The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

MENS REA IN CYBER CRIMES UNDER BHARTIYA NYAYA SANHITA: CAN ARTIFICIAL INTELLIGENCE COMMIT CRIME?

~ Riya Marathe[1]

Introduction:

Artificial Intelligence (AI) has moved beyond the realm of science fiction. AI-powered technologies are now integrated into various areas, such as autonomous cars, facial recognition, financial markets, healthcare, law enforcement, and military activities. As these systems make decisions that impact real-life situations, issues of responsibility arise, especially when an AI's actions cause harm. For instance, if a self-driving vehicle causes the death of a pedestrian or an algorithm wrongly identifies an innocent person as a suspect, who should be held criminally responsible? Is it possible for a machine to have the "intent" to commit a crime? This challenge calls into question fundamental principles of criminal law, particularly the concept of mens rea; the mental state that establishes guilt.[2]

The incorporation of AI has brought about a type of technological opacity, often called the “black box” issue, where even the creators might not completely grasp how an AI system reaches a specific decision[3]. This is especially troubling in areas like law enforcement, where AI-driven surveillance, facial recognition, can lead to negative outcomes for people without any obvious person to hold accountable. The risks are even greater in a democracy like India, where laws and

[1] Third Year BBA LLB(Hons) student at MIT World Peace University, Kothrud, Pune

[2]Andreas Matthias *When Robots Kill: Artificial Intelligence under Criminal Law* 7 (2013);, The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata, 6 Ethics & Info. Tech. 175 (2004).

[3] Genna Burrell, *How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms*

policies need to guarantee that technological progress does not compromise civil liberties or fundamental rights.

With more than 800 million internet users and a swiftly digitizing economy, India's legal system now faces the challenges posed by machine autonomy, accountability, and the critical need for protective measures. The increasing dependence on AI-powered systems in both public and private sectors calls for a reconsideration of criminal law principles originally created for human wrongdoers[4]. This article seeks to examine whether current legal frameworks are capable of determining responsibility when it becomes unclear who or what is responsible for the wrongful act.

The Indian legal system, similar to many others, is fundamentally centered around humans. It assumes human actions, feelings, and ethical judgment. However, AI technologies, particularly those driven by machine learning, function based on data inputs, probabilistic results, and neural networks instead of conscious decisions. This creates an increasing gap between legal principles and technological realities, causing difficulties for courts and lawyers in determining responsibility in a world influenced by AI.

An Analytical Definition of Cybercrime:

There is no unanimous agreement among experts on a universal, all-encompassing definition of cybercrime.[5] The main reason for this lack of consensus is that scholars have been unable to establish clear criteria to distinguish between real-world crime and cybercrime. Theoretically, a provisional distinction can be made by assuming that a crime qualifies as cybercrime if at least one element of the offense takes place in cyberspace. Susan

[4] Rashida Richardson, Jason M. Schultz & Kate Crawford, Dirty Data, *Bad Predictions: How Civil Rights Violations Impact Police Data*, 94 N.Y.U. L. Rev. Online 15, 20–21 (2019)
[5] Kirsty Phillips et al., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, 2 Forensic Sci. 379–398 (2022)

W. Brenner has effectively illustrated the conceptual connection between crime and cybercrime using the following equation:

Cybercrime = Cyberspace + Crime

It is a widely accepted proposition that the basic elements of crime are mens rea and actus reus. It can also be reduced to the following equation:

Crime = Actus Reus + Mens Rea

If the two equations are combined together, the following equation will be generated: - **Cybercrime = Cyberspace + (Actus Reus + Mens Rea)**

Mens rea refers to the criminal's mental state and is theoretically always present within the mind of the offender. Therefore, mens rea cannot exist in cyberspace. For an offense to be deemed a cybercrime, the actus reus must take place in cyberspace. Often, actus reus involves multiple actions. It is thus suggested that a crime should be classified as a cybercrime only if both of the following conditions are met: (a) one or more of the actions that make up the actus reus occur within cyberspace; and (b) the actus reus is completed in cyberspace

This analytical method for understanding cybercrime can be better illustrated by looking at examples such as online fraud/theft and online defamation. For instance, in a case of online fraud/theft, a criminal illegally obtains the victim’s internet banking login details from a physical notebook where the victim had written them down. This illegal act of acquiring the login information is part of the actus reus (the physical element) of the crime, but it takes place in the physical world, not in cyberspace. Next, the criminal uses the stolen login details to access the victim’s online bank account and transfers money to another account electronically. This act of transferring money, which is also part of the actus reus, happens within cyberspace. Moreover, the wrongful act of transferring money is completed entirely within cyberspace, as the crime is considered complete once

the money has been transferred. Therefore, according to the proposed framework, this particular offense qualifies as a cybercrime.

Judicial Interpretation of Mens Rea in Section 66 of the Information Technology Act,2000

The judiciary has consistently highlighted that the presence of "dishonestly" or "fraudulently" is a necessary condition for an offence under Section 66. This is notably different from some other provisions, like the former Section 66A, which was invalidated due to its vagueness and lack of clear definitions of offences.

In the significant case of *Shreya Singhal v. Union of India*[6], which primarily addressed the constitutionality of Section 66A, the Supreme Court implicitly supported the framework of Section 66. The Court pointed out that Section 66, unlike Section 66A, uses clearly defined terms such as "dishonestly" and "fraudulently," which have established legal meanings under the Bhartiya Nyaya Sanhita (BNS). The judgment stated, "It will be clear that in all computer-related offences mentioned in Section 66, mens rea (criminal intent) is a component, and the terms 'dishonestly' and 'fraudulently' are defined with some specificity, unlike the terms used in Section 66A." This highlights the legislature’s intention to punish only those actions under Section 43 that are carried out with a definite criminal mindset.

The Supreme Court further clarified the importance of proving dishonest intent in the case of *Ramesh Rajagopal v. Devi Polymers Pvt. Ltd*[7]. Here, allegations under Section 66 read with Section 43 involved the creation of an allegedly false electronic record on a website. The Court dismissed the charges under Section 66, noting that "there is no evidence to show that he lacked authority to access

[6] AIR 2015 SC 1523
[7] (2016) 6 SCC 310

the company's computer system or network. Moreover, there is no evidence of an offence under Section 65 of the IT Act. It was already observed that the appellant's actions did not involve any dishonest intention when considering other allegations. Therefore, no case is made out under Sections 65 and 66 of the IT Act, 2000." This ruling firmly establishes that without dishonest or fraudulent intent, Section 66 does not apply, even if an act under Section 43 has taken place.

Complications In Applying Mens Rea To Autonomous Systems:

Artificial intelligence inherently disrupts the conventional structure of criminal law. Unlike humans, machines do not develop intentions, experience emotions, or anticipate consequences in the same way. Their "decisions" result from algorithms rather than conscious will[8]. This makes applying the concept of mens rea to autonomous systems more complex. For example, if an AI-powered drone causes a wrongful death during a surveillance mission, assigning intent becomes both legally and jurisprudentially challenging.

Three main theories have been put forth by academics to address AI and criminal liability: the tool model, the agent model, and the hybrid model. Because AI is seen as an extension of the human user, the tool model holds operators, programmers, and designers accountable for any illegal consequences. Liability for misusing weapons or animals is comparable to this.

The agent model treats AI as a quasi-legal person, capable of limited autonomy and thus deserving of distinct accountability. This model is controversial because it implies recognition of some form of machine agency. The hybrid model suggests shared liability, where both human actors and AI systems bear differentiated responsibilities.

For India, the tool model appears most consistent with existing legal doctrines. Holding developers or users liable under negligence or vicarious liability

[8] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap* (2017)

principles would help in making them accountable without reworking the basis idea of mens rea[9]. However, this model fails when AI evolves beyond its programming or learns new behaviours autonomously through Large Language Models (LLMs).

Recommendations on bridging AI and criminal liability in India:

To successfully address the existing gap in regulations pertaining to AI and its potential criminal implications, India needs to implement a comprehensive strategy that incorporates proactive legislation, changes in institutions, and ethical frameworks. To begin, the Indian legislative body should deliberate on passing specific legislation that deals with responsibility in AI, clearly specifying the entitlements and duties of those who create, manage, and use AI. This legal framework needs to precisely define significant concepts like damage caused by algorithms, independent choices made by machines, and authority in the digital space to prevent uncertainty in interpretation.

Subsequently, the implementation of a strict accountability system could be initiated for AI uses that carry substantial risks, such as self-driving automobiles or facial identification tools used by policing agencies. This action would transfer the responsibility of proof from the person affected to the organization deploying the technology, thereby guaranteeing a fairer application of justice. Using concepts from environmental law, where parties responsible for pollution are held accountable regardless of their intentions, this strategy could give precedence to preventing harm over determining subjective fault.

In addition, it is essential to formalize openness by requiring evaluations of algorithmic impact through legal mandates. These evaluations should analyze the possible social, financial, and legal repercussions of using AI systems and should be available for public viewing. Self-governing regulatory agencies possessing

[9] Andreas Matthias, *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning* (2004)

specialized technical knowledge should be authorized to examine these evaluations and impose penalties for failures to comply.

Lastly, methods for safeguarding data must advance at the same rate as AI regulations. While the DPDP Act creates a base for permission and decreasing data usage, it does not have strong regulations regarding biases in algorithms, creating profiles, and discrimination[10]. Changes to the law should include defences against unclear handling of data particularly in circumstance where decisions are made automatically.

Conclusion:

India stands on the verge of a significant technological shift, necessitating an equivalent evolution in its legal structures. The core question revolves around whether our legal system can adapt to the changing dynamics of accountability and ownership, rather than focusing on the possibility of AI committing a crime. The legal system should persistently function as both a protective measure and a directional tool, guaranteeing that technological advancements do not compromise human rights and the essence of democratic principles. An elaborately designed and fundamentally guided strategy towards AI and criminal culpability will ascertain that India excels not only technologically but also in fairness and inclusivity.

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