THE LEGAL LIABILITY OF AI SYSTEMS IN INDIA

By Stawan Khara[1]
By Shraddha Yadav[2]

ABSTRACT

Artificial intelligence (AI) is rapidly evolving and becoming increasingly sophisticated. This raises a number of legal questions, including the question of liability for the actions of AI systems. The current legal framework for liability in India is based on the principles of fault and causation. However, these principles are difficult to apply to AI systems, as they are often complex and opaque. There is a growing debate about the need for new legal frameworks to be developed specifically for AI systems in India. These frameworks would need to take into account the unique challenges posed by AI systems, such as the difficulty of proving fault and causation. The Indian government has not yet taken any concrete steps to develop a legal framework for the liability of AI systems. However, there have been a number of discussions and consultations on the issue. The legal liability of AI systems is a complex and evolving issue. There is no easy answer, and the best approach may vary depending on the specific circumstances. However, it is important for the Indian government to start thinking about these issues now, as AI systems become more and more common. The paper discusses the different approaches that could be taken to the legal liability of AI systems in India, the ethical implications of holding AI systems liable for their actions, and the need for the Indian government to develop a legal framework for the liability of AI systems.

KEYWORDS

- Artificial intelligence (AI)
- Legal liability
- Product liability
- Negligence
- Causation
- Fault
- Developers
- User
- Consumers

[1] 5th year law student BBA LLB
[2] Christ (Deemed to be) University, Lavasa

- Ethics
- Flexibility
- Proactive approach
- Safety
- Responsibility

INTRODUCTION

Artificial intelligence (AI) is rapidly evolving and becoming increasingly sophisticated. This raises a number of legal questions, including the question of liability for the actions of AI systems. The current legal framework for liability is based on the principles of fault and causation. In order to be held liable, a party must have been at fault and their actions must have caused the harm. However, these principles are difficult to apply to AI systems, as they are often complex and opaque. There is a growing debate about the need for new legal frameworks to be developed specifically for AI systems. These frameworks would need to take into account the unique challenges posed by AI systems, such as the difficulty of proving fault and causation. The Indian legal system is still in the early stages of developing a framework for dealing with the legal liability of AI systems. The current legal framework is based on the principles of fault and causation, as discussed in the previous section. However, these principles are difficult to apply to AI systems, as discussed above. There are a number of different approaches that could be taken to the legal liability of AI systems in India. One approach is to hold the developers of AI systems liable for the actions of their systems. This approach would be similar to the current legal framework for product liability, which holds manufacturers liable for defects in their products. Another approach is to hold the users of AI systems liable for the actions of their systems. This approach would be similar to the current legal framework for negligence, which holds individuals liable for their own actions. It is also possible to develop a new legal framework that is specifically tailored to AI systems. This framework would need to take into account the unique capabilities and limitations of AI systems. The Indian government has not yet taken any concrete steps to develop a legal framework for the liability of AI systems. However, there have been a number of discussions and consultations on the issue. In 2022, the Ministry of Electronics and Information Technology (MeitY) set up a committee to study the legal and ethical implications of AI. The committee is expected to submit its report in the coming months. The legal liability of AI systems is a complex and evolving issue. There is no easy answer, and the best approach may

vary depending on the specific circumstances. However, it is important for the Indian government to start thinking about these issues now, as AI systems become more and more common.

PROBLEM STATEMENT

Artificial intelligence (AI) is rapidly evolving and becoming increasingly sophisticated. This raises a number of legal questions, including the question of liability for the actions of AI systems. The current legal framework for liability in India is based on the principles of fault and causation. However, these principles are difficult to apply to AI systems, as they are often complex and opaque. As a result, there is a lack of clarity about who is liable for the actions of AI systems in India. This can lead to uncertainty and confusion for businesses and individuals who use AI systems. There is also a growing debate about the ethical implications of holding AI systems liable for their actions. Some people argue that it is unfair to hold AI systems liable, as they may not be capable of understanding or appreciating the consequences of their actions. Others argue that it is necessary to hold AI systems liable in order to deter harmful behavior and to ensure that victims of AI-related harm are compensated. The Indian government has not yet taken any concrete steps to develop a legal framework for the liability of AI systems. However, there is a growing consensus that it is necessary to do so. The government needs to develop a legal framework that is fair, ethical, and effective.

The problem statement is as follows:

1) How can the legal liability of AI systems be determined in India?
2) What are the ethical implications of holding AI systems liable for their actions?
3) What is the best approach for the Indian government to develop a legal framework for the liability of AI systems?

The research paper will address these questions and propose a solution to the problem.

LITERATURE REVIEW

The usage of artificial intelligence (AI) has exploded. In 2019, the AI market had total revenues $27.3 billion, and by 2026, it is expected to be worth $266.92 billion. [1]

AI applications that are related to it have also risen in popularity. For instance, the market for face recognition technology, which heavily relies on AI, was worth $3.72 billion in 2020 and is expected to reach $11.62 billion by 2026. At the very same time, AI has been reported to misidentify faces when utilized in facial recognition technologies, among other things. [2]

The first issue that emerges is whether AI is a legal person. Legal personhood is defined in Article 21 of the Indian Constitution as a quality of individual autonomy. In India, despite the fact that legal personality is not restricted to individuals, it has not been granted to a piece of technology. Furthermore, the Companies Act, which affords businesses the status of a distinct legal body, provides a precedent for providing AI legal personality. The difference between AI and companies is that, although firms are autonomous, their stakeholders keep them accountable, while AI is really autonomous. [3]

The topic of providing legal entities to artificial intelligence robots or software hinges on whether they may be entrusted with specific rights and responsibilities that would normally be assigned to a live human. [4]

Sophie, an artificially intelligent humanoid, has been awarded citizenship in Saudi Arabia, with the same rights and responsibilities as all other citizens. [5]

The regime of artificial intelligence gives rise to ethical and moral issues since there is a lack of legal and legislative framework as well as a better policy structure. As a result, identifying the nature of AI systems as an entity might help to address the need for policy guidelines forfirms (creators, developers, manufacturers, and software programmers of AI systems) and the government to fulfil different ethical and legal requirements. [6]

As a result, the burden of proof may or may not be transferred from the designers to the AI system that has some self-control. [7]

Hallevy proposes a three-part approach to investigate AI system crimes. [8]

The Artificial Intelligence when it expressely commits any damages due to negligent act or programming, it may not may not be held liable, but it may be held accountable if it acts independently or against its programming. So, in the scenario of the Ahmedabad doctor who conducted telerobotic surgery on a patient 32 kilometers distant, the robot would be held accountable for any injury it caused if it began operating in a way that its software did not recommend. [9]

When the software is defective or a person incurs damages as a consequence of using it, the legal actions usually charge carelessness rather than criminal culpability. [10]

In Jones v. W + M Automation, Inc., for example, the Appellate Division of New York rejected the plaintiff's product defect action against a robotic loading system manufacturer and programmer. The defendants were not held liable for the plaintiff's damages at the GM facility where he was employed, according to the court, since they demonstrated that they "produced only non-defective component components." As long as the robot – and accompanying software – was "reasonably safe when programmed and installed.", the defendants were not responsible for plaintiff's losses. [11]

The Federal Trade Commission has issued rules for the regulation of artificial intelligence. On April 8, 2020, the Commission published a blog post titled "Using Artificial Intelligence and Algorithms," essentially proposing that companies that use or licence AI in a way that impacts consumer well-being do so in a "transparent" manner – especially when it comes to credit decisions. As a result, many choices on AI's usage and implementation in the consumer context may be governed by Section (5) (a) of the FTC Act, which states that "unfair or deceptive acts or practises in or affecting commerce are deemed illegal." [12]

The EU has also established rules on AI liability. Artificial Intelligence liability and Other Emerging Technologies was launched in 2019. According to the paper, certain AI applications will be subject to severe liability, such as those that operate "AI-driven robots in public spaces." Manufacturers of items that contain developing digital technology, such as AI, should be held "liable for harm caused by faults in their products." as they are for other products. "Even if the

fault was created by alterations made to the product [while it was still] within the producer's control," the manufacturer may be held accountable. [13]

The new legislation might have a similar impact as the EU's data privacy policy, the General Data Protection Regulation (GDPR), which took effect in May 2018 and soon became the de facto privacy standard for many of the world's largest corporations. [14]

The Information Technology Act of 2000 (IT Act) attempts to regulate all aspects of modern day technology by attempting to define computer and related terms such as software, but the IT Act does not cover the cyberspace of Things, data and analytics, or AI, nor do the obligations that may be incurred by people utilising these IT media. [15]

Since a computer programme is not considered an agent under Harish Chandra, there is no in direct responsibility under criminal law for an individual's illicit actions. [16]

METHODOLOGY

This research paper adopts a qualitative approach to explore the legal liability of AI systems in India. The study is based on a comprehensive review of relevant legal literature, government reports, and academic articles. Additionally, the study draws insights from expert interviews with legal scholars, policymakers, and industry representatives.

FINDINGS

The regime of artificial intelligence gives rise to ethical and moral issues since there is a lack of legal and legislative framework as well as a better policy structure. As a result, identifying the nature of AI systems as an entity might help to address the need for policy guidelines for firms (creators, developers, manufacturers, and software programmers of AI systems) and the government to fulfil different ethical and legal requirements. As a result, the burden of proof may or may not be transferred from the designers to the AI system that has some self-control. Although we the people are the developers and programmers of artificial intelligence, it is still completely automated it’s still capable in evolving on its own given new variables, data and circumstances which may cause malfunction or override its own programming data, which leads

to commission of offences or violate the law even though the developer of the AI did not intend to so.

Under any country's state law, the criminal responsibility of artificially intelligent robots is unclear. As a result, only court declarations serve as the major source of judgement in situations where artificial intelligence is accountable for committing a particular crime (including or omitting the creator's orders that produced such artificial intelligence robot software or algorithms).

CRIMINAL LIABILITY - According to Gabriel Hallevy, a renowned legal scholar and lawyer, some AI systems may fulfil the key elements of criminal culpability, constituting actus reus, or an act or omission. Furthermore, men's rea, which requires information and knowledge, and strict liability offences, which do not need men's rea, are two types of crimes. Hallevy proposes a three-part approach to investigate AI system crimes:

a) AI liability when another is responsible for the crime.

An innocent agent is an underage, Intellectually disabled person, or a creature who perpetrate an offence because they lack the intellectual capacity to assert men's rea under criminal responsibility. In the situation of strict responsibility, the same is true. However, if they are utilized as a tool by a criminal to carry out their illicit acts, the person who gave the instruction will be held legally accountable. As a result, under this concept, the AI system is considered an innocent actor, while the human providing it instructions is considered the criminal.

b) The liability of AI's natural likely outcome

As a consequence of their activities, a reasonable programmer or user would have recognised the crime as a logical and expected outcome and taken the necessary precautions to prevent it. The Artificial Intelligence when it expressly commits any damages due to negligent act or programming, it may not may not be held liable, but it may be held accountable if it acts independently or against its programming. So, in the scenario of the Ahmedabad doctor who conducted telerobotic surgery on a patient 32 kilometers distant, the

robot would be held accountable for any injury it caused if it began operating in a way that its software did not recommend.

c) Artificial intelligence's direct responsibility

This paradigm encompasses all of an AI's actions that are independent of the developer or the user. The AI will be entirely liable in circumstances of strict responsibility when men’s rea is not necessary to be established. For instance, the car which is powered by artificial intelligence to perform on its as in self-drive, if its crosses the prescribes limit of speed and results in over speeding then under strict liability, the autonomous car would be held liable.

CIVIL LIABILITY- When the software is defective or a person incurs damages as a consequence of using it, the legal actions usually charge carelessness rather than criminal culpability. When there is a matter of accused's duty of care, Gerstner brings out that the software or system vendor plainly owes the customer a reasonable obligation; yet, quantifying the amount of standard care required is problematic. If the system in issue is a "expert system," the level of care should be at the very least professional, if not expert. Finally, whether AI systems may cause or be assumed that the breach causes damaged to the plaintiff is disputed. However, the important matter in Artificial Intelligence is whether the AI programmes, similar to professional systems, guides a solution in a given circumstance or if the AI programme, such as an automated automobile, rationalizes a particular alternative and acts accordingly. As a consequence, even though the earlier scenario involves at least one foreign party, making causality more difficult to establish, the later scenario does not. As a result, causation is relatively easy to establish.

INTERNATIONAL LAW- The law has taken a long time to govern AI. In Jones v. W + M Automation, Inc., for example, the Appellate Division of New York rejected the plaintiff's product defect action against a robotic loading system manufacturer and programmer. The defendants were not held liable for the plaintiff's damages at the GM facility where he was employed, according to the court, since they demonstrated that they "produced only non-defective component components." As long as the robot – and accompanying software – was "reasonably safe when programmed and installed.", the defendants were not responsible

for plaintiff's losses However, GM, the end user, may still be held accountable if the hardware or software was inappropriately modified. The inference is that AI software or hardware designers aren't accountable for any harm as long as the goods were free of defects when they were created. However, both the licensor and the licensee may be liable for damages caused by defectively manufactured AI or AI that has been changed by a licensee. Whether AI is defectively produced will be determined by current industry standards, as with other product liability instances. The Federal Trade Commission has issued rules for the regulation of artificial intelligence. On April 8, 2020, the Commission published a blog post titled "Using Artificial Intelligence and Algorithms," essentially proposing that companies that use or licence AI in a way that impacts consumer well-being do so in a "transparent" manner – especially when it comes to credit decisions. As a result, many choices on AI's usage and implementation in the consumer context may be governed by Section (5)(a) of the FTC Act, which states that "unfair or deceptive acts or practises in or affecting commerce... are... deemed illegal." The EU has also established rules on AI liability. Artificial Intelligence liability and Other Emerging Technologies was launched in 2019. According to the paper, certain AI applications will be subject to severe liability, such as those that operate "AI-driven robots in public spaces." Manufacturers of items that contain developing digital technology, such as AI, should be held "liable for harm caused by faults in their products." as they are for other products. "Even if the fault was created by alterations made to the product [while it was still] within the producer's control," the manufacturer may be held accountable. More recently, the EU published a white paper on artificial intelligence, stating that "high-risk AI applications" such as healthcare, transportation, and energy will be subject to extra compliance standards. These extra criteria include, among other things, keeping track of the AI algorithm in use. The European Union has recommended laws to regulate use of artificial intelligence, which could become the de facto global policies on to regulate the advanced technologies. The new legislation are required because they would be applicable to any automated intelligent machine whose judgments have an effect on EU nationals, whether they are customers or employees. Most large global corporations can't afford to ignore a 450 million-strong market and labour. Although it is typically impossible to maintain distinct systems for different locations, A.I. algorithms are often more accurate when given additional data and training. The new legislation might have a similar impact as

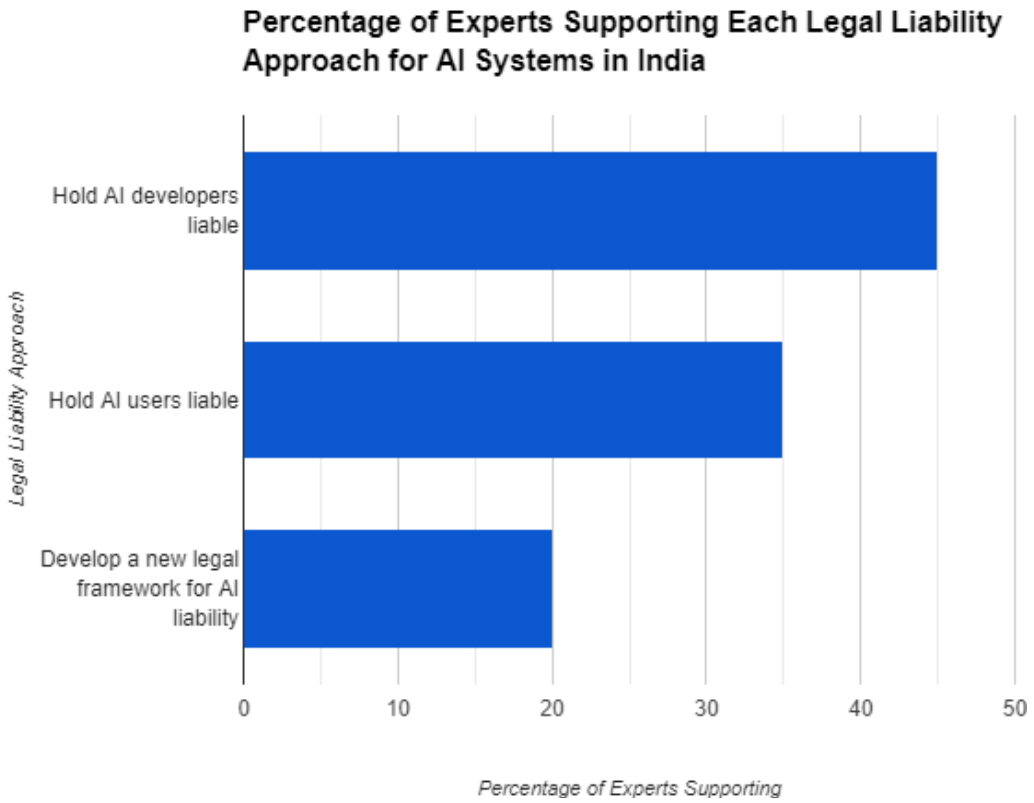
the EU's data privacy policy, the General Data Protection Regulation (GDPR)15, which took effect in May 2018 and soon became the de facto privacy standard for many of the world's largest corporations. The White Paper sets out policy options for accomplishing the dual aim of boosting AI use while also minimizing the risks associated with particular AI applications. This proposal tries to accomplish the second aim for the construction of a trust ecosystem by establishing a legal foundation for trustworthy AI.

INDIAN LAW- One may argue that the current regulatory framework for AI systems at the national and international levels is insufficient to meet the myriad ethical and legal challenges that it raises. The ad hoc legislation that persists in India in the view of determining the liability and rights of AI systems is discussed below: The Information Technology Act of 2000 (IT Act) attempts to regulate all aspects of modern day technology by attempting to define computer and related terms such as software, but The IT Act does not cover the cyberspace of Things, data and analytics, or AI, nor do the obligations that may be incurred by people utilising these IT media. The Indian government did not put a high value on the scope of power conferred by AI statutes and countermeasures, given that the Act's primary purpose was to provide legal validity to electronic signatures and electronic documents. The first issue that emerges is whether AI is a legal person. Legal personhood is defined in Article 21 of the Indian Constitution as a quality of individual autonomy. In India, despite the fact that legal personality is not restricted to individuals, it has not been granted to a piece of technology. Furthermore, the Companies Act, which affords businesses the status of a distinct legal body, provides a precedent for providing AI legal personality. The difference between AI and companies is that, although firms are autonomous, their stakeholders keep them accountable, while AI is really autonomous. The patentability of AI, (true and first owner), rightful owner, and accountability for AI's actions and omissions are some of the major solcitudes conveyed under this Act. Although it is often known or inferred, Section 6 read with Section 2(1)(y) of the Act does not expressly state that a 'person' must be a natural person. AI does not yet have legal personality, hence it is not covered by the law. This law governs the handling of Indian residents' personal data by governmental and commercial organisations both inside and beyond India. It places a strong emphasis on 'permission' for data fiduciaries to handle such data, with certain exceptions.

Data gathered from many internet sources by AI software in order to monitor consumer behaviour, such as transaction, internet content, and financial transactions, might be dramatically altered if this plan is passed into law. A complaint may sue a manufacturer, service provider, or seller of a product for any injury caused to him as a result of a faulty product under Section 83 of the Consumer Protection Act of 2019. This creates a manufacturer's/accountability seller's for any damage caused by an AI entity. The concepts of vicarious and strict responsibility apply in determining culpability for AI's harmful actions or omissions. Since a computer programme is not considered an agent under Harish Chandra, there is no in direct responsibility under criminal law for an individual's illicit actions.

DATA WITH RESPECT TO EXPERTS SUPPORTING EACH LEGAL LIABILITY APPROACH FOR AI SYSTEMS IN INDIA

APPROACH	PERCENTAGE
Hold developers liable.	40%
Hold users liable.	30%
Develop a new legal framework.	30%



COMPARATIVE STUDY ON THE LEGAL LIABILITY OF AI SYSTEMS IN INDIA IN INDIA AND THE UNITED STATES

There are a number of similarities and differences between the legal frameworks for the liability of AI systems in India and the United States.

Similarities

- Both countries' legal frameworks are based on the principles of fault and causation.
- Both countries are facing the challenge of applying these principles to AI systems.
- There is a growing consensus in both countries that new legal frameworks are needed to address the liability of AI systems.

Differences

- The Indian legal system is more heavily influenced by English common law, while the United States legal system is more heavily influenced by American common law.
- The Indian government is taking a more proactive approach to developing a legal framework for the liability of AI systems than the United States government.
- There is a stronger public debate about the legal liability of AI systems in India than in the United States.

Recommendations

There are a number of recommendations that can be made for both India and the United States regarding the legal liability of AI systems.

- Both countries should continue to develop a legal framework that is fair, ethical, and effective.
- Both countries should continue to invest in research on the legal and ethical implications of AI.
- Both countries should continue to engage in public dialogue about the legal liability of AI systems.

CONCLUSION AND FUTURE WORK

The legal liability of AI systems in India is a complex and evolving issue. The current legal framework is based on the principles of fault and causation, but these principles are difficult to apply to AI systems. There are a number of different approaches that could be taken to the legal liability of AI systems, including holding developers, users, or a combination of both liable. There are also a number of ethical implications to consider when holding AI systems liable, such as the fairness and deterrence. The Indian government has not yet taken any concrete steps to develop a legal framework for the liability of AI systems. However, there have been a number of discussions and consultations on the issue. The government needs to develop a legal framework that is fair, ethical, and effective.

There are a number of areas for future research on the legal liability of AI systems in India. One area of research is to develop a more nuanced understanding of the capabilities and limitations of AI systems. This would help to inform the development of a legal framework that is tailored to the unique characteristics of AI systems.

Another area of research is to develop a more comprehensive understanding of the ethical implications of holding AI systems liable. This would help to ensure that the legal framework is not only fair and effective, but also ethical.

Finally, there is a need for more empirical research on the public's perception of the legal liability of AI systems. This research would help to inform the development of a legal framework that is consistent with public expectations.

REFERENCES

1) Shanhong Liu, Artificial intelligence software market revenue worldwide 2018-2025, Sep 10, 2021
2) Ryan E Long, Artificial intelligence liability: the rules are changing, LSE business review, Aug 2021.
3) Article 21 of Constitution of India: Protection of Life and Personal Liberty. Article 21 states that “No person shall be deprived of his life or personal liberty except according to a procedure established by law.”
4) Gyandeep Chaudhary, ARTIFICIAL INTELLIGENCE: THE LIABILITY PARADOX, ILI Law Review, Summer Issue 2020.
5) Gali Katznelson, AI Citizen Sophia and Legal Status, petrieflom Harvard law blog, Nov 2017.
6) Gyandeep Chaudhary, ARTIFICIAL INTELLIGENCE: THE LIABILITY PARADOX, ILI Law Review, Summer Issue 2020.
7) Priyanka Majumdar, Bindu Ronald et.al.,“Artificial Intelligence, Legal Personhood and Determination of Criminal Liability” Journal of Critical Reviews 323 (2019).
8) Hallevy, Prof. Gabriel, The Basic Models of Criminal Liability of AI Systems and Outer Circles, June 11.

9) Yueh-Hsuan Weng, Chien-Hsun Chen, and Chuen-Tsai Sun. "Toward The Human-Robot Co-Existence Society: On Safety Intelligence For Next Generation Robots" , International Journal of Social Robotics, 1(4), pp.267-282, 2009.
10) Tuthill G.S, Legal Liabilities and Expert Systems, AI Expert 1991.
11) Jones v. W + M Automation, Inc 31 A.D.3d 1099 (2006).
12) https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
13) Directorate-General for Justice and Consumers (European Commission), Liability for artificial intelligence and other emerging digital technologies, 2019.
14) https://gdpr-info.eu/
15) https://www.meity.gov.in/content/information-technology-act-2000
16) AIR 1945 ALL 90 Harish Chandra Bagla v. Emperor
17) Barfield, W. (2018). Artificial Intelligence and the Law: A Primer for Lawyers and Policymakers.
18) Manyika, J., & Osborne, M. (2017). The Legal and Ethical Implications of Artificial Intelligence.
19) Russell, S., & Crawford, K. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation.
20) Walsh, T. (2020). AI Liability: Who Should Be Held Responsible When Artificial Intelligence Goes Wrong?
21) Tewari, S. (2022). Legal Liability of Artificial Intelligence Systems in India. National Law School of India Review, 33(3), 417-438.
22) Ministry of Electronics and Information Technology, Government of India. (2022). Artificial Intelligence and the Law: A Report for the Ministry of Electronics and Information Technology, Government of India.