actus reus and mens rea is applicable only to human beings who engage in illegal activity with intention. This poses challenges to applying criminal liability to Artificial Intelligence as this system does not possess consciousness or moral awareness.[11]

In one of the most discussed theories, the author presents three models of criminal liability: (i) perpetrator-via-another, in which Artificial Intelligence is an innocent agent, (ii) naturalprobable-consequence model, in which criminal liability arises in connection with expected results and (iii) direct criminal liability model, in which Artificial Intelligence is

[8] *K.S. Puttaswamy v. Union of India (2017) 10 SCC 1*

[9] *M.C. Mehta v. Union of India (Oleum Gas Leak Case, 1987) 1 SCC 395*

[10] *Jacob Mathew v. State of Punjab (2005) 6 SCC 1 precedents highlights the urgent need for legislative intervention to provide clear guidance on criminal liability in the context of Artificial Intelligence*.

[11] Andrew Ashworth, *Principles of Criminal Law* (9th edn, OUP 2021) 85–92

recognized as the offender.[12] Even though the suggested approach has a number of interesting ideas, it has

faced some criticism. Namely, the proposed framework was criticized as being too theoretical to be applied to real legal cases since punishment could hardly be applied to Artificial Intelligence.

However, some academics, such as Ugo Pagallo, oppose the notion of giving AI legal personalities. The stance is that legal systems should have a human focus since any liability would lie on those responsible for designing, creating, and implementing the technology.[13] This perspective is more consistent with the current laws and sidesteps the complications involved in recognizing AI as a separate legal personality.

Also essential is Ryan Calo's work on regulatory gaps caused by new technological advances. It holds that the law is typically unable to keep up with innovations, resulting in cases of illegal behavior that exist outside the legal purview.[14] This idea is significant regarding AI crimes committed since neither the Indian Penal Code nor the Information Technology Act is sufficient for handling autonomous technology.

Moreover, the concept of distributed responsibility has been extensively analyzed by scholars such as Thomas Weigend.

Despite these different positions, however, a general trend can be observed within the literature, suggesting that scrapping all traditional doctrines is neither feasible nor appropriate. Instead, what needs to prevail is the combination of traditional doctrines and AI-specific legislation. This way, continuity in law will be maintained while still ensuring adaptation and responsiveness to changes in technology.

Within the context of India, this issue gains even more significance given the lack of proper AI legislation. Although the Digital Personal Data Protection Act aims at solving the problem of data protection, it does not settle the matter of criminal responsibility. In light of this, the engagement with scholarly works shows how important it is to have the proper legislation in place.[15]

As far as I am concerned, following an entirely human-centered model of liability is neither feasible nor legally acceptable, especially in the context of an emerging legal jurisdiction such as India. Instead, what might work better is a mixed model whereby liability can remain humanfocused yet technologically backed.

[12] Gabriel Hallevy, *When Robots Kill: Artificial Intelligence under Criminal Law* (Northeastern University Press 2013) 45– 63.
[13] Ugo Pagallo, *The Laws of Robots* (Springer 2013) 117–125.

[14] *Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103 California Law Review 513.*

[15] *Digital Personal Data Protection Act, 2023* (India).

Conclusion

Artificial Intelligence is no longer a future concept; it has already become a part of everyday life, influencing decisions, systems, and even human behaviour in subtle but powerful ways. While it has brought efficiency and innovation across sectors, it has also created new forms of

---

risk that the traditional legal system was never designed to handle. This study has shown that the existing legal framework, particularly laws such as the Indian Penal Code and the Information Technology Act, continues to rely heavily on human intention, control, and direct causation. These assumptions do not always hold true in the case of autonomous or semiautonomous AI systems.

One of the key issues that emerges is the difficulty in assigning criminal liability when harm is caused without clear human intent. Unlike traditional offences, AI-related crimes often involve multiple actors, indirect control, and evolving system behaviour. This makes it challenging to apply established principles such as mens rea in a straightforward manner. At the same time, completely shifting liability onto AI systems themselves is neither practical nor legally viable, as AI lacks consciousness, moral judgment, and the capacity to be punished.

The analysis of academic literature further highlights that there is no single agreed solution to this problem. While some scholars advocate for recognising AI as a legal entity, others strongly reject this idea and instead support a human-centric approach to liability. The more balanced view appears to be a hybrid model, where responsibility is primarily attributed to human actors—such as developers, operators, or organisations—while also introducing regulatory safeguards to address the unique risks posed by Artificial Intelligence.

From an Indian perspective, the situation becomes more pressing due to the absence of a dedicated legal framework addressing AI-related criminal liability. Although developments such as the Digital Personal Data Protection Act mark progress in the area of data governance, they do not fully resolve the challenges posed by autonomous systems. There is a clear need for legislative reform that goes beyond adapting existing laws and instead directly engages with the realities of AI-driven harm.

In conclusion, the law is currently trying to fit a rapidly evolving technology into an outdated framework. While judicial interpretation and existing statutes provide temporary solutions, they are not sufficient in the long run. What is required is a forward-looking approach that combines legal clarity, technological understanding, and policy innovation. In my view, the most practical path forward is not to replace traditional legal principles entirely, but to adapt them thoughtfully while introducing specific provisions that address accountability in the age of Artificial Intelligence. Only then can the legal system effectively balance innovation with responsibility and ensure justice in an increasingly automated world.

Consumer Protection Authorities

References

1. *Ashworth, Andrew, Principles of Criminal Law (9th edn, OUP 2021).*
2. *Hallevy, Gabriel, When Robots Kill (2013).*
3. *Pagallo, Ugo, The Laws of Robots (2013).*
4. *Calo, Ryan, Robotics and the Lessons of Cyberlaw (2015).*
5. *Digital Personal Data Protection Act, 2023.*
6. *K.S. Puttaswamy v Union of India (2017).*
7. *M.C. Mehta v Union of India (1987).*
8. *OECD AI Principles (2019)*
9. *Digital Personal Data Protection Act, 2023 (India).*