INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 6 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 6 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-6-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"CRIMINAL LIABILITY FOR AI SYSTEMS: A COMPARATIVE STUDY OF THE UNITED STATES, EUROPEAN UNION, AND INDIA"

AUTHOR – JYOTIKA MAURYA* & DR. LAKSHMI PRIYA VINJAMURI**

* LAW STUDENT, LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN

** PROFESSOR AT LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN

BEST CITATION – JYOTIKA MAURYA & DR. LAKSHMI PRIYA VINJAMURI**,** "CRIMINAL LIABILITY FOR AI SYSTEMS: A COMPARATIVE STUDY OF THE UNITED STATES, EUROPEAN UNION, AND INDIA", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 699-705, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The high rate of adopting artificial intelligence (AI) in the daily routine has created sophisticated legal issues, especially in the area of criminal responsibility. Conventional criminal law paradigms, which have been established on the concept of actus reus and mens rea, have challenges in accommodating autonomous systems, which can make independent decisions. The paper will analyse the problem of criminal responsibility of AI systems by comparing the United States, the European Union and India. It assesses the response of various jurisdictions to questions of attribution, accountability and responsibility in the event of harm caused by AI-powered technologies like chatbots and autonomous robots. The United States still heavily depends on product liability and negligence based on the doctrines, but the European Union is shifting towards a regulatory system based on risk-based responsibility. India, on the contrary, is still a developing country of law in this area. The paper identifies weaknesses in the current legislation and indicates the necessity to have a globally responsive and consistent liability system.

Introduction

Artificial intelligence has become a disruptive element that has revolutionized industries, government, and human communication. The autonomous cars to state-of-the-art chatbots, AI systems can now perform tasks with little or no human participation. Yet, technological progress has been faster than the advancement of law, especially on criminal liability. In situations where AI systems are harmful, such as due to malfunction, bias, or autonomous decision-making, the fundamental question is, who is to be charged criminally?

The classical conception of criminal law is based on human agency, in which either the guilty deed (actus reus) and the guilty state of mind (mens rea) must be found guilty. By being unconscious, having no consciousness or will in the sense of human beings, AI systems are disruptive to such principles. Consequently, current legal principles find it challenging to know who should be held liable (specifically whether it be developers, users, or corporations) or possibly even the AI system itself.

This paper will compare three major jurisdictions namely the United States, the European Union and India. The United States takes a piecemeal method based on tort, corporate, and sector specific regulations. Conversely, the European Union has moved with active actions towards global regulation of AI, focusing more on accountability, transparency as well as risk categorization. Although India is starting to realize the increased significance of AI, it has not developed a solid legal standard in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

which to establish criminal liability in this respect.

Through such contrasting approaches, the paper aims at determining the existing legal gaps and trends. It also seeks to determine whether the current principles are adaptable or new principles have to be developed that would help to respond to this specific situation that artificial intelligence systems present in criminal law.

MAIN BODY

1. The conceptual basis of crime liability and AI.

Historically, the notion of criminal liability has been based on the notion of human culpability. In its most fundamental form, criminal law presupposes two fundamental elements: actus reus (physical act) and mens rea (Intent to commit). All these factors are in place to guarantee that one has both committed a wrong act, and one had a guilty state of mind that led to the imposition of the punishment. Yet, the advent of artificial intelligence (AI) systems does not fit such a conventional structure by presenting agents, who can behave independently without having human mind or will.

The AI systems, specifically advanced machine learning models and autonomous robots, can make decisions based on the data input, algorithms and adaptive learning. These systems are able to vary with time giving their results which might not have been directly anticipated by their intended developers. This brings up a very critical question and that is, may a person or creature, which is not in charge of its own existence, have mens rea? The current legal trend in all jurisdictions is that AI cannot form intent in some traditional sense because AI lacks moral awareness and volition.

Regardless, the fact that we cannot pursue intent liability in the context of AI does not deny the existence of harm that is inflicted by these systems. Autonomous vehicles can lead to accidents, chatbots can be used to commit fraud or defamation, and algorithm systems can be discriminatory. In those situations, a party must still be pointed at in the law. This has contributed to the discussion of other theories of liability, including strict liability, vicarious liability, and approaches on the basis of negligence.

Moreover, the notion of foreseeability is further complicated under the spill of AI. Machine learning developers may not always predict the exact results of the machine learning systems especially those that are based on the self-learning algorithms. Because of this, it is problematic to assign liability on the basis of traditional ideas of foreseeability and control. This makes the reconsideration of the fundamentals of the principles of criminal law necessary to conclude on whether they can be reworked to accommodate AIs-related harms or new legal frameworks need to be created.

2. AI Systems attribution and responsibility problem.

Attribution is one of the greatest problems of regulating AI-related crimes. With AI agents becoming more complex networks of agents, such as developers, programmers, data providers, manufacturers and end-users, there is no clear human agent to identify unlike the traditional criminal activities. The question of which of these actors to be subject to criminal responsibility is very contentious.

The many hands problem can lead to challenges in attitudinal allocation since various individuals are involved in the operation of an AI system. An example is the design of an algorithm by a developer, its implementation by a company, and its application by the user in a specific scenario. When damage has been done it becomes tough to pinpoint where exactly the event of failure has taken place or who to blame. This spreads of responsibility questions the old legal principles that use the idea of individual culpability.

A potential solution to this problem is to shift the responsibility to the party that has the highest level of control over the AI system. In most

instances, however, there is decentralized control instead of a centralized one. Machine learning systems will act in an unpredictable manner particularly because of their capacity to learn new sources of data. This uncertainty makes it even harder to attribute responsibility.

The other method is the liability imposed using the concept of negligence. Within this framework, both developers and operators, that do not use reasonable care in the design, testing, or deployment of AI systems, can be liable. Although this practice is compatible with the current legal principles, it may not be effective in those instances where the harm is caused by the unanticipated AI behaviour.

Other researchers have suggested the concept of making AI systems have legal personhood, and hence have the capacity to be liable on their own. But this offer is not that simple, because it brings up the philosophical and practical issues concerning the punishment, its implementation and the problem of moral responsibility.

Finally, the issue of attribution underscores the shortcomings of the current criminal law developments to handle harms associated with AI. It highlights the necessity of novel legal strategies, which can consider the distributed and autonomous character of AI systems.

3. Criminal Liability in the United States Approach to AI.

The US has casually pursued AI control by drawing upon the traditional legal theories of their current laws instead of developing a comprehensive model. The U.S. legal system, when it comes to criminal liability, puts more of its stress on human responsibility, where it makes more sense to first consider developers, corporations, or users of an AI system instead of the AI system itself.

The application of the principles of negligence and product liability is one of the most important mechanisms employed in the United States. The developers and manufacturers can be legally responsible in case they do not make sure that the artificial intelligence systems are safe and they do not introduce unreasonable risks. To illustrate, when the autonomous vehicle is involved in an accident as a result of the design defect, responsibility can be given to the manufacturer according to the product liability provisions.

The U.S. also has a prominent role of corporate criminal liability. Companies that implement AI systems can be implicated in committing criminal acts due to their operation, especially where they do not put proper safeguards. This practice is in line with the larger concept that corporations are also liable to the acts of its agents.

Nevertheless, the strategy used by the U.S has a number of challenges. It is also possible that the dependence on established doctrines will not be sufficient to manage AI systems peculiarities, including autonomy and the lack of predictability. Also, there is a lack of a unified regulatory framework, which introduces disparities in various sectors and jurisdictions.

Nevertheless, in the face of these issues, the United States has already made measures to mitigate AI related risks by implementing sector-specific regulations and guidelines. Federal agencies, including the Federal Trade Commission (FTC) have stressed the need to be transparent, accountable, and fair when it comes to AI systems. But even these measures are focused mainly on the civil liability and not on the criminal responsibility. Altogether, the U.S. strategy can be considered a pragmatic strategy based on a legal principle established, yet it might need to be developed to cover the issue of AI-based criminal behaviour.

4. The EU regulatory framework on the liability of AI.

The European Union (EU) is a rising power in AI regulation featuring a proactive and holistic outlook concerning solving the issues associated with the new AI. In contrast to the United States, the EU has attempted to come up with a common set of legal principles that

admitly cover AI-related risks, such as the problem of liability.

One important aspect of the EU strategy is its risk-based regulation. Based on the potential impact, AI systems can be divided into various categories with the most dangerous systems being those with stronger requirements. This strategy is evident in the legislative efforts, including the proposed AI Act, which focuses on setting up regulatory principles in the development and implementation of AI technologies.

Within the scope of criminal responsibility, the EU is concerned with responsibility and control. As creators and users of AI systems, developers and operators must make sure that their technologies meet safety, transparency, and ethical standards. Inability to address them might lead to legal obligations, such as even criminal accountability in some situations.

Human control of AI systems is also of the priority in the EU. The EU tries to keep humans in the loop to keep track of a clear chain of responsibility and thus allow the attribution of liability. This is an indication of acknowledgment in that fully autonomous systems are a major problem to the legal systems.

The other interesting feature of the EU approach is that it is concentrated on fundamental rights. The deployment and design of AI systems should be in a way that does not violate human dignity, privacy, and non-discrimination. Such an approach that prioritizes rights is an aspect that the EU framework is unique in comparison to other jurisdictions and supports its dedication to AI governance through ethics.

The approach of the EU is a major step in the direction of regulating AI, but it is not devoid of difficulties. The adoption of broad regulation can exert enormous compliance cost on companies, which can probably drive out innovation. There are also doubts as to whether the current doctrines concerning criminal law can possibly be tailored to meet the regulatory framework of the EU.

5. Indian Legal Stance on AI and Criminal Liability.

The current status of India regarding the regulation of AI remains in its own sphere of development, and there are few legal tools to tackle the problem of AI-related criminal liability specifically. The current law system is mostly based on the traditional laws like the Indian Penal Code (IPC) and the Information Technology Act, 2000.

With the IPC, the criminal responsibility is usually connected with the individuals having the necessary mens rea. This gives a serious dilemma over AI as autonomous systems have no intent as humans. Consequently, the responsibility of liability should be put on human actors, developers, operators, or users.

The Information Technology Act affords a certain level of coverage in the resolution to AI-related challenges especially when it comes to cybercrime. Nevertheless, it does not specifically refer to the special management issues of AI systems. The existence of this regulatory gap reflects the necessity to change legislation.

Regular policy discussions about AI have seen India appreciate the potential of AI through policies like the National Strategy for Artificial Intelligence. Such initiatives are though mostly aimed at enhancing innovation and economic developments as opposed to addressing issues of legal liabilities.

As a matter of fact, the Indian courts can use the principles of negligence and vicarious liability to deal with harms related to AI. As an illustration, an organization that implements AI can be responsible to compensate the damages that occurred in its activities. Nonetheless, the lack of particularly legal provisions makes it less predictable and can make it more challenging to enforce it.

To cope with these difficulties, India might have to choose a more complex approach to AI regulation, relying on international experience and taking into account its socio-economic

specifics. This can involve coming up with relevant legislations that need to regulate the liability of AI, and the modification of the existing legal philosophies to consider the self-governing aspect of the AI systems.

6. Towards a Coherent Global Approach to Criminal Liability in AI.

The contrast of the United States, European Union, and India demonstrates that their attitudes towards addressing AI-related criminal liability differ greatly. Unlike in the United States where the nation depends on the legal doctrines, the European Union has chosen to take the initiative of regulation and India is still at a developing stage. All these variations indicate that a more unified international practice should be adopted.

One of the main obstacles to creating such a framework is the consideration of both innovation and accountability. Excessive regulation can suppress technological advancement and at the same time excess regulation can endanger individuality and the society. This balance can be attained only with a delicate awareness of the peculiarities of AI systems.

It has been suggested that a hybrid liability approach, which incorporates the aspects of strict liability, negligence, and regulatory frameworks, is one of the possible solutions to it. In this system, the developers and operators of high-risk AI systems can be held to more rigorous standards of liability, whereas less risky ones can be regulated by less strict regulations.

The other fact that needs attention is the power of international collaboration. The technologies used in AI work across borders, and it can be quite challenging to take them regulated by their respective jurisdiction. Cooperation, including international guidelines and treaties, could assist in developing similar standards in AI governance.

Also, there is an increasing awareness of the necessity of ethical aspects in AI regulation. Legal frameworks should not just deal with the problem of liability but also be designed so that the AI systems can be designed and implemented so as to not violate human rights and values of the society.

To sum up, the emergence of AI poses new challenges to criminal law in ways never previously seen. To deal with them, it is necessary to reconsider old-fashioned legal postulates and come up with new methods of control. Through the experiences of other jurisdictions, policymakers may strives to achieve a more consistent and functional international approach to AI criminal liability.

Conclusion

The advent of artificial intelligence as an independent force of decision making has increasingly challenged the conventional bases of criminal law. On a foundation of actus reus and mens rea, traditional legal regimes have failed to equip themselves to deal with instances whereby injury is inflicted by an actor who is not conscious, does not possess intent and lacks the element of moral agency. Criminal liability of AI-driven actions, as can be witnessed in the comparative analysis of the United States, the European Union, and India, has no standardized method of establishing criminal liability, making the responses to criminal actions in AI fragmented and emerging.

The United States is still dependent upon the old doctrines, including, negligence, product liability, and corporate criminal liability as the pragmatic yet narrow sounding changes of classical ideas. Conversely, the European Union has been more progressive by coming up with a broad regulatory framework that focuses on risk categorization, responsibility and human control. Although India appreciates the role of AI, it is still in its early phase and the legal system does not have many stipulations to deal with AI-related criminal responsibility.

This disjuncture illustrates the pressing necessity of a unified legal framework that may be able to support the individual nature of AI-

systems. This framework must not be confined to an extreme dependence on human will and is supposed to involve other models of liability such as strict liability and hybrid accountability systems. It should also make sure that there is proper distribution of responsibility among the developers, operators and corporations without suppressing the issue of technological advancement.

Finally, it is not merely the question of how to allocate blame but also maintain even the notion of responsibility in the era of intelligent machines. A proactive and dynamic legal framework adhered to and upheld by collaborating with other countries and embracing morality would be needed to secure that the legal framework is not obsolete, and it is effective to curb the fast-changing environment of artificial intelligence.

BIBLIOGRAPHY

Books

1. Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed., Pearson, 2021).
2. Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap* (Brookings Institution Press, 2020).
3. Woodrow Barfield & Ugo Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing, 2018).
4. Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford University Press, 2020).
5. Mark Coeckelbergh, *AI Ethics* (MIT Press, 2020).

Journal Articles

1. Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities – From Science Fiction to Legal Social Control", (2010) 4 *Akron Intellectual Property Journal* 171.
2. Ryan Calo, "Robotics and the Lessons of Cyberlaw", (2015) 103 *California Law Review* 513.
3. Abbott Ryan, "I Think, Therefore I Invent: Creative Computers and the Future of Patent Law", (2016) 57 *Boston College Law Review* 1079.
4. Thomas Burri, "The Politics of Robots: Regulation of Robotics and Artificial Intelligence in the European Union", (2017) 35 *European Journal of Risk Regulation* 341.
5. Joanna J. Bryson, Mihailis Diamantis & Thomas D. Grant, "Of, for, and by the People: The Legal Lacuna of Synthetic Persons", (2017) 25 *Artificial Intelligence and Law* 273.

Reports & Policy Documents

1. European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, 2021.
2. NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll*, Government of India, 2018.
3. OECD, *Artificial Intelligence in Society*, OECD Publishing, 2019.
4. European Parliament, *Civil Law Rules on Robotics*, 2017.

Statutes & Legal Instruments

1. Indian Penal Code, 1860.
2. Information Technology Act, 2000 (India).
3. General Data Protection Regulation (GDPR), European Union, 2016.
4. U.S. Federal Trade Commission Act, 1914.

Web Sources

1. European Commission, "Artificial Intelligence Act", available at: https://digital-strategy.ec.europa.eu (last visited on April 8, 2026).

2. NITI Aayog, "AI for All Strategy Document", available at: https://www.niti.gov.in (last visited on April 8, 2026).
3. OECD AI Policy Observatory, available at: https://oecd.ai (last visited on April 8, 2026).

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344