



This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Legal Liability of AI Chatbots for Providing Harmful Advice: Examining Accountability in the Age of Artificial Intelligence

Lavanya Anand^a

^aMaharaja Surajmal Institute, New Delhi, India

Received 27 May 2026; Accepted 27 June 2026; Published 01 July 2026

Artificial Intelligence (AI) chatbots have rapidly transformed the way to access information, advice and assistance from people. Advanced generative AI systems, including ChatGPT, Gemini, Claude and similar large language models, are increasingly being turned to for advice on medical, legal, financial, educational and psychological matters. The technology enablement of various processes is beneficial as it increases accessibility and efficiency. What remains a concern, however, is accountability in case the wrong or harmful advice causes injury, economic loss, and so on. Regulatory frameworks now available were made for human actors and conventional products, creating uncertainty regarding their applicability to autonomous AI systems. This piece looks at the legal accountability of AI chatbots for giving harmful advice from the perspective of negligence, product liability, and consumer protection law. It also examines the developing regulatory strategies in the European Union, the United States and India. Current legal doctrines afford only partial solutions, argues the article, mainly owing to the specificities of AI systems, including opacity, unpredictability and autonomy of learning. In fact, it is necessary to create a comprehensive regulatory framework which allocates responsibility to developers, deployers and service providers as well as ensures adequate protection to users. Moreover, the article suggests reforms for enhancing transparency requirements, product liability frameworks, and the enactment of a dedicated AI governance law in India.

Keywords: *artificial intelligence, chatbots, negligence, product liability, consumer protection.*

INTRODUCTION

In this article, we examine the legal liability of the AI chatbot in terms of negligence, product liability and consumer protection law. It also examines regulatory developments in various jurisdictions and considers whether AI systems should have legal personality. Ultimately, the article argues that specific regulatory intervention is needed to address the distinct risks of AI chatbots and that current legal principles provide the basis for accountability.

UNDERSTANDING AI CHATBOTS AND HARMFUL ADVICE

Nature and Function of AI Chatbots: AI chatbots are computer programs that employ natural language processing and machine learning to replicate human communication. Modern chatbots are typically built on Large Language Models (LLMs) trained on a large range of text from books, the internet, academic material and other digital sources.¹ It is in this training that the models learn statistical linguistic patterns. They answer based on likelihood, not actual understanding.

Conventional software programs operate based on a set of rules, whereas generative AI systems produce replies on the fly. This versatility enables them to answer difficult inquiries and to participate in intricate exchanges. But it also allows for uncertainty, because as a developer, you can never foresee or control the result.²

AI chatbots are getting smarter, and consumers are asking for guidance on really sensitive issues. Legal professionals are increasingly utilising AI tools for legal research and drafting. Patients ask chatbots about symptoms and treatment alternatives. Investors turn to AI-powered platforms for financial advice. Such usage blurs the boundary between informative help and professional advice, thus raising the potential for harm.

Types of Harmful Advice: The damage of AI-generated advice can take several kinds. First, medical misinformation can cause serious physical injury. A chatbot could wrongly advise to stop taking prescription medication, misdiagnose symptoms, or offer dangerous remedies. Such errors can have a direct impact on the health and well-being of the person.

¹ Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021) 1–10

² Ryan Abbott, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability' (2018) 86(1) *The George Washington Law Review* 1, 30 <<https://www.gwlr.org/wp-content/uploads/2018/04/86-Geo.-Wash.-L.-Rev.-1.pdf>> accessed 20 May 2026

Second, legal disinformation might cause users to miss statutory deadlines, misunderstand their legal rights, or pursue improper litigation methods. The intricacy of legal systems makes it highly prejudicial to rely on wrong legal counsel.

Third, AI-generated financial advice can lead to economic loss. Users who follow wrong investing tips may face huge financial losses.

Fourth, psychological harm can occur when AI systems offer bad advice on mental health or fail to respond effectively to sensitive people. With conversational AI becoming a greater and more prevalent emotional support tool, concerns over mental health dangers have grown.

These instances show that bad advice from AI is not just a theoretical problem, but a real and growing problem that should be addressed legally.

EXISTING LEGAL FRAMEWORKS FOR AI CHATBOT LIABILITY

Negligence Liability: Negligence continues to be one of the most salient legal theories for addressing the harms produced by AI-generated guidance. In common law torts, the claimant has to prove four basic elements: a duty of care owed by the defendant, the violation of that obligation, causation and damage caused by that breach.³ The theory is intended to ensure that people and entities use reasonable care to avoid foreseeable risks of harm to others.

In *Donoghue v Stevenson*, the court made a major ruling creating the current tort of negligence with the “neighbour principle” by which persons must take reasonable care to avoid acts or omissions which could foreseeably hurt others who are closely and immediately impacted by their behaviour.⁴ In *Caparo Industries plc v Dickman* the House of Lords later established a three-part test of foreseeability, proximity and whether it is fair, just and reasonable to impose a duty of care.⁵ Applying these principles to AI chatbots is not an easy matter. Developers and providers of AI systems can plausibly be said to owe a duty of care to consumers, especially if the chatbot is advertised as a dependable source of information. In cases when an AI system repeatedly provides bad advice in situations where harm should

³ James Goudkamp and Dolan Nolan, *Winfield and Jolowicz on Tort* (20th edn, Thomson Reuters (South Asian Edition 2019)

⁴ *Donoghue v Stevenson* [1932] AC 562

⁵ *Caparo Industries plc v Dickman* [1990] 2 AC 605

be expected, courts might rule that developers did not take reasonable care in developing, training, or monitoring the system.

For example, if a healthcare chatbot gives a user bad medical advice, such as telling them to stop taking prescribed medication, leading to serious harm, the affected person might claim the developer failed to exercise due care by not having sufficient safeguards against medical misinformation. Similarly, legal AI systems that give incorrect advice, resulting in a user missing a statutory limitation period, could subject the developers to negligence charges. But demonstrating fault in AI situations is typically tough. AI systems do not work the same way as human professionals do; they rely on intricate machine-learning processes that are not always obvious. It can, therefore, be difficult to tell exactly how an erroneous output was generated. Additionally, developers often contend that the warning to not rely only on answers from AI is clear and that the technology is only meant to be a source of information and not a replacement for professional counsel.⁶

Another problem is causality. The courts usually want evidence that the defendant's actions were the direct cause of the claimant's loss. In AI conflicts, the users often act independently on the output of a chatbot. It may consequently be controversial to decide if the damage was caused by the advice of the AI, the conduct of the user or the context. Negligence law is an important tool to deal with AI-related problems, notwithstanding these challenges, because it is concerned with whether action is reasonable, rather than the nature of the technology as such. As AI begins to encroach on sensitive areas, courts may slowly apply established negligence concepts to the new realities of technology.

Product Liability: Another route for holding AI chatbot providers accountable is under product liability law. Product liability is often a type of liability that makes manufacturers and producers responsible for damages caused by defective items without the need to establish negligence. The doctrine is intended to shield consumers by requiring products offered for sale to meet reasonable safety standards.⁷

The application of product liability principles to AI systems has been a subject of much controversy. Traditionally, product liability rules were developed with physical objects in

⁶ Abbott (n 2)

⁷ David G Owen, *Products Liability Law* (3rd edn, West Academic Publishing 2014) 5

mind, such as cars, machines, drugs and consumer goods. AI chatbots, on the other hand, are software programs that are constantly updated and improved using machine learning. This begs the question of whether AI software should be classified as a “product” for reasons of liability. More and more, the EU has seen the necessity to adapt product liability frameworks to new technology. Policymakers have realised that software and AI systems might inflict harm similar to that caused by physical items. Hence, the calls to extend the laws of responsibility to digital products and AI-enabled systems have been increasing.⁸

From a legal angle, an AI chatbot may be regarded as faulty if it does not deliver the safety that users have a right to anticipate. For example, a chatbot sold as a medical assistant could be flawed if it often provides unsafe medical advice due to improper training or poor protections. Similarly, a design error may be found if there were no warning mechanisms or content management systems in place.

There are many advantages of product liability over negligence lawsuits. First, claimants may not be required to prove culpability, thus lowering the burden of proof. Second, liability can attach even if a developer has taken reasonable care and the product has caused harm. This is a useful strategy in cases involving AI, for example, where it’s difficult to identify precise negligent behaviours. But product liability is similarly limited in its applicability to AI chatbots. Unlike traditional products, AI outputs are very contextual and depend on user engagement. The response generated for one user may be very different from the response generated for another. This heterogeneity makes it difficult to know if a fault exists and who is responsible for it. Furthermore, AI ecosystems often involve several actors, such as developers, deployers, cloud service providers, and data providers. One of the biggest challenges in regulating AI today is working out who is liable among various parties.

Consumer Protection and Regulatory Liability: Consumer protection laws might provide another foundation for holding AI chatbot providers liable for providing harmful advice. Consumer protection schemes are designed to protect customers from unfair, deceptive and misleading commercial practices, unlike negligence and product liability.

⁸ European Commission, ‘Proposal for a Directive of the European Parliament and of the Council on liability for defective products’ COM (2022) 495 final

The Consumer Protection Act, 2019 in India has greatly enhanced the rights of consumers and put in place measures for defective products and poor services.⁹ The Act puts obligations on producers, service providers and sellers to guarantee that consumers are provided with safe and reliable goods and services. Consumer protection law can apply to AI chatbots that are provided as commercial services. If a corporation claims that an AI chatbot can provide reliable legal, medical, or financial aid but fails to disclose the chatbot's limits, such claims could be considered misleading ads or unfair trade practices.

"The principles of consumer protection are especially pertinent as AI systems frequently create an aura of authority and dependability." Sophisticated AI platforms may fairly expect users to expect answers to be accurate and trustworthy. Even without physical injuries, providers could be liable if they willfully misrepresent the capabilities of their systems.

The Information Technology Act 2000 also provides a limited regulatory regime for digital platforms in India. Although the legislation was not tailor-made for AI technologies, several of the clauses regarding intermediary responsibility and digital governance may have increased relevance as AI systems grow further.¹⁰

Another issue is one of disclaimers. Most AI vendors have terms of service that state that chatbot outputs may not be accurate and should not be relied upon as expert advice. Although such disclaimers may limit liability in some cases, courts are reluctant to allow corporations to escape all responsibility for foreseeable losses, particularly when customers legitimately rely on statements made by providers. Consumer protection law thus plays an important supplementary role in regulating AI chatbots if consumers are harmed by deceptive promises or inadequate disclosures.

CHALLENGES IN IMPOSING LIABILITY ON AI CHATBOTS

Even if traditional legal theories are available, there are many practical and theoretical challenges to imposing liability on AI chatbot providers.

Problem of Black Box: One of the most important issues with AI systems is the lack of transparency. Today's AI models are built on very complicated algorithms that frequently

⁹ Consumer Protection Act 2019

¹⁰ Information Technology Act 2000

generate results without explaining how they arrived at those results. This characteristic, popularly known as the “black box problem,” makes it impossible for courts, regulators, and even developers to understand why a certain detrimental response was generated.¹¹ In litigation, causation and fault are often contingent on identifying the source of the error. But when an AI model produces a detrimental output because of the complex machine learning processes involved, it becomes even more difficult to assign guilt.

Self-learning and Uncertainty: AI systems, unlike traditional software, can learn and get better with training updates and human interactions. Hence, engineers are not able to forecast all the outputs that the system would generate. This raises serious considerations about the extent to which creators should be held liable for unforeseen actions generated by autonomous systems.¹² The nature of AI-generated information is inherently unpredictable, so it cannot be subjected to the traditional legal presumption that culpability is predicated on purposeful action or foreseen outcomes.

Diverse Stakeholders: AI ecosystems involve many players, including software developers, data providers, cloud infrastructure operators, deployers, and end users. Failures at many points in the AI lifecycle can result in harmful advice. False outputs can be the result of biased training data, a poor model architecture, insufficient testing methods or incorrect deployment procedures. The identification of the actor who should be legally responsible is thus a complicated task. In many circumstances, blame may have to be shared by several parties.

Contractual Disclaimers: Most AI companies have lengthy warnings indicating their outputs may be wrong and not to be relied on as expert guidance. These disclaimers are meant to mitigate legal liabilities by informing users of the limitations of AI systems. However, disclaimers do not offer total immunity. The courts have always been suspicious of exclusion provisions, particularly where there is a significant imbalance of bargaining power between the service provider and the consumers.¹³ In addition, disclaimers may not

¹¹ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 3–18

¹² Joanna J Bryson et al., ‘Of, for, and by the People: the legal lacuna of synthetic persons’ (2017) 25 *Artificial Intelligence and Law* 273, 281–286 <<https://link.springer.com/article/10.1007/s10506-017-9214-9>> accessed 21 May 2026

¹³ Richard Stone and James Devenney, *The Modern Law of Contract* (14th edn, Routledge 2022) 245–258

be effective where suppliers make express statements concerning the reliability and accuracy of their products.

INTERNATIONAL COMPARATIVE PERSPECTIVES

European Union (EU): The EU has become a world leader in AI regulations. The EU Artificial Intelligence Act adopts a risk-based approach to regulating AI systems, categorising them by their potential impact on society.¹⁴ In this paradigm, AI applications identified as higher risk will have stricter compliance duties, including transparency obligations, risk assessments, human oversight processes and documentation standards. The Act attempts to find a balance between innovation and the protection of fundamental rights and public safety. The EU's approach accepts that current legal frameworks may not be sufficient to meet the special challenges brought by AI technologies. The Act seeks to impose *ex ante* regulatory obligations to prevent harm before it happens rather than to rely mostly upon post-harm responsibility mechanisms.

United States: The United States has relied primarily on existing legal theories to handle AI-related concerns, including negligence, product liability, and consumer protection legislation. There is no comprehensive federal regulation regarding AI liability as of now, unlike the European Union. American courts are facing more and more conflicts over algorithmic decision-making and AI-generated content. While classic legal principles are still applicable, there is much uncertainty about how these doctrines should be applied to fast-emerging technologies. The US strategy focuses on innovation and flexibility of the market but has been accused of not having a clear framework to tackle AI-related issues.

India: At present, India does not have legislation regulating AI liability. Disputes relating to AI technologies will have to be dealt with using existing laws such as the Consumer Protection Act 2019, the Information Technology Act 2000, contract law principles and tort law doctrines.¹⁵ The Government of India and NITI Aayog have acknowledged the revolutionary potential of AI while also stressing the need for responsible innovation. NITI Aayog's reports encourage ideals of fairness, accountability, transparency, privacy and inclusivity.¹⁶ But these suggestions are mostly policy-based and do not impose strict legal

¹⁴ EU Artificial Intelligence Act 2024

¹⁵ Consumer Protection Act 2019; Information Technology Act 2000

¹⁶ *Responsible AI #AIForAll* (NITI Aayog 2022) 22–37

duties. As AI use continues to accelerate across healthcare, banking, education, and public administration, the lack of a comprehensive regulatory framework may bring about legal uncertainty for users and developers alike.

SHOULD AI POSSESS LEGAL PERSONALITY?

One of the ongoing debates in AI governance is whether advanced AI systems should be allowed legal personality, akin to businesses. Proponents say fully autonomous AI systems are becoming capable of making their own judgments and should thus be held responsible for the outcomes of their actions. There are researchers who argue that if AI were recognised as an independent legal entity, assigning liability would be easier, as it would allow claims to be made directly against the AI system.¹⁷ But this proposal has serious objections. Legal personality has always had rights, duties, and the ability to have legal obligations. An AI system does not have consciousness, moral agency, intent, or independent assets. That means they cannot pay or meet legal obligations in the same way that humans or corporations can.

Legal personality could also be a way for developers and businesses to shift culpability to technology systems, providing an escape route. Such a move would be at odds with the very purposes of tort law and consumer protection. Thus, it is human actors that design, develop, deploy, market and profit from AI systems who should bear culpability.

RECOMMENDATIONS

Some adjustments should be addressed to tackle the increasing hazards of bad advice produced by AI.

Pass Specific AI Legislation: India should develop a separate comprehensive law on AI governance and liability. Such legislation should specify the duties of the developers, deployers and service providers and provide compensation and conflict settlement methods.

Enhance Transparency Requirements: AI companies would have to disclose known hazards, system limitations, and training procedures. Transparency leads to better

¹⁷ Shawn Bayern, 'THE IMPLICATIONS OF MODERN BUSINESS-ENTITY LAW FOR THE REGULATION OF AUTONOMOUS SYSTEMS' (2015) 19 Stanford Technology Law Review 93, 110-118
<https://law.stanford.edu/wp-content/uploads/2017/11/19-1-4-bayern-final_0.pdf> accessed 23 May 2026

accountability and helps people to make better decisions about whether to accept AI-generated advice.

Move to risk-based regulation: Not all applications of AI are equally risky. The healthcare, legal, finance and public administration sectors are more sensitive since they might affect the rights and well-being of people and hence need more control.

Have Human Oversight: AI systems should still be subject to human inspection, even in sensitive sectors. Such vital decisions about health, liberty or financial security should not be entrusted to automation alone.

Explain how Liability is Allocated: Legislation should define the allocation of responsibilities between developers, deployers and other stakeholders. Clarity would eliminate ambiguity and contribute to effective implementation.

CONCLUSION

AI chatbots have transformed our approach to finding information and assistance, paving the way for new possibilities in innovation and efficiency. But the increasing use of advice produced by AI systems also poses significant legal and ethical challenges. Harmful outputs can cause bodily harm, financial harm, psychological harm, and violation of legal rights.

Traditional legal theories, such as negligence, product liability, and consumer protection legislation, provide means to redress these harms. Yet the very characteristics that make AI systems different, their opacity, unpredictability and autonomous decision-making, present issues that existing legal frameworks were never built to tackle.

Comparative analysis demonstrates that jurisdictions worldwide are actively investigating regulatory responses to AI-related issues. The EU has embraced a complete regulatory strategy, while the United States remains mostly reliant on current legal standards. India is yet to develop a comprehensive regulatory regime for AI and has no specific liability regime.

As AI technologies continue to advance, legal accountability must adapt as well. Good legislation should facilitate innovation and simultaneously protect individuals from expected harm. Ultimately, it is the human actors who design, develop, deploy and profit from these systems that are responsible for harmful AI-generated advice. Only a balanced

structure of accountability, transparency and monitoring will enable society to harness AI completely while minimising its threats.