Page 2367 - 2374 **DOI:** *https://doij.org/10.10000/IJLMH.116377*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

AI Liability and Accountability: A Complex Landscape in an Evolving World

VISMITHA S[1] AND SRI VIJAI[2]

ABSTRACT

Artificial intelligence (AI) is rapidly transforming our world, with applications in virtually every industry and sector. As AI systems become more powerful and autonomous, it is essential to consider the potential for damages that they could cause. Imagine AI breaches the codes of law or causes any damage, who is liable for damages caused? This is a complex question with no easy answer. Liability will depend on the specific facts and circumstances of each case, as well as the applicable legal framework. However, there are a number of factors that could be considered, including the designer, developer, manufacturer, owner, operator, and user of the AI system, as well as any third-party that contributed to its development or use. In addition to the question of liability, there is also the question of accountability. Who should be held accountable for AI damages? This is a broader question, encompassing not only legal responsibility, but also moral and ethical responsibility. Accountability is important because it helps to ensure that those who are harmed by AI systems have access to justice and that those involved in the development and use of AI systems are held responsible for their actions. There are a number of challenges to developing a legal framework for AI liability and accountability. One challenge is the complexity of AI systems. It can be difficult to determine who is at fault when an AI system malfunctions, especially if the system is being used in a complex or unexpected way. Another challenge is the difficulty of anticipating all of the potential ways in which AI systems could cause harm. AI systems are constantly evolving, and new applications are being developed all the time. This makes it difficult to develop laws and regulations that can keep up with the pace of change. Despite these challenges, it is important to develop a legal framework for AI liability and accountability. Therefore, this research article aims to discuss the liability and accountability regimes in place and its flaws to help to protect the public from harm and ensure that the benefits of AI are realized in a responsible and equitable manner.

[1] Author is a student at SASTRA Deemed University, India.
[2] Author is a student at SASTRA Deemed University, India.

 [ISSN 2581-5369]

I. INTRODUCTION

In the grand tapestry of human innovation, few threads have been as transformative as the rise of Artificial Intelligence (AI). But what exactly is AI? It's a branch of computer science that aims to create systems capable of performing tasks that would normally require human intelligence. These tasks range from learning from data, reasoning, problem-solving, and understanding natural language, to making informed decisions. Essentially, AI strives to mimic human-like cognitive functions in machines, enabling them to learn from data, adapt to new situations, and perform tasks that typically require human intelligence.

AI's influence has spread far and wide, with its applications seeping into virtually every industry and sector. However, the rise of AI has also brought about unique challenges to existing legal frameworks. Courts are grappling with complexities introduced by AI systems as traditional legal doctrines are put to the test.

This article delves into the civil liability that can be attributed to AI. The liability for damages caused by AI has been a controversial subject as there is a lot of ambiguity in fixating on the kind of liability to be attracted and to whom it must be subjected. The 'Black-Box Paradox', a term coined to describe the opacity of AI decision-making processes, further complicates matters.

The need for a comprehensive governance framework and an effective international legal response is increasingly being recognized. Nonetheless, creating such a framework is not without its challenges. This article also analyses the use of the sandbox approach to regulate high-risk AI in India.

II. CURRENT STATUS OF AI IN INDIA

In the rapidly evolving digital landscape of India, the legal status of Artificial Intelligence (AI) remains undefined. Despite the government's recognition of AI as a crucial area for legal and policy deliberation, and its efforts to nurture a digital economy, there is a conspicuous absence of specific legislation addressing AI.

The call for AI to be granted a legal status akin to that of a corporation is growing louder, yet such a status remains elusive. However, this does not imply a governmental disregard for AI and its potential impact. On the contrary, the Indian government is actively promoting the digital economy, with AI as a focal point.

The proposed Digital India Act (DIA) is poised to bring AI regulation under its purview. The Union Budget 2023-24 underscored the government's commitment to 'Making AI in India and

 [ISSN 2581-5369]

Making AI work for India', which includes the establishment of three 'Centres of Excellence' dedicated to AI research.

Government bodies such as the Ministry of Electronics and Information Technology (MeiTY), NITI Aayog, Telecom Regulatory Authority of India (TRAI), and the Department of Telecommunications (DoT) are deeply engaged in this domain. Industry-led initiatives include NASSCOM's Responsible AI Resource Kit and 'Future Skills Prime' programme.

Efforts to foster AI technology and social skills among the youth are evident in programs like 'Responsible AI for Youth' and 'Youth for Unnati and Vikas with AI'. Internationally, India plays a significant role in the Global Partnership on Artificial Intelligence (GPAI), a collaborative initiative supporting advanced research on AI-related priorities.

The legal landscape of AI in India can be likened to a ship navigating uncharted waters. While there are no specific laws governing AI currently, the government's openness to considering such regulations shines a light of hope. The proposed Digital India Act could potentially guide this ship towards a well-defined legal framework.

III. RISKS POSED BY ARTIFICIAL INTELLIGENCE

It is well-recognised that AI poses various risks including the threat to fundamental rights, such as privacy, and to individual and public safety and interests.[3] Modern AI systems are not confined to performing operations based on fixed and unchanging instructions. They possess the ability to collect data and learn autonomously. Specifically, these algorithms can enhance their performance over time and develop the capacity to predict outcomes and make choices that they were not directly coded to do. Applications, particularly those categorized under deep learning, can operate under human supervision, partial supervision, or even without any supervision at all. Hence, their "actions" progress with time (and will continue to do so increasingly in the upcoming future), influenced by the data and feedback gathered and analyzed from numerous diverse shared resources (commonly referred to as "machine learning" and "deep learning"). Indeed, it's fair to say that algorithms not only execute tasks but also learn how to carry them out over time.

It follows from the provided explanations that, beyond a known degree of autonomy, artificial intelligence also features the ability to alter its operation. In other words, AI can generally be characterised by four vital elements, namely, the ability of the system:

[3] European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (2021/0106) (COD) COM (2021) 206 Final

 [ISSN 2581-5369]

- to alter its initial algorithm via machine learning;
- to adapt to previously unknown situations;
- to independently interpret the available set of information for making a specific decision;
- to perform a set of actions, which cannot be done by a traditional computerised system[4].

To safeguard fundamental rights, it's crucial that AI systems exhibit impartiality in their decision-making and data evaluation to avoid biased results. This might not be achievable if there's a lack of transparency or comprehension of the workings of an AI application.[5]

Imagine a world where AI is like a black box, a mystery that's exclusive to none but still remains elusive. It's like a puzzle where the pieces, the data samples used or the decision-making processes, are hidden from the human eye. Researchers have stumbled upon outcomes that are not only obscure but also discriminatory. This black box AI, primarily composed of opaque neural networks, is like a locked room where neither the user nor any other interested party can see what's happening inside. It's an impenetrable system, a fortress that keeps its secrets well.

As Bathaee pointed out, our modern AI systems are built on machine-learning algorithms that often function as black boxes to us humans. They pose a real and immediate threat to the intent and causation tests that are a cornerstone of virtually every field of law. These tests, which evaluate what is foreseeable or the basis for decisions, lose their effectiveness when applied to black-box AI.[6]

This poses a significant challenge for liability, as it becomes difficult to trace the harm back to the developer. It's like trying to find a needle in a haystack, except the haystack is a black box and the needle could be anywhere."

Truby[7] suggests three paths that could be taken when it comes to AI liability. The first path is to establish a strict liability regime. This would put the responsibility of understanding the source of the liability squarely on the shoulders of the developers and users of AI. It's like saying, 'You made it, you understand it.'

The second path is to ban black box AIs completely. It's a bit like saying, 'If we can't understand

[4] Kārkliņš, J. (2020). Artificial Intelligence and Civil Liability. , 13, 164-183.
[5] Truby J and others, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications" (2022) 13 European Journal of Risk Regulation 270
[6] Y Bathaee, "The artificial intelligence black box and the failure of intent and causation" (2018) 31 Harvard Journal of Law & Technology 889.
[7] Truby J and others, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications" (2022) 13 European Journal of Risk Regulation 270

 [ISSN 2581-5369]

it, we shouldn't use it.' Both the first and second paths share a common thread - they address the problem of information asymmetry by shifting the burden onto the developer.

But these paths have a downside. They could potentially dampen the spirit of innovation just when we're in the middle of an AI revolution. The third path is a more nuanced approach. It involves sandbox regulation that targets the intent, causation, and mitigation of liability in specific high-risk scenarios. It's like creating a safe playground where we can experiment and learn without causing harm.

IV. LIABILITY REGIMES FOR AI

There are two major regimes that take the front in governing AI, they are fault liability and strict liability.

Imagine a world where the actions we take have consequences, and those consequences are our responsibility. In this world, if you cause harm, you're held accountable. This is the essence of fault liability, a cornerstone of justice in many European jurisdictions. It's all about assessing the level of care based on a legally recognized duty and a corresponding breach and causation. It's like a balancing act, where actors are incentivized to stay within the expected level of care, as determined by courts through policy and cost-benefit analysis, to avoid the risk and cost of liability.[8]

On the other hand, here's the thing about 'strict liability' -it's not about defects or mal-performance. It's about causation. It's about connecting the dots. But when you look closer, you see there's more to it. Now, strict liability isn't applicable in every situation. It's for those times when significant harm could happen, even when there's no fault, no defect, no mal-performance. It's for when proving these elements would be so hard for the victim that it would lead to under-compensation or inefficiency.

There are two parts to strict liability: factual causation and legal causation. Factual causation is about the 'but for' test. If damage wouldn't have happened without a condition, that condition matters. Legal causation, on the other hand, limits the causes that matter.

Different EU Member States have different takes on this. Some stick to the 'but for' test. Others use the theory of adequate causation or a more flexible approach. Adequate causation means the harm must be a direct and foreseeable result of behavior.

Traditional legal concepts of causation assume we know who the wrongdoer is. But with AI,

[8] Truby J and others, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications" (2022) 13 European Journal of Risk Regulation 270

 [ISSN 2581-5369]

it's not that simple. AI is opaque, and there are many stakeholders involved. So, finding the actual cause or source of harm isn't always straightforward[9]. This complexity can discourage individuals from filing a claim. But here's the silver lining - new technologies offer new ways to record and monitor the system in operation, which could make things a bit easier[10].

Zech[11] points out a limitation in fault-based liability's regulation of AI - the information asymmetry between courts and producers. It's like a game of hide and seek, where the courts, which are unlikely to have the same technological and risk knowledge and resources as developers and manufacturers, are left searching for the risk knowledge. The incentive to adhere to the level of care may fail in the face of novel technologies like AI, when the actor lacks the risk knowledge needed to meet the level of care. It's like trying to navigate a maze blindfolded - the information asymmetry between the user and the producer could prevent the user from meeting its level of care. And finally, fault-based liability may not cover the risks posed by new technologies that are unforeseeable and therefore could not meet the requirements of legal causation. It's like trying to predict the weather - sometimes, the unforeseen happens.

Strict liability, while it has its merits, also has significant downsides. The biggest one? It can stifle innovation. It can deter companies, especially small start-ups, from taking on the risk of liability exposure. A cost that might be a drop in the bucket for a large company could be the end of the road for a small start-up. These start-ups rely on innovation and experimentation, with a lower risk threshold from prototype to market.

While strict liability can be justified due to the problem of information asymmetry, regulators might not see the whole picture. The development of AI involves multiple parties, each with their own information asymmetry about data, algorithms, or people. Plus, AI can pose high risks that producers and operators can't foresee. Take the development of neural networks, for example. They're like black boxes - their processes are virtually unknown to the developer and operator. In these cases, the strict liability approach falls short[12].

The scenarios with multiple producers or operators and the black box scenario can also raise issues about causation. The EU, for instance, handles this in the EC Proposal by shifting the burden of proof onto the producer or operator. However, this approach could end up favoring

[9] Yavar Bathaee, 'The Artificial Intelligence Black Box and The Failure of Intent and Causation' (2018) 31(2) Harvard Journal of Law & Technology 889, 891; Chinen (n 99) 343.
[10] Wagner (n 1) 46; the EP JURI Study proposes that a 'logging by design' requirement be established: EP JURI Study (n 29) 83.
[11] Fault-based liability is the default approach in the EU Member States. ibid; H Zech, "Liability for AI: public policy considerations" (2021) ERA Forum 147
[12] Truby J and others, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications" (2022) 13 European Journal of Risk Regulation 270

 [ISSN 2581-5369]

large companies that already dominate the AI industry. They have the upper hand over small companies in the AI development process and could use this to shield themselves from liability.[13]

V. POTENTIAL REGULATORY REGIME IN INDIA

Whilst a fault and strict liability can be an acceptable regime while handling low-risk AI, it may fall shorts in many grounds.

In India, a country that's become a hotbed of innovation and entrepreneurship in the fintech space, regulatory bodies like the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the International Financial Services Centres Authority (IFSCA) have embraced the concept of regulatory sandboxes.

A regulatory sandbox is a framework that allows live, time-bound testing of innovations under a regulator's oversight. It's a playground for creativity, a space where innovators can test their ideas, push the boundaries, and disrupt the status quo, all under the watchful eyes of the regulator.

The RBI, for instance, has set up a sandbox that allows fintech firms to test their products, ensuring that any potential risks are identified and mitigated early. Entities applying for the RBI's regulatory sandbox must have a net worth of INR 25 lakh and be incorporated and registered in India or licensed to operate in India.

SEBI, on the other hand, has created a sandbox framework that gives registered entities an opportunity to test their fintech solutions on a small number of actual customers in a live and controlled environment for a limited time. The IFSCA's Sandbox framework extends this concept to entities operating in the capital market, banking, insurance, and financial services space. These sandboxes are more than just safe spaces for innovation. They're catalysts for change, platforms that foster creativity, and incubators for groundbreaking ideas. They give regulators a chance to work with fintech innovators, mitigate potential risks, and develop evidence-based policy[14].

But the journey is far from over. As we continue to push the boundaries of what's possible with AI, we must also continue to evolve our regulatory frameworks. We must learn from global best practices, adapt to new challenges, and above all, ensure that our regulations foster innovation,

[13] Fault-based liability is the default approach in the EU Member States. ibid; H Zech, "Liability for AI: public policy considerations" (2021) ERA Forum 147

[14] Shashidhar K.J., "Regulatory Sandboxes: Decoding India's Attempt to Regulate Fintech Disruption," ORF Issue Brief No. 361, May 2020, Observer Research Foundation.

 [ISSN 2581-5369]

not stifle it.

VI. CONCLUSION

In the end, it all comes down to this: AI is a game-changer, and how we choose to govern it will shape our future. Fault liability and strict liability, two major regimes, each have their own merits and challenges. They represent the scales of justice, balancing the need for accountability with the drive for innovation.

Regulatory sandboxes, embraced by India's leading regulatory bodies, offer a promising solution. They provide a safe haven for creativity, a testing ground for groundbreaking ideas, and a platform for change. But remember, innovation is a journey, not a destination. As we continue to push the boundaries of AI, our regulatory frameworks must evolve in tandem.

*****

 [ISSN 2581-5369]