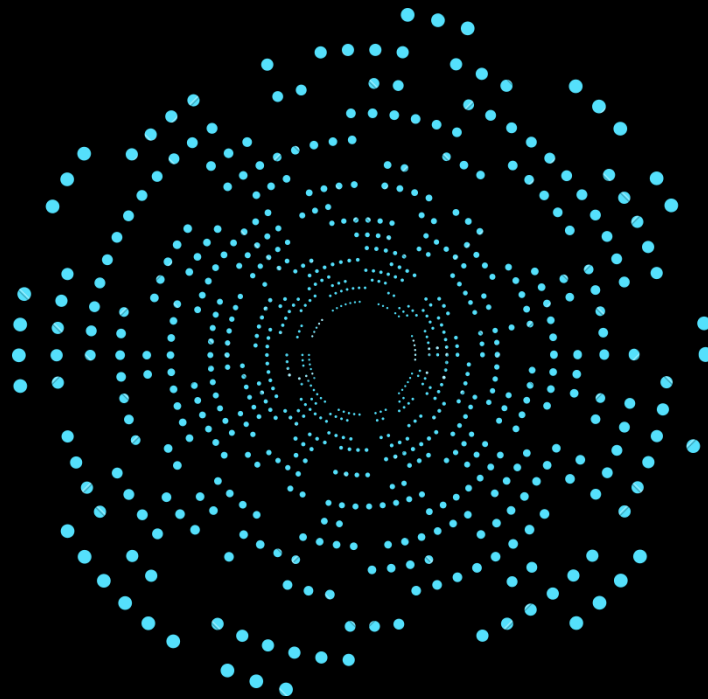




INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY



VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION





International Journal on Cyberspace Law and Policy

(Free Publication and Open Access Journal)

Journal's Home Page – <https://ijclp.iledu.in/>

Journal's Editorial Page – <https://ijclp.iledu.in/editorial-board/>

Volume 1 and Issue 1 (Access Full Issue on – <https://ijclp.iledu.in/category/volume-1-and-issue-1-of-2023/>)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 – info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://ijclp.iledu.in/terms-and-condition/>



LIABILITY FOR HARM OR DAMAGE IN ARTIFICIAL INTELLIGENCE

Author - S.SRINIDHI, Student at SAVEETHA SCHOOL OF LAW, SIMATS

Best Citation - S.SRINIDHI, LIABILITY FOR HARM OR DAMAGE IN ARTIFICIAL INTELLIGENCE, *International Journal on Cyberspace Law and Policy*, 1 (1) of 2023, Pg. 38-42, ISBN - 978-81-960677-4-8.

ABSTRACT

The development of artificial intelligence (AI) has led to a range of legal issues, including the question of who should be held responsible for harm or damage caused by AI systems. This paper examines the liability for harm or damage in artificial intelligence, with a focus on the Indian legal framework. The objective of this study is to explore the legal and ethical challenges posed by AI, with a view to understanding the key issues and potential solutions. The paper highlights the challenges and uncertainties surrounding liability for harm or damage caused by AI. It emphasises the need for greater clarity and guidance from regulators and the courts in India, where the legal framework is still in early development. The paper concludes that an effective and ethical legal framework must be developed through collaboration among policymakers, industry leaders, and legal experts to ensure that the benefits of AI are realised while protecting the rights and interests of individuals and society.

KEYWORDS: Liability, Artificial Intelligence, Legal Framework, India, Ethics considerations

INTRODUCTION:

Artificial Intelligence (AI) is becoming increasingly prevalent in modern society, with a growing number of industries and sectors using AI-powered tools to streamline processes, improve efficiency, and enhance decision-making. However, as the use of AI becomes more widespread, so too do concerns about the

potential for harm or damage caused by AI. As a result, the issue of liability for harm or damage caused by AI has become a critical topic of discussion in legal and policy circles. The question of liability in the context of AI is complex and multifaceted, and involves a range of legal, ethical, and practical considerations. One key challenge is the fact that AI systems can operate autonomously and make decisions independently, raising questions about who should be held responsible in the event of harm or damage. Additionally, AI systems are often trained on large datasets, which can contain biases and inaccuracies that can result in discriminatory or harmful outcomes.

INDIAN LIABILITY FRAMEWORK FOR AI HARM OR DAMAGE:

In India, the legal framework for AI harm or damage is governed by the tort law. Liability can be imposed under the principles of strict liability, negligence, and vicarious liability. Strict liability applies when harm is caused by a defect in the AI system, and the injured party does not need to prove fault. Negligence applies when harm is caused by the failure to exercise reasonable care in the development, design, or operation of the AI system. Vicarious liability applies when the AI system is owned and operated by a third party, and the third party is held liable for the harm caused by the AI system.

The Indian Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the Personal Data Protection Bill, 2019 are two relevant regulations related to AI harm or damage in India. These regulations establish the obligation of organisations to implement reasonable security practices and procedures to safeguard sensitive personal data or information from unauthorised access, use, disclosure, and destruction.

TYPES OF AI HARM OR DAMAGE IN INDIA:

In India, AI harm or damage can take various forms, including physical harm, financial harm, and reputational harm. Physical harm can



occur due to a malfunction in an autonomous vehicle or a surgical robot. Financial harm can result from automated trading algorithms, while reputational harm can result from the misuse of personal data or biased algorithms that discriminate against certain groups. For example, in the Aadhaar data breach case, over 1 billion Indian citizens' personal data, including biometric data, was leaked due to a security flaw in the Aadhaar database, causing reputational harm to the government and UIDAI (Unique Identification Authority of India).

LEGAL RESPONSIBILITY FOR AI DECISIONS:

As AI systems become more complex and involved in decision-making processes, it raises important questions about who should be held legally responsible when an AI system causes harm or makes a mistake. Assigning legal responsibility to an AI system itself may be difficult or even impossible, since AI systems are typically designed and operated by humans. As a result, legal frameworks for assigning responsibility for AI decisions may need to consider the roles of different human actors involved in developing and using AI systems, such as the designers, programmers, and users of AI systems. In addition, legal responsibility may be shared among multiple parties, such as when an AI system is developed by one company and used by another. There are also questions about how to hold individuals or organisations accountable for harms that may arise from "black box" AI systems, where the decision-making processes are not transparent and may be difficult to understand or interpret.

PRODUCT LIABILITY FOR AI SYSTEMS:

AI systems can be considered products, and as such, may be subject to product liability laws in the event that they cause harm. However, applying existing product liability laws to AI systems may be challenging, given the unique features of these systems. For example, AI systems may involve complex and opaque decision-making processes, making it difficult to identify and address defects. In addition, the human role in developing and using AI systems may complicate the analysis of defects, since

human decisions may affect the functioning of the AI system. Nonetheless, it is important for legal frameworks to account for the potential risks of harm posed by AI systems, and to provide appropriate legal remedies for individuals who are harmed by defective AI products. In addition to product liability, AI systems may also be subject to tort liability if they cause harm. Tort liability is a broader concept that includes a range of legal wrongs, such as negligence, strict liability, and intentional torts. In the context of AI, tort liability may be particularly challenging to establish, given the difficulty of proving causation and harm. For example, it may be difficult to determine whether an AI system was the actual cause of harm, or whether other factors were involved. Similarly, it may be difficult to establish the extent of harm caused by an AI system, particularly if the harm is diffuse or indirect. Nonetheless, legal frameworks may need to account for the possibility of tort liability in the context of AI systems, particularly as these systems become more pervasive and involved in decision-making processes.

INSURANCE FOR AI SYSTEMS:

As the risks of AI-related harm become more apparent, it may become necessary to develop specialised insurance products to cover these risks. However, pricing and underwriting such insurance products may be challenging, given the uncertainties surrounding the risks of AI-related harm. For example, it may be difficult to assess the likelihood and severity of harm caused by AI systems, particularly as these systems become more complex and opaque. Nonetheless, specialised insurance products may be important for managing the risks associated with AI systems, particularly as they become more pervasive in a range of industries and contexts.

COMPARISON OF INDIAN LIABILITY FRAMEWORK WITH OTHER COUNTRIES:

The liability framework for AI harm or damage varies in different countries. In the United States, the legal framework is similar to India's, where the principles of strict liability, negligence, and

vicarious liability apply. However, in the European Union, the liability framework is more stringent, as the EU has proposed a regulation that would establish a mandatory insurance requirement for AI systems. This would ensure that compensation is available in the event of AI harm or damage, even if the injured party is unable to prove fault or negligence. In India, the principles of proportionality and reasonableness apply to AI harm or damage. The principle of proportionality suggests that the level of responsibility should correspond to the level of control the AI system has over the harm or damage. The principle of reasonableness suggests that the standard of care should be determined by what is reasonable under the circumstances. The Indian case of *K.R. Purushothaman v. Union of India and Others* is an example of a case where AI harm occurred due to negligence. In this case, a glitch in the computerised evaluation system resulted in an incorrect valuation of answer sheets. The court held the authorities liable for. Another relevant principle in India is the doctrine of 'res ipsa loquitur,' which means 'the thing speaks for itself.' This principle applies when the harm or damage caused by the AI system is so obvious that it can be inferred that the defendant was negligent. For example, if an autonomous vehicle crashes into a pedestrian, it can be inferred that the manufacturer was negligent, as the vehicle is designed to prevent such accidents.

Another Indian case relevant to AI harm or damage is the case of Aadhaar data breach mentioned earlier. In this case, the government and UIDAI were held responsible for the data breach and were ordered to take steps to improve data security. This case highlights the importance of implementing reasonable security practices and procedures to prevent harm or damage caused by AI systems.

In terms of liability for harm caused by biased AI systems, the Indian Constitution and the Information Technology Act, 2000 provide protection against discrimination based on race, gender, religion, and other factors. The

Supreme Court of India has also recognized the right to privacy as a fundamental right under the Indian Constitution, which may be violated by the use of biased AI systems.

In comparison to other countries, India's liability framework for AI harm or damage is relatively similar to that of the United States, with principles of strict liability, negligence, and vicarious liability applying. However, the European Union's proposed mandatory insurance requirement for AI systems goes beyond India's liability framework and may provide greater protection for injured parties.

INTERNATIONAL COVENANTS.

The legal frameworks for liability for AI-related harm may vary across different countries and regions, which could create challenges for the development and use of AI systems across international borders. The following are the few international bodies and statutes

- *United Nations Guiding Principles on Business and Human Rights: These principles were endorsed by the UN Human Rights Council in 2011 and provide a framework for businesses to respect human rights, including the right to remedy for harms caused by their activities, products, or services.*
- *The Organisation for Economic Co-operation and Development (OECD) Principles on Artificial Intelligence: These principles were adopted in May 2019 and outline five principles for the responsible development and deployment of AI, including the principle of accountability, which states that those responsible for developing, deploying, or operating AI systems should be accountable for their proper functioning and any harm caused.*
- *The European Union's General Data Protection Regulation (GDPR): The GDPR, which came into effect in May 2018, sets out rules for the protection of personal data and imposes liability on data controllers and processors for any harm caused by their processing activities.*

- *The Council of Europe's Convention on Cybercrime: This convention, which was adopted in 2001, aims to harmonize national laws related to cybercrime, including the criminalization of certain acts related to computer systems, and includes provisions related to liability for damage caused by cybercrime.*

Harmonising liability laws across international borders may be particularly challenging

THE WAY FORWARD:

The intersection of artificial intelligence (AI) and law presents both opportunities and challenges. On the one hand, AI has the potential to transform the legal industry by making legal research and analysis more efficient, improving access to justice, and even helping to predict legal outcomes. On the other hand, AI raises significant ethical and legal questions, such as who is liable when an AI system causes harm or makes a mistake, and how to ensure that AI systems are transparent, unbiased, and trustworthy.

To move forward in this area, several steps can be taken. One is to continue to develop and refine AI systems that can assist legal professionals in their work. For example, AI can help lawyers to review large amounts of data, identify relevant cases and statutes, and even predict legal outcomes. However, it is important that these systems are transparent and explainable so that legal professionals can understand how they arrived at their recommendations.

Another important step is to establish legal frameworks and regulations that address the unique challenges posed by AI. For example, liability laws may need to be updated to account for the fact that AI systems can cause harm or make mistakes, and regulations may need to be put in place to ensure that AI systems are transparent, fair, and trustworthy.

Finally, it is important to engage in public debate and education around AI and the law. This includes not only educating legal professionals and policymakers about the potential benefits and risks of AI, but also

involving the public in discussions about how AI should be regulated and deployed in the legal industry.

CONCLUSION:

The increasing use of AI systems in various industries in India and other countries raises the potential for harm or damage caused by these systems. The liability framework for AI harm or damage in India is governed by the principles of strict liability, negligence, and vicarious liability. Indian regulations, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the Personal Data Protection Bill, 2019, impose obligations on organizations to implement reasonable security practices and procedures to safeguard sensitive personal data or information from unauthorised access, use, disclosure, and destruction. Principles such as proportionality, reasonableness, and 'res ipsa loquitur' are relevant to AI harm or damage in India, and the Aadhaar data breach case highlights the importance of implementing reasonable security practices and procedures. India's liability framework for AI harm or damage is relatively similar to that of the United States, while the European Union's proposed mandatory insurance requirement for AI systems may provide greater protection for injured parties.

REFERENCES:

1. Berman, D., & Yu, H. (2018). The promise and perils of machine learning algorithms in employment decision-making. *George Washington Law Review*, 87(6), 1681-1714.
2. Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *SSRN Electronic Journal*.
3. Calo, R. (2017). Liability for autonomous systems. *University of Washington School of Law Research Paper*, 2017(08).
4. Chopra, K., & Ravi, S. S. (2020). Artificial intelligence and liability: Indian perspectives. *International Journal of Law and Management*, 62(2), 226-240.



5. Daga, A. (2020). Emerging AI and its Liability Regime in India. *International Journal of Scientific Research*, 9(7), 102-105.
6. Dignum, V., & Dignum, F. (2018). Ethics and liability of artificial intelligence. *Science and Engineering Ethics*, 24, 1485-1498.
7. European Commission. (2018). Liability for artificial intelligence and other emerging digital technologies. Brussels: European Commission.
8. European Commission, "A European approach to excellence and trust in AI," 2021.
9. European Union Agency for Cybersecurity. (2021). Legal aspects of cybersecurity: liability and new technologies. European Union Agency for Cybersecurity.
10. Indian Constitution.
11. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
12. Information Technology Act, 2000.
13. K.R. Purushothaman v. Union of India and Others, 1995 SCC (5) 467.
14. Katz, D. M., & Callier, S. (2020). Liability for artificial intelligence under US law. *AI & Society*, 35, 677-683.
15. K.S. Puttaswamy v. Union of India (2017)
16. Li, R., Liang, Q., & Li, Y. (2021). Product liability for artificial intelligence. *AI & Society*, 36, 645-656.
17. Mangan, C. (2020). Liability for autonomous systems in the era of artificial intelligence. *Journal of International Affairs*, 73(1), 107-126.
18. Morgan, S., & Liang, X. (2019). Artificial intelligence and the law. *Annual Review of Law and Social Science*, 15, 537-550.
19. Pasquale, F. (2018). Artificial intelligence and the future of legal services. *Fordham Law Review*, 87(5), 2321-2347.
20. Raja, R. A., & Gupta, A. (2020). Artificial Intelligence and Law: A Study on Liability for Harm or Damage Caused by AI. *International Journal of Advanced Science and Technology*, 29(8), 3742-3755.
21. Singla, S., & Singh, S. (2020). Artificial intelligence: An emerging risk and liability scenario. *Journal of Insurance and Financial Management*, 2(2), 38-53.
22. Singh, A. (2019). Artificial Intelligence: Liability Framework in India. *International Journal of Advanced Research in Computer Science*, 10(6), 167-171.
23. Vashistha, A., & Gupta, R. (2021). Understanding Artificial Intelligence and Its Legal Challenges in India. *International Journal of Information Technology and Computer Science*, 13(2), 59-64.
24. Weber, R. H. (2020). Insuring artificial intelligence. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45, 462-483.