



# Criminal Liability of Artificial Intelligence: A Comprehensive Analysis of Legal Issues and Emerging Challenges

Teena Arora<sup>1</sup>, Dr. Shailja Thakur<sup>2</sup>

<sup>1</sup>LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

<sup>2</sup>Assistant Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

## ABSTRACT

The seemingly growing adoption of AI in drastically boosted various industries and sectors and has created crucial questions to the existing criminal law responsibility concepts rooted in mens rea and actus reus. When autonomous and stochastic AI systems operate at their own discretion, current laws—Bharatiya Nyaya Sanhita included—suffer from a lack of specificity. This paper explores the issue of legal accountability for AI, arguing as to whether AI is capable of forming an intention to commit a particular act or not. Finally, it considers the European Union's risk-based approach and notions of electronic personhood as possible global regulatory measures to address these problems. The study urges the Indian government to come up with legal structures that complement AI development by coming up with risk categorization, compulsory disclosures, as well as the formation of an AI ethical governance body to address issues with accountability. Such measures include having strict liability for developers and operators, disclosure of use cases with high-risk components, and limited electronic personhood for particular AI entities. While India faces such challenges, we deserve an integrated approach that equally aspires to accountability without killing innovation. To do so, India has to enhance progressive regulatory mechanisms that ideally respond to the legal challenges the AI AI-driven actions and at the same time protect the public interest while promoting innovation on the other.

**Keywords** Artificial intelligence, criminal liability, Bharatiya Nyaya Sanhita, mens rea, actus reus, AI ethics, liability attribution, electronic personhood, transparency

## 1. INTRODUCTION

In the constantly changing environment, a previously unfamiliar subject such as AI has quickly found its field of application in everything, including technology and law, and creates difficult and relevant issues. Of these, one of the most complex and universal issues is the problem of criminal liability for actions carried out by AI systems independently. What used to remain as an academic question has turned into an actual question with practical questions arising as to how we are going to solve them now for policymakers, legal scholars, corporate entities, and the general population. When an AI system is a component of an appliance that makes its decision and operates independently, such as self-driving cars, robotic health care support, and automated financial consultants, then risks arise. However, there is no comprehensive legal pattern for apportionment of criminal responsibility to AI in India or globally to this date. <sup>1</sup>Liability for AI blurs the lines of ordinarily understood cause and effect and therefore presents substantial questions of justice and ethics to the mainstream understanding of the preventive measures part of the criminal law. It is important to discover how key legal ideas, such as intent, mens rea, and actus reus, pertain to—or do not pertain to—AI since such systems can occasionally function autonomously and eccentrically.<sup>2</sup>

For instance, the emergence and growth of such things as surveillance and a new and enhanced policing system are examples of why it is important to address these matters. As companies look to increase productivity and minimize the role of human interference, AI's capability to inadvertently discriminate or even harm is the new legal and ethical dilemma. The BNS provides standards for liability; it acknowledges culpability and punishment, but such standards are based on rationalistic precepts that presume human purpose, blame, and foreseeable risk. This essential structure, which defines knowledge as responsibility, is problematic due to the autonomy of AI. The least of the BNS criminal responsibility principles are based on mental aspects that AI lacks. AI is not a sentient machine and does not possess 'intent' in the legal sense or 'knowledge' in the human sense, and this means that conventional criminal liability cannot come into operation readily under Indian law as it depends on the doctrine of mens rea. Still, with the spread of

<sup>1</sup> Sadaf Fahim, *Ethico-Legal Aspect of AI-driven Driverless Cars: Comparing Autonomous Vehicle Regulations in Germany, California, and India* 186 (Oxford University Press, Delhi, 1st edn., 2024).

<sup>2</sup> Hifajatali Sayyed, "Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges", 10 *Cogent Social Sciences* 15-34 (2024).

autonomous AI systems in all segments of society, pursuing common law that regulates such systems became crucial.<sup>3</sup> 280 (Routledge, London, 1st edn., 2020).

At present, the criminal responsibility in India has been laid down on the two doctrines of the law; namely mens rea and actus reus. The concepts on which the Foundation of criminal liability in the Bharatiya Nyaya Sanhita is based, are anthropocentric, and it is difficult to generalize human concepts of criminals to non-human actors such as AI. Consequently, legal blame for the autonomous actions of AI remains in a state of legal uncertainty. Internationally, other jurisdictions have also faced this question and the solutions have been presented in a spectrum from proposals of making AI as a legal person to holding liability with the developers only. Reflectively, the AI draft regulation of the European Union has set the precedence for apportioning some degree of responsibility on the AI entities. Nevertheless, the question pops up, particularly in Indian law, as technological distances in AI advance faster than the law to govern it. Hence, research on likely legal arrangements of AI accountability does not only call for an academic discourse but also a necessity for today's criminal justice.<sup>4</sup>

---

## 2. CONCEPTUAL FRAMEWORK OF CRIMINAL LIABILITY

The very notion of criminal responsibility extant for centuries of legal culture is based on the principles that presuppose human actors as rational controlling responsible for wrongful actions. Criminal responsibility implies a mental factor that can be intention, knowledge, or recklessness and a physical one that will cause harm or unlawful results. This framework is captured by baseline principles such as the mens rea (the mental component of a crime) and the actus reus (the physical ingredient). But as AI assumes a more institutionalized towed defining the legal framework for corporate organizations is quite challenging and while with the current trends of AI as an almost self-acting force in society, its incorporation into the contemporary criminal liability law poses complications that are still not fully apprehended by the existing legal systems. From the perspective of criminal justice, the problem is that AI systems, which are capable of working without human intervention, are anthropocentric by definition.

### 2.1 Traditional Criminal Liability Principles

Conventional criminal responsibility is tightly connected with human activity and ethics. In the Bharatiya Nyaya Sanhita (BNS) and other existing criminal laws from around the world, the blame for crimes as well as criminal responsibility lies with a rational, voluntary control of the actions of a defendant. For example, in situations of murder or robbery, the legal system believes that agents have knowledge of the function of such activities, and are in a position to change from such a function. This kind of assumption is in tandem with retributive justice theories of punishment to penalize an offender as well as to punish him as the moral consequence of his negligent misconduct. Some parts such as "Section 100" of the BNS which deals with culpable homicide assume intention or knowledge of death, and this supports the view that people have a natural appreciation of the consequences of their actions.<sup>5</sup>

### 2.2 Mens Rea and Actus Reus: Key Components of Criminal Liability

The doctrines of mens rea and actus reus remain some of the most important parts of criminal responsibility. Men's rea means the principle of the guilty mind or the mental element that forms part of the actus reus of the offense. Before a person is found criminally responsible for a wrongful act there must be proof of the elements of the unlawful act (actus reus) coupled with the required state of mind as criminal responsibility. According to "Section 100" of the BNS, in India, intent or lack of it to commit a particular offense together with knowledge thereof forms the basis of a person being accused of a crime.

However, AI systems do not have mens rea as they are not conscious, do not have emotions, or have no moral compass. Though higher-level AI can mimic a reasoning process, such actions are the consequences of computer programming and not actual intent. Self-driving cars do not 'choose' to run a red light or kill a pedestrian as a human car driver does; instead, actions follow the data fed into the machine and real-time calculations. Therefore, when it comes to using AI's ability to create actus reus without mens rea this brings a challenge in an endeavour to apply traditional criminal liability principles. This problem is even aggravated by what may be termed the learning feature: with systems adapting as they progress in terms of the data, they are fed. While operating conventional machines, one can blame a certain act by an individual or a decision by a certain programmer for a wrongful act to happen because the machines do not display these quirks that AI systems do. Such complexities mean that the organization of an AI system does not correspond with the distinction made in criminal law between men's rea and actus reus, creating legal problems in determining criminal responsibility.

### 2.3 Challenges in Applying Traditional Liability to AI Systems

Examining the AI systems through traditional criminal liability highlights conceptual difficulties, basically stemming from the disparity between how the criminal law works, and how it is employed by the AI system. First of all, AI currently does not possess qualities that belong to the quality mens rea:

---

<sup>3</sup> Dennis J. Baker & Paul H. Robinson, *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*

<sup>4</sup> Nora Osmani, "The Complexity of Criminal Liability of AI Systems", 14 *Masaryk University Journal of Law and Technology* 53 (2020).

<sup>5</sup> Thomas C. King, Nikita Aggarwal, et. al., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", 26 *Science and Engineering Ethics* 89-120 (2020).

intention or knowing cannot be attributed to an entity that is not conscious or moral. Consequently, AI cannot 'intend' something in the legal sense, as is an essential ingredient under Indian criminal law. For example, when a self-driving car causes an accident and someone dies, apportioning responsibility can become complicated; the AI system does not know that it is endangering lives. Many traditional legal attempts at remedy making

– like those envisaged under 'Section 106' of the BNS and which pertain to death by negligence

– do not adequately include AI because negligence suggests a human's inability to exercise reasonable care – an appreciably human weakness.<sup>6</sup>

Thirdly, the very way that AI learns compounds the problem of accountability. Most of the AI systems employ advanced formulas that transform over time which could mean unpredictable consequences. This unpredictability creates a dilemma: When, for example, an AI system makes a decision on its own and crime or harm occurs as a consequence, the question of who is responsible – the programmer, the end user, or the AI system – is contentious. Furthermore, merely the concept of making an AI system legally responsible is absurd under modern law, or punishment hence deterrence, two aims of criminalization, cannot be applied to a physical object. Punishment is meant for human offenders making it impossible for AI to learn a lesson say from punishment or endure the same way imprisonment is endured by human beings.<sup>7</sup>

### 3. TYPES OF AI-RELATED OFFENSES AND POTENTIAL LIABILITIES

AI-related offenses vary from minor offenses to actual physical harm offenses or even economic-related offenses. The increased complexity of AI systems means that an ever-wider range of possibilities can be considered to be a potential area of liability, including both direct and indirect damages. A subcategory based on the offenders is the self-driving cars that from time to time have led to fatal crashes. For instance, self-driving cars could quickly make decisions causing injuries, say when the AI system has gotten a wrong estimate of a traffic scenario. In such events; it becomes legally challenging to identify who is legally responsible relating to the manufacturer of the particular vehicle, the developer of particular software, or the own social responsibility. Based on the principles of product liability laws, manufacturers and developers are usually held legally liable for system failures, however, these laws do not fully protect against scenarios resulting from AI's self-acting characteristics.<sup>8</sup>

Another way that AI may create risk across sectors is that the AI algorithms themselves might make decisions resulting in unfair or negative outcomes, for example for persons of colour or women in law enforcement or within health care. An example of some of the brave new technologies that have received backlash include; predictive policing where it was accused of propping up racism and classism. In India, and more so given the significant social diversity existing in the country, any tool that implements artificial intelligence for policing or hiring, and at the same time discriminates in a manner that it did based on the sample results, then it would be open to the possibility of legal challenge under the discrimination laws of the country. Although not necessarily criminal per se these biases pose questions of legal accountability from civil liability laws to human rights laws.

However, former types of cyber offenses aided by AI include a new form of risk classification. Criminals also deploy artificial intelligence technology in programs that engage in using the bot to perform DDoS attacks and phishing scams, for instance. The various kinds of cyber offenses that exist under Indian law fall under Section 66 of the Information Technology Act, 2000, and Section 43 of the Information and Technology Act, 2008 which still do not recognize or prohibit AI cyber-attacks. When the system is programmed to change its ways and means of hacking without human interference, apportioning responsibility for the losses is not easy. The developers may claim that the AI worked beyond its capabilities while the victims may likely claim that the developers are fully to blame. The employment of AI in crime makes calls for subsequent legal reforms that can fit into the kind of scenarios depicted above.<sup>9</sup>

### 4. LEGAL ISSUES IN ESTABLISHING AI CRIMINAL LIABILITY

Introducing criminal liability of AI raises a host of legal issues using such ideas as accountability or lack of it, legal concerns, and the question of the legal subjectivity of AI. Indian law especially written law traditionally assumes human actors and thus poses great challenges when it comes to shifting to a complicated structure of an informed autonomous system. Another problem that emerges is when AI assumes operational command; this paper addressed another fundamental concept in criminal law, known as accountability.<sup>10</sup>

<sup>6</sup> Sheshadri Chatterjee and Sreenivasulu N.S., "Artificial Intelligence and Human Rights: A Comprehensive Study from Indian Legal and Policy Perspective", 10 *International Journal of Law and Management* 94 (2021).

<sup>7</sup> Jennifer Cobbe & Jatinder Singh, "Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges", 42 *Computer Law & Security Review* 579 (2021).

<sup>8</sup> Chidiogo Uzoamaka Akpuokwe, et. et., "Legal Science & IT Research Journal Challenges of Artificial Intelligence and Robotics: A Comprehensive Review", 5 *Computer* 546 (2024).

<sup>9</sup> Fatima Dakalbab, Manar Abu Talib, et al., "Artificial Intelligence & Crime Prediction: A Systematic Literature Review", 6 *Social Sciences & Humanities Open* 142 (2022).

<sup>10</sup> Report on Criminal Liability, Robotics & AI Systems, available at: <https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2021-02/2021%20Report%20on%20Criminal%20Liability%20Robotics%20&%20AI%20Systems.pdf> (last visited on October 14, 2024).

#### 4.1 Issues of Accountability and Attribution

One of the most significant legal issues in establishing AI criminal liability is the question of accountability: who is to blame when an artificial intelligent system does something that if a man had done it, he would be criminally prosecuted? Conventional legal responsibility in Indian criminal law involves apportioning blame on an individual or a legal person exercising management over conduct resulting in loss or damage. However, with the help of learning algorithms, AI is capable of making decisions independently which quite interferes with the chain of accountability. That is, AI can perform actions outside of the control of any one human, and the question of whether developers, operators, or even the end-users of AI products should bear responsibility for these actions arises. For example, concerning accidents caused by self-driving cars, when a system causes harm a failure mode is typically not readily identifiable as being due to a single flawed design or mode of operation. This paper demonstrates an actual case between a manufacturer and a software developer of a modern car where each party may blame the other as the fault attributions shift the blame to the other weak link in the chain: the manufacturer may claim that the developer should be held responsible for the software flaw, while the developer may accuse the manufacturer of failing to exercise sufficient control over the operator who installed the AI in the car without proper supervision. The dispersal of responsibilities is such that legal loopholes emerge thus making it almost impossible to push forward the actualization of accountability.<sup>11</sup>

More specifically, from a criminal law point of view, one is not usually liable unless one has a “guilty mind” – an intent to engage in criminal conduct. However, AI, basically being devoid of consciousness or any form of intent, can only lack the real mens rea. For instance, the deaths that occurred due to homicide or injury by a self-driving car, recent occurrence of the same in other jurisdictions, leads to a problematic attempt at attributing criminal intent. If Indian courts can never ascertain intent, they would fail to categorize AI actions in “Sections 100” and “106” of BNS of culpable homicide and negligence, respectively. The thinking that underpins these statutes presupposes a power of reason that AI is constitutionally incapable of, and there is no clear answer as to who, if anyone, should be held criminally liable.<sup>12</sup>

11

12

## 5. AUTONOMOUS DECISION-MAKING AND UNPREDICTABILITY IN AI

Automated and autonomous decision-making is another fascinating, though unrealistic from the legal point of view, feature of AI. Cognitive autonomous systems run on sophisticated informatics algorithms that enable them to work with large volumes of information and learn by changing scenarios, without prior instruction from the operator. Despite these being assets in industries such as transport, health, and banking, this capability is disadvantageous because it has raised questions about the volatility of Artificial Intelligence behaviours. As AI systems propose their actions from data inputs they take and change their actions, even to their owners who implemented it becomes challenging to predict what the systems will do. This particular unpredictability presents a massive problem to criminal law, especially since criminal law hinges its attributions of intent and foreseeability on the unpredictability of human behavior. In the present case, they have criticized the provision of “Section 100” of the Bharatiya Nyaya Sanhita which holds a person criminally negligent if the death resulted from the consequence of negligence and there could be a direct causal link, something which autonomous AI disrupts. As the decision-making of AI gets more and more intricate, it results in actions that might cause harm or even criminal outcomes but are hard to plan or prevent.<sup>13</sup>

### 5.1 The Problem of Autonomous AI Acting Beyond Human Control

One other core legal concern arises where carrying out their precise operations fully autonomous of all human activity also has further implications for the legal principle of criminal liability. Legal convention's calendar of expectation assumes that those involved in legal transactions or their representatives act on their own accord and are responsible for their and/or others' behavior. However, due to its autonomic characteristic, AI can perform actions and decide on its own sometimes with astonishing results that (often) go beyond the possibilities or will of its developers. This lack of control is even more worrisome concerning high-risk contexts like self-driving cars, financial platforms, or looming surveillance mechanisms like autonomous weapons, financial trading platforms, or algorithms for predictive policing, where unchecked decision-making could inflict mortal harm.

The absence of control over the actions by artificial intelligence raises the question of agency which forms the basis of many provisions of the Indian criminal law. For instance, under “Section 45” in the BNS, the law encompasses abetment as the support or instigation of another to commit a wrong as founded on the agency of human influence. However, suppose an AI system on its own performs a malicious action that does not serve the purpose for which the AI system was designed; surely, it becomes hard to operationalize such provisions above mentioned. New challenges appear when an AI system

<sup>11</sup> Analysing the Possibility of Imposing Criminal Liability on AI Systems, available at: <https://criminallawstudiesnlj.wordpress.com/2021/01/19/analysing-the-possibility-of-imposing-criminal-liability-on-ai-systems/> (last visited on October 05, 2024).

<sup>12</sup> AI and Intent Data: How Do They Contribute to Full-Blown Intent Intelligence?, available at: <https://www.algolia.com/blog/ai/ai-and-intent-data-how-do-they-contribute-to-full-blown-intent-intelligence/> (last visited on October 05, 2024).

<sup>13</sup> Criminal Liability of the Artificial Intelligence Entities, available at: <https://docs.manupatra.in/newsline/articles/Upload/4e5c9c80-320b-4433-9f87-f56059a5345c.pdf> (last visited on October 05, 2024).

works within the Internet space and affects customers from different countries, which creates problems with exercising control and assigning responsibility. If an AI bot operates independently and autonomously launches a cyber-attack that leads to a great deal of loss and the script does not involve a human actor in the equation somewhere, then trying to prosecute based on extant statutes becomes extremely onerous. Such scenarios raise the issue of how deeply embodied human legal doctrines are insufficient in the face of autonomous artificial intelligence and that criminal law must change to be able to address conduct for which no person is making a decision.<sup>14</sup>

### 5.2 Addressing Foreseeability and Culpability in AI-Driven Crimes

In criminal law, foreseeability has a subsequent significance in the process of punishment as in the cases connected with the questions of negligence or recklessness. In India especially when it comes to “Section 100” of the BNS which relates to culpable homicide the element of foreseeable harm is mandatory in proving intent or knowledge. However, the foreseeability requirement is made difficult to achieve by AI because these systems do not make decisions on their actions in the same manner as other individuals who practice AI systems. But when there is a function or action performed outside the intended capability of the design, it can be immensely challenging to determine if the result was foreseeable and therefore whether or not there is criminal liability.<sup>15</sup>

The unpredictability of the offenses committed by AI means that the legal system has to rethink not only the core of the concept of blame. If an AI system independently harms people — for example, if in identifying a specific person as a threat, the system uses force — then defining who is guilty is a legal question. In such cases, it becomes difficult to measure or apply the common ingredients of knowledge or intent that may be measured under criminal law.<sup>16</sup>

AI has no mind, or at least it does not have one in common with human beings as per the criminal law. Despite recognizing that product liability laws might address some other types of damage, they do not exhaustively offer the criminal aspects of foreseeability and blame in AI-related crimes because the harm to be brought about is not the fruit of volitional action or design but of autonomous adaptation. Indian law at present does not have rules under which the blame can be placed in these scenarios since neither could the AI commit the action nor foresee any of the humans.<sup>17</sup>

Following the advancement of AI technology, the foreseeability and the level of culpability which define the legal norms, should also be developed. All the changes announced make lawmakers and legal scholars debate possible developments that might vary from the creation of new regulatory agencies to overlook the AI operations to developing a new structure of liability that would take into consideration degrees of control and foreseeability. It may be possible to draw on these measures in attempts to navigate situations where the AI’s action results in a crime without input or control from the human operator. In the end, it is only possible to speak about foreseeability and culpability using increased legal responsibility for autonomous AI with the help of new principles that differ from conventional doctrines appropriate for modern society. With the increased uptake of AI in such critical strands of our society, Indian law will be forced to look for innovative ways how it can embrace the new technology while at the same time seeking to punish AI-enabled crimes, which are fully cognizable in the modern world, through the confines of the old legal provisions.<sup>18</sup>

## 6. CONCLUSION

The emergence of AI in our daily lives has left legal scholars grappling with new rules of criminal liability once a loss is occasioned by an autonomous action initiated by an AI system. In India, the Bharatiya Nyaya Sanhita and other criminal statutes accord with traditional mens rea and actus reus, both of which rest on human intent. However, about the AI’s distinctive features including self-functioning, randomness, and lack of premeditation, these notions are not enough. Technological applications, such as AI and robotics, are increasingly being integrated into critical industries, including health, public security, and law enforcement, that are especially susceptible to the negative influence of new technologies and where AI can cause harm; there is a need for liability systems that are capable of grasping the novelties that AI brings into the regulation of technologies.

Analyses of current global trends show different models of addressing AI’s criminal responsibility from the EU, Japan, and Singapore. Implications of such models include a need for an inclusive approach of risk mapping, transparency rules, and ethical standards as indispensable aspects of any regulatory structure for introducing AI in India. Internationally, topics of electronic personhood, and strict liability for developers are potentially promising theories of AI liability, though each faces problems within the Indian legal system.

An effective Indian regulatory approach needs to therefore aim at achieving the two related, but not identical, goals of preventing risk to the public, while at the same time not preventing innovation in the financial sector. Proposed and explained herein is an ‘AI-specific’ framework that should draw from

<sup>14</sup> Artificial Intelligence, Criminal Acts, Criminal Responsibility, available at: <https://theartofcrime.gr/artificial-intelligence-criminal-acts-criminal-responsibility/> (last visited on October 05, 2024).

<sup>15</sup> Accountability of AI Under the Law: The Role of Explanation, available at: <https://doi.org/10.2139/ssrn.3064761> (last visited on October 05, 2024).

<sup>16</sup> Artificial Intelligence: Shift in Liability, available at: <https://blog.ipleaders.in/artificial-intelligence-shift-liability/> (last visited on October 05, 2024).

<sup>17</sup> Vahid Yazdanpanah, Enrico H. Gerding, et. al., "Reasoning About Responsibility in Autonomous Systems: Challenges and Opportunities", 38(4) *AI & Society* (2022).

<sup>18</sup> Artificial Intelligence and Criminal Justice System in India: A Critical Study, available at: <https://www.lawjournals.net/assets/archives/2023/vol5issue4/5123.pdf> (last visited on October 05, 2024).

imperfect International Law, but is situated within the best principles of Indian Law and that primarily anchors its gains to humans. Meeting AI's new challenges with progressive legal frameworks will remain crucial to understanding and governing AI-driven change, fairness, and security in the ever-innovating world.

---

## 7. SUGGESTIONS

The idea of 'AI' criminal liability in India requires a multi-dimensional solution that engages the development of technology with the principles of justice accountability. The following ideas are intended to construct a symmetrical approach to a proper and secure environment for AI applications while maintaining and developing innovativeness.

- Classification of AI and other related autonomous systems is rather essential in Indian law. There is a need to distinguish between the various capabilities, ranging from machine intelligence, machine learning, and fully autonomous systems for ease of interpretation under the law.
- These are Bharatiya Nyaya Sanhita and other relative criminal laws that must include the provision of liability related to AI, regarding the basic concepts of men's rea and actus reus in the context of AI operation. Some of these provisions may enable liability to be shifted to the parties that deserve it whenever harm occurs due to the decisions made by AI.
- Still, using the EU model, India might choose a risk-based regulation where products are divided by the level of risk they might introduce to people. This would make high-risk applications such as self-driving cars and predictive policing even higher risk and closely monitored while certain other systems could be subject to much less regulation.
- To respond to the black box problem, all AI systems that are to be implemented in important industries should be obliged to provide transparency and explainability. This will assist in the creation of and adherence to standards of how AI comes to the decisions it makes, as well as trace the decisions back to the decision-makers and hold them accountable if harm or misconduct has occurred.
- India could set up an AI ethics regulatory commission to coordinate the use and application of AI and to check on adherence to the principles. Such a body could complement the Digital Personal Data Protection Act, 2023 about data protection and mostly to maintain ethical grounding on AI applications.
- Implementing strict liability standards for developers, manufacturers, and operators of AI, especially for self-initiated actions would bring responsibility for AI-caused harm. This approach could be useful in those occasions when it is difficult to establish one guilty 'mind,' simplifying the task to the goal of providing safe design and deployment solutions.
- AI frequently spans the borders of different countries and it makes India develop relations with other countries to reconcile many liabilities of AI through establishing clear structures. This could also be useful in creating cooperation of international natures that would enable the formulation of enforcement systems that work across the globe to deal with artificial intelligence crimes.
- Even if the legal personhood for AI is still a heated topic, India may look into offering limited electronic personhood to some high-risk AI systems. This would permit unique legal personality to some AI entities while at the same time confining legal responsibility to certain actions.
- Judging AI impact assessments before deploying its autonomous systems in sectors needed to avoid risks and liabilities would be helpful. This could help regulators assess the risks of AI systems and the things that might go wrong as well as how to best better integrate this technology into society.
- Since AI technology is dynamic, means that constant legislation revision will be required to fit the current type of technology. The formation of an AI legislative review committee will enhance the capacity of the legislation to phase the laws with the current levels of development in marking the societal interests as well as the technological.

These suggestions are made to form a complete legal structure that is well-equipped to address the issues that are provoked by this advanced technology and it focuses on the public good, responsibility, and flexibility. With clear legislation, ethical supervision, and more importantly, multilateralism India can prepare well to face the challenge of criminal responsibility that artificial intelligence brings.