INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

WWW.ijlar.com
Volume 3 Issue 4 | April 2026 *ISSN: 3049-043X*

CRIMINAL RESPONSIBILITY IN AI MISUSE - WHO SHOULD BE PENALISED?

AUTHORED BY - OMKAR MAHAPATRA
PhD. Scholar, KIIT University

CO-AUTHOR - ANGELINA BERNARD
Advocate, Calcutta High Court

ABSTRACT

Artificial Intelligence is spreading like wildfire and posing huge problems to criminal laws. A lack of principles for criminal responsibility makes it hard to hold people accountable when AI applications are used in ways they were not supposed to be, such as deepfakes, fraud, unintended harm, and biased results. The main question that is addressed in this doctrinal research article is: Who must be punished for using AI in an improper way?

The study introduces the fundamental concepts of *actus reus, mens rea,* causation and legal personality. It then examines various forms of AI misuses and the doctrinal challenges that they pose, especially the gaps in causation, foreseeability issues, opacity of AI systems and the attribution of responsibility amongst multiple actors. This is followed by an overview of the existing legal provisions, including product liability regimes, corporate criminal liability, European Union's risk-based AI Act, the more diffuse US sectoral and judicial response and India's regulatory approach via data protection laws and IT laws.

The EU's approach is prevention and oversight, the US and UK's approach is flexible and innovative, and India's approach is digital growth, the comparative analysis shows. Both methods have their advantages and disadvantages when it comes to accountability. The article suggests a hierarchy of responsibility based on existing criminal law principles. High-risk models should have more stringent responsibilities for developers in the area of safety and transparency. There is a duty to deploy and a duty to organisations based on a notion of negligence, and humans must be involved. Intentionally misusing the product remains the responsibility of end-users. These rules

can be fairly applied using a combination of a control-plus-foreseeability test, rebuttable presumptions and safe harbour provisions.

The study concludes that the responsibility for crime should not be shifted from individuals and organisations to AI itself. Unless specific legislative measures are introduced, harmful consequences can go unpunished, undermining the rule of law. This article presents a doctrinally sound pathway for a balance between innovation, justice and public safety in the age of AI.

Keywords: AI misuse, criminal responsibility, Deepfakes, causation challenges, AI governance

1. Introduction

The use of Artificial Intelligence is now rapidly becoming widespread in everyday life. Businesses and the government use it to make decisions that impact on people on a large scale. But this development comes with the use of it. Deepfakes can be used to create deception about individuals or attempt to alter election outcomes. AI tools can be used for committing fraud or generating malicious content. Autonomous systems occasionally are malicious, and not a direct part of human control. These cases simply ask a simple question. Who is liable for the criminal damage when AI is responsible for it?

Artificial Intelligence is an AI-based system that, for given objectives, makes predictions, recommendations or decisions that impact on the real or virtual world. This is based on definitions provided in US law, and in international discussions.

Misuse of AI occurs when individuals exploit AI systems to commit crimes or when AI systems generate illegal results. This can involve producing fake content for defamatory purposes, facilitating any financial scam and making decisions that are prejudiced in a manner which causes discrimination. Criminal Responsibility: The legal obligation to be held accountable for committing a crime within the framework of *actus reus* and *mens rea*. Most of the time, the law will equate liability to human actions and intent.

Traditional criminal law takes for granted the agency of humans. AI makes things complicated. The technology often works as a black box. Some outputs are so unexpected that even the developers can't explain how they are generated. Autonomy is distance from the original programmer to the final harm. There are lots of actors involved: developers, data trainers,

deployers, and end users. Causation is interrupted or complicated. When systems learn and adapt following release, foreseeability is reduced.

This is a challenge faced by courts and legislators. Existing laws and principles of corporate liability and negligence do not necessarily apply. Others question whether AI itself may ever be considered to have a legal personality. That is not being accepted by most views at this time. The responsibility remains in the hands of humans or organisations.

The gaps in these aspects are considered with doctrinal analysis and with the analysis of the existing legal framework. It does not create new facts but reviews statutes, cases and doctrines.

Research question and objectives

The overarching issue is who is to be held accountable for improper use of AI? Sub-questions follow. What is the role of the concepts of intention and cause? What are people's current laws? What are their weaknesses? The purpose of the study is to trace the issues and to outline the various methods used to address the issues, and to suggest future directions in legal doctrine.

Significance and scope

The misuse of AI is impacting public safety, elections, and trust in institutions. The deepfakes made an appearance in elections in countries such as the United States and Slovakia. The deepfakes made their way into elections in the United States and Slovakia, among others. The regulators issue rules such as the EU AI Act, which prohibits practices such as manipulative systems or social scoring. India is also in the process of developing digital laws. The study is based on the doctrinal analysis. It’s based in the United States, the United Kingdom, the European Union and India. This includes general law and civil law effects and new laws.

Methodology

This is a doctrinal research. It uses primary sources (statutes, case law and official documents). Secondary sources provide commentary. The technique used is an analytical and comparative method. There is no empirical data collected.

Chapter scheme

Theoretical foundation of criminal responsibility is reviewed in Chapter 2. Chapter 3 introduces forms of misuse of AI and the issues they pose for the old doctrines. Chapter 4 reviews existing legislation. Comparative analysis and recommendations for change are provided in Chapter 5. A summary of conclusions and recommendations is provided in Chapter 6.

In many areas, the development of AI is ahead of the law. The purpose of this article is to present some clarity on the question of criminal responsibility.

2. Theoretical Foundations of Criminal Responsibility

The foundation of criminal law is fundamental concepts which determine whether a person is to be punished. Typically, two significant components need to come together. First, there's the act. Next comes the guilty mind. Neither of them exists without the other, and in most systems, no crime remains.

The *actus reus* is the physical aspect. It is an action done on one's own volition or at times an omission when there is a duty to act. The behaviour has to bring about the harm. Causation is broken down into factual cause and legal cause. Factual cause is asking the question, if the action did not occur, would the result have occurred? Legal cause considers if the connection is close enough to be held accountable. Courts tend to block out far-reaching and unusual consequences. This is where AI comes in. The flow of information from the human to the output grows longer once a system begins to learn and act independently. So, who did the act then? The developer who wrote the code years earlier? Who was the user who provided prompt? Or the system itself.

Mens rea deals with the mental element. It can be from an obvious intent to recklessness or negligence. Intention is the desire to see the outcome of the risk. Recklessness is defined as awareness and willingness to ignore the risk. Negligence would be that they should have been aware of the risk but failed to be. These concepts are based on the assumption of a thinking, choosing human mind. The body of the AI does not suffer from consciousness nor from true desires. Works with patterns to make outputs. Connecting *mens rea* to AI heads into trouble.

Lawyers sometimes use doctrines like complicity. There is also liability for a person who assists or encourages a crime. An alternative route is corporate criminal liability. If an employee's conduct occurs during the scope of the business and is in the best interests of the business, then the company may be held liable for that conduct. This was an early jumping off point in the famous American case of *New York Central & Hudson River Railroad Co. v. United States.* The principle of identification and vicarious liability are similar in UK law. In some regulatory offences, the *mens*

rea element is eliminated by strict liability. However, even in the case of strict liability, the person and/or entity must still be a human or a business entity.

Why punish at all? Retribution is what the wrongdoer deserves. The punishment is commensurate with the wrong. The purpose of deterrence is to prevent reoffending. It may be targeting the individual or send a message to all. The goal of rehabilitation is to transform the offender so he doesn't commit crimes again. Emphasizes treatment and education. These theories make an assumption of a being that can feel pain, understand consequences, or change its behaviour. When they are applied to AI, they immediately pose questions. Fining a company works because it has money. How about punishment for code?

Legal personality

Legal personality is a quality that permits an entity to have rights and duties. It is automatically understood by humans. Companies get it by law. The question is whether the advanced AI deserves the same status. Most, for now, don't want to do it. AI is not free will, it is not conscious and it is not morally aware. These are essential for it to develop the blameworthy mind criminal law requires. The concept of treating AI as a legal entity could also pose practical issues. Who would act on its behalf in court? What would be the consequences for fines or sentence? The discussion remains active, and the general consensus remains that humans remain responsible in the chain.

Tool vs agent

This leads to the main discussion. Should AI be considered a tool such as a hammer or gun? If it is, the man or woman who uses it bears the responsibility. Or, has it turned into more of an agent working freelance? A lot of the existing systems are still dependent on human prompting and remain controlled. Newer agentic AI, however, can start to plan steps and undertake less supervision. The line blurs. If something does not turn out the way the creator expects, the output is unexpected and the tool view is further undermined. Still, law has not accepted AI as a true independent agent for criminal purposes. It is a matter of their responsibility.

These are the bases that were created for human actors. When it comes to AI, they do stretch. In the following chapters, they will face real types of misuse and be put to the test.

3. AI Misuse Typologies and Challenges to Traditional Liability Doctrines

There are various forms of AI misuse. In some cases, the system is used as any other instrument. Others continue to stretch the technology limits, as the technology operates more independently. This chapter categorizes the primary types and reveals where the old criminal law rules begin to fail.

Types of misuse

The first type applies to the use of AI in the investigation of old crimes. The criminals use it to create a deepfake to defame or commit fraud. In one 2024 incident, a company lost more than 25-million USD due to scammers setting up a video call as the chief financial officer and tricking the employee into sending the funds. Voice cloning can aid with equivalent scams. They receive calls which seem to be from family in difficulty and transfer cash. Generative AI also helps with creating better phishing emails or fake documents. These acts would fit into the statute on fraud or forgery but the fact that the AI makes them easier to make and more difficult to track makes them cheaper.
The second type is when the content is generated by AI but fails to adhere to certain rules. There are plenty of examples of non-consensual deep fakes. Political deepfakes try to influence elections by spreading false statements. Some systems produce child pornography, but without any actual children being involved. In this case, the harm is in the product itself.
When systems are more self-governing, third category will appear. Accidents could be caused by autonomous vehicles or drones. But trading algorithms have caused market crashes such as the 2010 flash crash. Some places have equality laws which look like discrimination when such discrimination is caused by biased algorithms in hiring or policing. System learns and adapts after deployment. That distance from the original human input creates fresh problems.
Systemic harms are included in fourth type. Predatory loan practices or something like a ‘predictive policing’ program that gives rise to bias. They're more difficult to classify as crime but they affect many people and over a period of time.

Main challenges

Traditional law requires an act and the guilty mind. AI muddies both.
When an AI learns new behaviour after training, the courts question whether the "harmed code was the cause of the harm.” There is a lot of opacity and a lot of models operate as black boxes.

Even the creators are unable to fully account for the reason that a certain output came out. This is bad for proof in all cases where it requires detailed explanation.

Then there is the element of *mens rea.* A human mind is required for intention or recklessness or negligence. AI has none. Years later a trained model could do something that a developer never thought of. A user provides ambiguous input and receives undesirable output. A user provides ambiguous input and receives undesirable output (harmful results). Complicity rules require knowledge or intent to help the crime. Who helped who when thousands are using the same open model? There are times when courts extend the standard of negligence, but the fit is still awkward. Across a number of actors, layers are added to the attribution. The base model is developed by the developers. Training sets are provided by data companies. The system is installed by companies. Users give prompts. Every link can take responsibility for the next link in the chain having broken. Contrary to the case of defective goods, product liability ideas do not exist for software. Just as in some areas of regulation, strict liability is an exception in criminal law, which prefers fault.

Foreseeability shrinks too. It can be difficult to anticipate all its uses because it is learned and implemented so quickly. For powerful AI, there are no such rules or defences as safe harbour in effect. These gaps are reflected between jurisdictions. Some existing computer misuse and data protection laws assist on the fringes but not the whole. Humans are sometimes charged at one end of the chain of command, by prosecutors. However, many cases still conclude without clear liability as the doctrines aren't as far-reaching as they should be.

How these issues are being addressed in the currently available frameworks and where they are still lacking is explored in the next chapter.

4. Current Legal Frameworks and Attribution Models

Now, lawmakers and courts are attempting to adapt the rules to accommodate AI. Some methods consider it as any products or company activity. Others set new "rules" for risk level. This chapter examines the current state of affairs and how people seek to blame.

In certain cases, software and AI are considered products rather than services. This leaves way for strict liability for design defects. Recent cases prove this. In the Garcia v. Character Technologies case, the court ruled that claims are admissible when the plaintiffs allege that the chatbot app was defective in design features such as missing age checks. They didn't treat the conversation outputs as products - the app was a product. Such actions are used in social media algorithm litigation

cases. The premise is that if the system is unreasonably dangerous, then the maker may be held liable even if they have not been negligent in using the term "full intent. However, there are many opinions that state that software is more like a service and the rules aren't always applicable. The line remains cloudy.

Businesses are liable for their employees' actions. The base in the US was established in the old NY Central case in 1909. The company may be liable for criminal charges if the employee acts within his or her job and benefits the company. There are some scholars who want to consider AI as an employee. The organisation should be responsible if the system hurts the company. Under the principle of identification in the UK law, senior individuals stand in for the company. Help is provided in many places, but there must be a human link somewhere. This connection becomes weak when AI operates in a more free-spirited manner.

The EU AI Act provides the most clarity. It prohibits some practices altogether. These range from manipulative methods that change behaviour, exploiting vulnerabilities, social scoring, untargeted scraping for facial recognition databases, and emotion recognition in the workplace or school context. Transparency, risk assessment and human oversight are critical considerations for high-risk systems. The Act began to have effect on a graduated basis from 2025. Fines can be high percentages of global turnover. This is a risk-based approach that attempts to prevent issues from escalating.

The United States has a system of sector rules and state laws. There is no single federal AI law that addresses all things. Existing fraud laws are applied to deepfake and AI-driven offenses. Certain states prohibit specific uses, such as election deepfakes, or mandate disclosures. Under the TAKE IT DOWN Act of 2025, non-consensual intimate deepfakes are criminal offenses. In many cases, courts deal with numerous matters as a result of product liability or negligence claims.

India has adopted the Digital Personal Data Protection Act 2023 and existing IT rules. Consent rules, data fiduciary duties and penalties for breaches are established in the DPDP Act. Does not establish overall criminal responsibility for most data problems. There is no specific statute for AI. Cyber laws are used in a wider context by regulators in cases of misuse. The approach remains less burdensome in terms of specific AI rules than in Europe.

Some proposals include compulsory insurance or change the burden of proof. The developers may need to demonstrate reasonable measures. The rebuttable presumptions may be helpful. If the harm is from a high-risk system, the deployer would have to demonstrate compliance with the standards.

It remains uncommon in practice to have an AI entity held responsible. Final responsibility is kept on humans or organisations by most experts. Guidelines for responsible AI responsibilities are currently legally non-binding.

These are the frameworks that assist at the edges. Clear defects are covered by product liability. If a company fails in a blatant way, corporate rules will catch it. The worst uses are banned in the EU. However, numerous cases do not make it to court. It's difficult to determine who was at fault with opacity. The multi-actor supply chain lets no one bear the blame. Personal fault is wanted by criminal law. If no one recognized the danger, then prosecutions were hard to come by. Legislatures continue to make changes, but large gaps remain.

The next chapter discusses these strategies and offers some ideas for change.

5. Comparative Analysis and Proposals for Reform

The approach to AI criminal liability varies from one location to another. The discrepancies are rooted in legal cultures and concerns about innovation versus harm.

EU has the most stringent position. The AI Act classifies systems according to their risk level. It prohibits certain uses and imposes significant requirements on high risk uses, and human review is mandatory. This method aims to prevent problems from occurring. It's effective for obvious dangers, but critics claim it can be a drag for small businesses.

The federal government remains more hands-off in the United States. It is based on old statutes regarding fraud, product liability and special state regulations. In some cases of chatbots, courts drive product liability concepts. This helps maintain flexibility and promotes quick development. The downside is uneven protection. There is no clear rule to cover many types of harms.

United Kingdom combines flexibility of the common law with new guidelines. It does not impose burdensome initial rules, but rather seeks solutions in the sector. Old doctrines such as negligence and corporate liability can be modified by courts. This allows judge to craft rulings on a case-by-case basis. But it leaves developers in confusion over boundaries.

So far in comparison, India is on a lighter footing. The Digital Personal Data Protection Act is about data duties and consent. Some cyber misuse is addressed in broader IT rules. There is no complete AI legislation in place. This aligns with India's thrust towards digitalization with significant accountability deficits in the event of harmful impact from strong AI.

The most obvious risk-based structure is that of Europe. In the United States, the value of using existing tools creatively is demonstrated. Common law provisions in the UK help cases to fill gaps. India serves as a reminder that excessive regulation can have a negative impact on adoption in developing markets. The multi-actor problem is common to all. Blame spreads thin. Proving something is hard when it's opaque. Even criminal law requires a clear guilty mind and that is difficult to come by.

Proposed model

It is best that there be a tiered responsibility structure within a pre-established doctrine. There are stringent responsibilities for developers in terms of safety and transparency of the base models, particularly for high-risk applications. They are required to demonstrate reasonable limits of testing and disclosure. For fine-tuners and companies that deploy or release systems, a negligence/recklessness standard is applied. They will need to be supervised by humans as to how they work in real world. End users remain responsible for any clear and intentional misuse, such as producing deepfakes with tools for fraud.

A control-plus-foreseeability test will aid courts in reaching their decisions. Was there meaningful control at critical stages by the person or company? Would they be able to reasonably anticipate the kind of harm? Taditional concepts of causation and *mens rea* are preserved and extended to AI. There may be rebuttable presumptions. When the harm is caused by a high-risk system that failed to adhere to basic safety rules, the onus is on the developer or deployer to demonstrate that it did so.

Good actors would be safeguarded under safe harbour conditions. Companies that adhere to recognised standards, submit risk reports, and cooperate with investigations are provided some protection from total criminal liability. The costs of high-impact systems can be distributed across mandatory insurance, while maintaining innovation.

This model is a balance between a number of goals. Prevents careless actions. It holds the humans accountable and not the code. It protects innovation by giving clearer rules. It does not extend the concept of legal persons for AI, and honours the doctrinal origins.

There is no single jurisdiction that has all answers now. The best way forward is perhaps a hybrid approach, combining elements of the EU risk categories, the US creativity, and the flexibility of common law.

The last chapter concludes these points and provides closing suggestions.

6. Conclusion

The study examines who should face criminal prosecution for misuses of AI. Clearly, the traditional doctrines are founded on guilty act and guilty mind. AI stretches these concepts. Gaps in causation and intent exist in reality, and they include autonomy, opacity of the black box, and long chains of actors.

The main findings are straightforward. AI should not be held liable for crimes. It lacks consciousness and moral agency. There should be a human and organisational responsibility throughout the development and use chain. But the subject or object of the action varies according to the context. High-risk base models have heavier duties for the developers. Users are responsible for any intentional misuse. The one-size-fits-all approach is not applicable here.

There are partial solutions in existing laws. The EU AI Act introduces convenient categories of risk and prohibitions. Product liability litigation is creatively pursued in the United States courts. UK common law is flexible. India’s structure is lighter. None of them has filled all the gaps in the face of the harm and changes in complex systems.

A multi-level solution addressing control and foreseeability offers a feasible solution. Stronger requirements for developers with respect to safety and transparency, and negligence standard for deployers and liability for the user's intentional misuse. This can be made possible with rebuttable presumptions and safe harbour provisions. These changes must be made by the courts and legislatures, not await perfection. The law needs to change at a quicker rate. Legislatures need to clarify attribution rules and can even mandate having insurance for high-impact AI. Judges can develop the control-plus-foreseeability test through cases. If these ste are not taken, there will be little checks and balances on the powerful AI and accountability will be weak.

Much of the larger question is that of the Rule of Law. If the harms caused by AI are severe, and if they are not punished on a regular basis, the public's trust in the justice system will be tarnished. Innovation is important but not at the expense of justice and safety.

This doctrinal study shows the path. There is a responsibility for humans. Now the question is how to make that principle apparent in the era of artificial intelligence.

REFERENCES

1. Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology, 31*(2). https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf
2. European Union. (2024). *Artificial Intelligence Act*. https://artificialintelligenceact.eu/
3. Khisamova, Z., & Begishev, I. (2019). Criminal liability and artificial intelligence: Theoretical and applied aspects. *Russian Journal of Criminology*, *13*(4), 564-574.
4. Sachoulidou, A. (2024). AI systems and criminal liability. *Oslo Law Review*, *11*(1).
5. Shestak, V., Volevodz, A., & Alizade, V. (2019). On the possibility of doctrinal perception of artificial intelligence as the subject of crime in the system of common law. *Russian Journal of Criminology, 13*(4), 547-554.
6. U.S. Code definitions of artificial intelligence (15 U.S.C. S. 9401 and related provisions).
7. Diamantis, M. E. (2020). When corporations use AI to break the law. *North Carolina Law Review*.
8. Hallevy, G. (n.d.). The criminal liability of artificial intelligence entity. *Akron Intellectual Property Journal*.
9. Just Security. (2026, January 28). Artificial guilt? A practitioner's guide to criminal liability in generative AI.
10. U.S. Supreme Court. (1909). *New York Central & Hudson River Railroad Co. v. United States*, 212 U.S. 481.
11. Ayres, I. (year). The law of AI is the law of risky agents without intentions. *University of Chicago Law Review Online*.
12. King, T. C., et al. (2019). Artificial intelligence crime: An interdisciplinary analysis of individual and state culpability in the age of artificial intelligence. *Available via PMC.*
13. U.S. Congress. (2025). TAKE IT DOWN Act.