Page 3191 - 3204 **DOI:** *https://doij.org/10.10000/IJLMH.116495*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

From Algorithms to Accountability: Deciphering Legal Responsibility in AI-Driven Systems

HARSH PRATAP SINGH[1] AND SHRIJETA PRATIK[2]

ABSTRACT

As artificial intelligence (AI) continues to permeate various aspects of society, the need to establish clear legal frameworks for addressing issues of accountability and responsibility becomes paramount. This paper delves into the intricate relationship between algorithms and legal liability in the context of AI-driven systems. The rapid advancement of AI technologies, fuelled by complex algorithms, raises challenging questions about the ethical and legal implications of their deployment.

In a recent publication from a well-known computing journal, the inquiry was raised regarding the applicable laws in the unfortunate event of a self-driving car causing harm to a pedestrian. This paper examines the broader issue of legal accountability concerning artificially intelligent computer systems. It explores the possibility of criminal liability, identifying potential recipients of such liability. Additionally, within the realm of civil law, the paper scrutinizes whether an AI program falls under the category of a product, making it subject to product design regulations, or if it is considered a service to which the principles of the tort of negligence are applicable. Furthermore, the analysis extends to the consideration of sales warranties in this context.

Keywords: *Artificial Intelligence, Accountability, Regulations, Challenges, Ethical Dimensions.*

I. INTRODUCTION

Humans have been able to develop machines that impersonate human brain. Artificial intelligence has given birth to an evolution in field of technology. With passing time, it is gaining a lot of importance because of its ability to interpret the data and make decisions that in one way or the other helps the humans in relieving the complexity of any situation. Be it a game of tic-tac-toe or resolving a legal dispute, AI has proved its intellect. It is an undisputed fact that AI has had an impact in every walk of life. These softwares mostly opine on subjects that demands human intellect and expertise. Digging deep into the working of these software

[1] Author is a student at NMIMS Kirit P. Mehta School of Law, Mumbai, MH, India.
[2] Author is a student at NMIMS Kirit P. Mehta School of Law, Mumbai, MH, India.

 [ISSN 2581-5369]

we gain insight of machine learning that takes data as input and the underlying algorithms discern patterns that gives output which is relevant to the input that was initially fed. Output received can be in the form of digital figures, visual particulars, text, fuzzy data. AI is known for its adaptive nature.

AI has been able to make its space in the legal field worldwide. The city of Chicago has won at originating AI driven "Strategic Subject List" that scrutinises people behind bars for the risk they possess as a culprit in near future. The offenders are ranked on a scale of 0 to 500 using parameters of age, drug arrest records, criminal activity, victimisation.[3]

Scholars are of the view that AI has mitigated biasness and has to lead to fairer sentencing system in the contemporary times.

AI provides Virtual customer aid which includes listening to customer's problems and providing them with best solution possible.

Artificial intelligence involves the creation of software and systems capable of intelligent thought processes akin to the human mind. Neural systems constitute AI systems, characterized by intricate algorithms and datasets generated by software rather than human design. The approach involves breaking down a problem into numerous pieces of information, processing them linearly, bit by bit, to produce a practical outcome. AI finds applications in various areas such as expert systems, natural language processing, speech recognition, and machine vision.

Notably, the calculations and strategies employed by an AI system to arrive at a particular decision are beyond the comprehension of the human mind. This gives rise to the 'black box paradox' or the 'explainability issue' concerning artificially intelligent systems and the associated legal liability.[4]

Beyond robots that are humanoid, artificial intelligence (AI) includes the creation of algorithms that mimic the intellect of humans, such as machine learning, bots, and self-driving cars. Pioneers in the field have expressed worries about the use of AI and its possible hazards. The current state of artificial intelligence law is insufficient, and managing AI will become more difficult as it develops quickly. People who are accustomed to making machines equivalent to humans and scholars of law needs to come up with some sort of accountability for greater good.

[3] Aaron Tucek, *Constraining Big Brother: The Legal Deficiencies Surrounding Chicago's Use of the Strategic Subject List*, The University of Chicago Legal Forum https://legal-forum.uchicago.edu/print-archive/constraining-big-brother-legal-deficiencies-surrounding-chicagos-use-strategic.

[4] Juris Centre, Artificial Intelligence and Liability, (Oct. 25, 2023), https://juriscentre.com/2023/10/25/artificial-intelligence-and-liability/.

 [ISSN 2581-5369]

II. CHALLENGES AND RISKS IN AI: LEGAL IMPLICATIONS

The ambiguity that has engulfed AI's liability lends way to infinite problems putting in place and maintaining an administrative structure. Its high time that we accept there is a need for well-established structure to overcome this hindrance of implementing laws on AI.

Liability of those using it: People are getting addicted to these AI chatbots with passing time and it's getting equally difficult to hold liability giving rise to perplex legal considerations. Confidentiality as an issue must be taken into consideration in a comprehensive legal approach for addressing privacy difficulties which are indeed a serious concern arising from the collection, use, and preservation of private information by AI systems.[5]

Bias and prejudice: To ensure equality and fairness, legal procedures must be put in place to prevent the danger of bias and discrimination in AI initiatives.

Regulatory analysis and safety measures ought to be applied to administrative surveillance and control activities, particularly talking about the use of biometric records and technologies for facial recognition. Arms with autonomous capabilities Ethics and accountability must be considered when AI uses weapons that are not guarded by humans. This is particularly valid when choices are taken that result in death of an innocent. Responsibility of self-driving cars It is crucial to create a regulatory structure that will specify who is responsible for what in the case of a mishap or glitch involving an autonomous automobile.[6]

Collectively, these elements play a significant role in determining who is in charge of machine learning technologies. Accountability under civil as well as criminal legislation for harm or loss arising from the application of machine learning is necessary.

III. AI AS A LEGAL PERSON

An organisation with the ability to enter into contracts, face litigation, bring legal action, and be held legally responsible is referred to as a "lawful individual." Traditionally, legal entity status has primarily included human beings and other genuine institutions; on rare occasions, it has even extended to fictional organisations like businesses. Nevertheless, as computational intelligence algorithms become more sophisticated and autonomous, issues about how they are governed by law have emerged. There are attempts underway in a number of countries to investigate regulatory structures that can take into account the special characteristics of AI

[5] What legal liability issues can arise out of the use of artificial intelligence chatbots? – Josh and Mak International, https://joshandmakinternational.com/what-legal-liability-issues-can-arise-out-of-the-use-of-artificial-intelligence-chatbots/.
[6] (Dec. 19, 2023), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8042627/.

 [ISSN 2581-5369]

advances. On average, the focus of these discussions is on the subject of accountability, obligation, and the legal implications of activities performed by artificial intelligence. In the context of automation and legal accountability, the tragic event that claimed Kenji Udhara's life in 1981 marked a turning point.

At the Kawasaki Heavy Industries plant, Kenji was killed by an automated device that was given a particular task. This incident made clear how urgently laws addressing criminality or mishaps using AI and robots are needed. It was accepted as the first robot-related tragedy ever reported globally.[7] The sequence of occurrences culminating in Kenji's death has demonstrated how difficult it is to place responsibility when dangerous accidents involving robots occur. The robot, which did not shut out for repair, mistakenly slaughtered Kenji by shoving him forcefully with its mechanical arm because it perceived him as an imminent danger. Even if these incidents were grave, there was a lack of assets in international criminal law, and the justice mechanism as a whole was not at all equipped for situations like this anywhere in the world.

By giving the computer programme Sophie nationality, Saudi Arabia[8] has shown boldness and rejected the ambiguous legislative structure that most of the other regimes follow. This revolutionary move not only grants Sophie privileges but also entails duties and obligations that are equivalent to those of other citizens of the Realm. Taking these things into consideration granting AI systems a legal status equivalent to that of humans is a debatable issue.

AI needs a legal recognition worldwide taking into account the absence of an obvious constitutional basis for determining who is responsible for the AI incidents raises important civil and disciplinary concerns. The key question revolves around if independent organisations are entitled to legal personality and how that would affect their accountability.

The market has been over clouded with the working of AI not only on legal but also on moral platforms affecting the social as well as commercial market. It's crucial to think about the real-world consequences of this shift even if moral problems regarding the viability of giving algorithms personality have been resolved. With AI systems emerging as increasingly important in many areas of the community, it is imperative that they be held responsible for their actions.

The need for developing an extensive legal structure is growing as we address the ethical, regulatory, and intellectual implications of artificial intelligence. The heart wrenching event that took place in 1981 and Saudi Arabia's incident bring into the light the dire requirement of

[7] Schneier on Security: Tagged robotics, https://www.schneier.com/tag/robotics/.
[8] Natasha Turak, Saudi Arabia announces major legal reforms, paving the way for codified law, (Feb. 9, 2021), https://www.cnbc.com/2021/02/09/saudi-arabia-announces-legal-reforms-paving-the-way-for-codified-law.html.

 [ISSN 2581-5369]

providing artificial intelligence with adamant lawful position so that it gets easier and justified to held the bots responsible for their criminal acts or any mishaps that might cause damage to living organisms.[9] This will mark the beginning of a new evolution in the field of law and technology.

IV. THE ACCOUNTABILITY OF ARTIFICIAL INTELLIGENCE WITHIN THE LEGAL FRAMEWORK

The rise of AI will raise ethical and moral questions because there isn't a clear legal and regulatory framework that is supported by a cohesive policy structure. In order to fill this gap, it may be possible to apply policy guidelines for different stakeholders in the field of AI systems, including developers, producers and software programmers with an interest in AI systems, by recognising that they are separate entities. It is essential that private entities and public authorities have this recognition, in order to comply with a wide range of ethics and law requirements.

Therefore, the burden of proof can or may not be shifted from engineers to artificial intelligence systems themselves, especially those with a high degree of autonomy.[10] Despite the fact that human beings are creators and programmers of AI, its wholly automated nature enables it to evolve autonomously according to new variables, data, and circumstances. Even in cases where the AI creator has not intentionally broken the law, this autonomy increases the possibility of faults or overrides of its programming data, which could result in criminal offences.[11]

The liability of Artificial Intelligence Robots for crimes is still unclear from the legal frameworks of different countries. For such cases, when deciding whether an artificial intelligence is to be held responsible for specific crimes, e.g. instances where it does not comply with the creator's order which shapes its software and algorithms, court rulings are a key source of judgment. The fact that there are no specific rules also highlights the need for a stronger legal framework to tackle the complexity and challenges arising from an increased role of AI.

(A) Criminal Liability

Gabriel Hallevy, an expert on law and attorney, suggests that some artificial intelligence systems might be able to meet essential criteria of criminal responsibility for the act or omission

[9] Dmitry Enikeev, Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? Unbroken, but Bent: Gendered Racism in School Lead https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322/full.

[10] Christiane Wendehorst, Strict Liability for AI and other Emerging Technologies, (Aug. 1, 2020), https://www.degruyter.com/document/doi/10.1515/jetl-2020-0140/html?lang=en.

[11] Andy Thurai, AI Isnt Ready to Make Unsupervised Decisions, (Sept. 15, 2022), https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions.

which includes actus reus. Moreover, he distinguishes between men's rea, which requires knowledge and information, and strict liability offenses, which do not necessitate men's rea.

In order to examine crimes relating to artificial intelligence systems, Hallevy proposes a three-part framework:[12]

a) AI Liability in cases where another party is responsible for the crime. In this scenario, an innocent agent, such as an underage person, someone with intellectual disabilities, or a non-human entity lacking the intellectual capacity to assert men's rea under criminal responsibility, may commit an offense. Similarly, in cases of strict responsibility, if such agents are used as tools by criminals to carry out illicit acts, the individual providing instructions will bear legal responsibility. Thus, the AI system is regarded as an innocent actor, while the human providing instructions is considered the offender.

b) Liability based on the Natural Likely Outcome of AI actions. A reasonable programmer or user should anticipate the crime as a logical and expected outcome of AI activities, taking necessary precautions to prevent it. If the AI expressly causes damages due to negligence or programming errors, it may or may not be held liable. However, if it acts independently or against its programming, it may be held accountable. For example, in the case of a telerobotic surgery conducted by an Ahmedabad doctor on a patient 32 kilometres away, the robot could be held accountable for any injuries caused if it deviated from its recommended software.

c) Direct Responsibility of Artificial Intelligence. This paradigm encompasses all actions of an AI that are independent of the developer or user. In situations where men's rea is not required to be established, the AI is entirely liable under strict responsibility. For instance, if an autonomous car, powered by artificial intelligence to operate in a self-driving mode, exceeds prescribed speed limits and causes over speeding, the car would be held liable under strict responsibility.

(B) Civil Liability

In situations where software defects lead to damages incurred by individuals, legal actions typically focus on negligence rather than criminal culpability. Gerstner emphasizes the accused's duty of care, highlighting that software or system vendors inherently owe customers a reasonable obligation. However, determining the precise level of standard care required can be challenging. In the case of "expert systems," the expected level of care should be, at a

[12] Gyandeep Chaudhary, ARTIFICIAL INTELLIGENCE: THE LIABILITY PARADOX, (Sept. 2, 2020), https://www.ili.ac.in/pdf/gyc.pdf.

 [ISSN 2581-5369]

minimum, professional, if not expert.[13]

An ongoing debate centres around whether AI systems can cause harm and, if so, whether the breach is attributable to them. The crucial consideration in the realm of Artificial Intelligence is whether AI programs, akin to professional systems, provide guidance for a solution in a given situation or, in the case of an automated vehicle, rationalize a specific alternative and act accordingly.

If artificial intelligence systems may be harmful, questions arise about whether the breach will result in an actual injury to the plaintiff. In particular, in cases where at least one foreign party is involved, the causation procedure may be complicated and therefore relatively easy to ascertain, but certain scenarios such as those related to automatic vehicles simplify this process.

Overall, negligence and the obligation of care owed to software or systems suppliers are often at issue in civil liability proceedings relating to artificial intelligence. It continues to be difficult to establish an appropriate level of care, in particular when there are expert systems involved. There is still a debate about causation, and the impact of AI programmes on outcomes, with different views as regards scenarios in which AI provides guidance or endorses actions in specific situations.

(C) The Trojan Defense In Ai Liability Cases

There is a need for highlighting cases where defendants accused of cybercrime are successfully using the Trojan defence when considering defences against AI system liability. The defendant's defence argues that a Trojan or similar malicious program broke into his computer and carried out the crimes for which he was not aware.

In one well-known instance from the UK, a computer with eleven Trojan programmes and pornographic pictures of youngsters was found. A teenage computer hacker was accused with executing a denial-of-service attack in a different case in the United Kingdom.[14] According to the defence, a Trojan programme on the defendant's computer launched the attempted attack before it was removed before forensic examination could be completed.

An analysis of these cases reveals a legal tactic whereby defendants, via their attorneys, have persuaded jurors that Trojan horses have infected their computers and caused them to commit crimes they were unaware of. To cast doubt on the defendant's direct involvement in cybercrime

[13] https://law.stanford.edu/transatlantic-technology-law-forum/projects/artificial-intelligence-civil-liability-an-economic-and-comparative-legal-approach-to-u-s-e-u-law/.

[14] Towards Increasing Trust in Expert Evidence Derived from Malware Forensic Tools, https://commons.erau.edu/cgi/viewcontent.cgi?article=1691&context=jdfsl.

is the goal of this defence.

The Trojan defence brought to light how difficult it is to assign blame in AI-related instances, particularly when malware is a major factor in the criminal acts that are being looked at. To better understand how liability for artificial intelligence evolves and the ever more complicated challenges facing justice systems to identify culpability, it is increasingly important to examine such judicial precedents.

V. CURRENT LEGAL FRAMEWORKS: ADAPTABILITY TO AI CHALLENGES

(A) International Regulation of Artificial Intelligence

It takes a long time in the area of law for AI to be regulated. In the case of Jones v. W + M Automation, Inc., the Appellate Division of New York dismissed a product defect action against a robotic loading system manufacturer and programmer. The court held that, even if the robot and its software were sufficiently secure during programming and installing, defendants who made nonfictive components could not be liable for damages.[15]

Nevertheless, if the hardware or software has been modified in a manner which is not appropriate, there may still be liability on the part of the end user, namely General Motors. It therefore follows that if their products were free of defects when they were created, AI software and hardware makers are not responsible for harm. However, with industry standards determining whether or not an artificial intelligence is defectively created, the licensor and the licensee may be liable for damages arising from defects in production or modification.

The Federal Trade Commission established rules for the regulation of AIFTC in April 2020, which focus on transparency with regard to company use or licensing of AIFTC, especially regarding consumer well-being. Unfair or deceptive acts and practices involving artificial intelligence are considered to be prohibited by the FTC Act.[16]

The regulation on the liability of artificial intelligence was also issued by the EU. The liability for some of the AI applications, e.g. driven robots in public areas, is outlined in a document entitled "AI Liability and Other Emerging Technologies".[17] Manufacturers of products which contain new digital technologies, including artificial intelligence, should have responsibility for any damage to a product due to its defects whether or not those changes were made in the

[15] Artificial intelligence liability: the rules are changing, Center for Internet and Society (Mar. 1, 2023), https://cyberlaw.stanford.edu/blog/2023/03/artificial-intelligence-liability-rules-are-changing-1.
[16] Airlie Hilliard, How is the FTC Regulating AI? (Sept. 22, 2023), https://www.holisticai.com/blog/ftc-regulating-ai.
[17] Artificial intelligence liability: the rules are changing, Center for Internet and Society (Mar. 1, 2023), https://cyberlaw.stanford.edu/blog/2023/03/artificial-intelligence-liability-rules-are-changing-1.

 [ISSN 2581-5369]

producer's control.

Further standards for compliance with high-risk applications of AI, such as healthcare, transport and energy, have been established in the recently published EU White Paper on Artificial Intelligence. The EU is planning to introduce legislation regulating the use of artificial intelligence that could be a global standard in AI policies. Any automated intelligent machine which has an impact on EU citizens and affects both consumers and workers would be covered by the legislation.

Comparable to the General Data Protection Regulation (GDPR), an international norm set by the European Union, the proposed AI legislation seeks to strike a balance between encouraging the use of AI and reducing its associated hazards. In order to build an efficient artificial intelligence ecosystem, the White Paper suggests policy options for establishing a legal basis for trusted AI.

(B) Ai Regulatory Landscape In India: An Analysis

In order to effectively cope with the complex issues of ethics and law that arise from AI systems, it is considered that existing regulation frameworks are inadequate both nationally and internationally. In this context, an examination of the current legislation in India seeking to lay down liability and rights for AI should be undertaken.

a. Constitution of India: Safeguarding Fundamental Rights

The concept of 'right to life and personal liberty' has been interpreted by the courts as covering basic aspects of human life, in accordance with Article 21 of the Indian Constitution. The courts have acknowledged the implied right of privacy as provided for in Article 21 in important cases, like R Rajagopal vs. State of Tamil Nadu[18] or K.S. Puttaswamy v Union of India.[19] The latter case emphasised the need for a complete legal framework that would be able to address emerging issues, such as artificial intelligence in India. Articles 14 and 15 could be invoked to protect the rights of equality and protection from discrimination if artificial intelligence were used, which is likely to result in unfair or discriminatory treatment.

b. Patents Act, 1970: Navigating Ownership and Liability

The 1970 Patent Act provides important questions in the field of computer science, such as patentability, inventorship, ownership and responsibility for an AI's action or omission. As there are no explicit requirements in law for people to be human beings, current conventions assume

[18] 1995 AIR 264, 1994 SCC (6) 632
[19] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

 [ISSN 2581-5369]

that this is the case. Currently, artificial intelligence is not recognised as a person and thus does not belong to the scope of this law.

c. Personal Data Protection Bill, 2019: Safeguarding Citizen Data

The need for a consent from data controllers is highlighted in the 2019 Personal Data Protection Bill, which deals with the processing by Public and Private Bodies of people's confidential information. This legislation will have a significant impact on the widespread use of AI software which gather user information for different purposes, e.g. to monitor how users buy and use online retailers or even make payments by electronic means.

d. Information Technology Act, 2000: Ensuring Data Security

S. 43 A of the I.T. Act 2000[20] provides that, in cases where adequate security practices have not been adhered to, an entity dealing with sensitive personal data must be liable for compensation. It is essential to put forth a lawful framework to ensure that private data if any is being stored with the bots it is safe and confidential and if at all they are given access to public they need to be regulated in a lawful manner.

e. Consumer Protection Act, 2019: Establishing Liability for Harm

Taking into consideration Section 83 of the Consumer Protection Act of 2019[21], states that every individual can file complaint in the form of a lawsuit against the dealer, seller, manufacturer who have been harmed due to defects in the products or the manufacturing process. This will help in holding the AI creator responsible for the act of negligence caused to other humans.

f. Tort Law: Determining Liability for AI Actions

Establishing AI's responsibility for any misconduct or carelessness in the framework of civil litigation requires an understanding of the principles of absolute and indirect liability. It was determined in the Harish Chandra v. Emperor case that when an AI body is regarded as an intermediary, there is no vicarious culpability under criminal law for the crime of a human being. Legal system of India has delved into the rights and liabilities of the AI and has considered ethical and legal consequences but hasn’t come up with any stringent laws.

VI. CRAFTING A COMPREHENSIVE FRAMEWORK FOR AI LIABILITY

Legal structures, ethical concerns, and technological breakthroughs must all be combined to build a comprehensive framework that addresses the subject of AI accountability. A comprehensive approach to managing AI's promise and challenges is provided in this part of

[20] Information Technology Act, 2000, Section 43, No. 21, Acts of Parliament 2000
[21] Consumer Protection Act, 2019, Section 83, No. 35, Acts of Parliament 2019

 [ISSN 2581-5369]

the article. As a result, the recommended approach seeks to achieve equilibrium amid accountability and innovation.

(A) Algorithmic Responsibility: Redefining Liability Standards

(i) Clarifying Legal Personhood for AI Entities

Establishing the legal status of AI companies is an essential first step in establishing liability. The subject at hand explores the concept of legal persons for AI, taking into account possible consequences and ramifications. They look at the issue of determining if at all AI systems should be treated like legal people with rights, responsibilities, and penalties similar to those of people.

(ii) Developing Transparent Decision-Making Processes

Any consequences that might be held against AI should be non-ambiguous and legitimate. The urgency of the use of AI and holding it liable for its mistakes has been a part of our discussion. Also, the laws so framed to decide its liability shall meet the Indian lawful standards.

(B) Legal Clarity in AI Development and Deployment

(i) Establishing Clear Guidelines for AI Developers

This demonstrates how important it is to provide straightforward directions in order to progress artificial intelligence. The establishment and maintenance of industrial principles and moral codes is also examined in relation to the growth, advancement, and use of systems based on artificial intelligence. Reducing confusion regarding law and fostering an environment that supports accountable creativity are the objectives.

(ii) Defining Liability in the Development Lifecycle

This describes the phases of the creation of artificial intelligence and assigns blame at different points in the relationship of technology lifecycle. Assigning culpability at the appropriate time and place ensures responsibilities for the actions and results of artificial intelligence (AI) algorithms from the time of their creation to their implementation.

(C) Ethical Considerations in AI Decision-Making

(i) Mitigating Algorithmic Bias and Discrimination

This explores the moral ramifications of artificial intelligence and explores methods to reduce biases and prejudices in robots. It underscores the need that unbiased mechanisms be created in accordance with social recommendations which underline the need of accountability, openness, and fairness in AI systems.

 [ISSN 2581-5369]

(ii) Safeguarding Privacy in AI Applications

There are legitimate worries about anonymity in AI applications. This subsection provides details concerning the ethics of using artificial intelligence records for commercial purposes in addition to recommendations for safeguarding confidentiality. The importance of data confidentiality, explicit consent, and stringent safeguards for privacy is emphasised.

(D) Adaptive Legal Framework: Anticipating Future Challenges

(i) Incorporating Flexibility in Legislation

The following asks that the laws be changed to reflect the quick development of machine learning. It is looking into ways to make laws more flexible so that they may be adjusted to take into account technological improvements without compromising the system's effectiveness.

(ii) International Collaboration on AI Standards

This pays respect to the worldwide scope of artificial intelligence while highlighting the significance of international cooperation in the creation of AI standards. The necessity of harmonising rules and regulations across national boundaries is considered in order to create a unified international structure that promotes accountability in the disciplines of artificial intelligence.

(E) Enforcement and Remedies: Ensuring Accountability

(i) Strengthening Enforcement Mechanisms

The following mechanism has been introduced to make sure that its quite effective. This paper examines the significance that oversight organisations, inspection protocols, and fines play in keeping artificial intelligence creators and users responsible when they break regulations.

(ii) Providing Adequate Remedies for AI-Related Harms

This subsection addresses the implications of AI-related problems and examines effective solutions. For the purpose of to address potential liabilities in a fair and reasonable manner, it examines the regulatory structures for recovering those who are injured by AI errors and unethical usage.

After a struggling decade a mechanism has finally been able to make its way for giving effect to the working of AI keeping into consideration the ethics and morals. In particular, the board seeks to achieve an equilibrium amongst encouraging creativity and protecting individuals and the community from possible risks associated with the advancement of artificial intelligence technologies.

 [ISSN 2581-5369]

VII. NAVIGATING LIABILITY IN AI OFFENCES: MODELS AND RESPONSIBLE PARTIES

Notwithstanding how these algorithms work, it indeed is a tedious task to assign blame for infractions involving artificial intelligence technologies. On the basis of Gabriel Hallevy's three models—direct transparency, inevitable or predictable repercussions, and perpetrator-by-another[22]—this study investigates the important topic of who is responsible.

1. Perpetrator-by-Another Offence: User or Programmer Liability

People are usually held legally accountable when they give commands to an AI system that might be construed as a perpetrator-by-other conduct. Software developers and consumers may find this pertinent, since it raises concerns about who should decide what the AI performs and who should only carry it out.

There may be disputes about who is more at fault—the user or the programmer. Identifying the boundaries of responsibility becomes critical, which then sparks legal debates over if user commands comply with the constraints and moral principles built into the AI's design.

2. Offence with Natural or Probable Consequences: Shared Liability and Foreseeability

A range of individuals are investigated in cases of breaches with natural or predictable consequences, when responsibility reaches those who anticipate the item in question getting abused. This covers both the programmer and the supplier of products and services. However, unless clear instructions were given outlining the restrictions placed on the technological use and the possible repercussions of abusing it, individuals would be less inclined to take accountability.

Examining the joint responsibility of several parties requires an in-depth examination of predictability. Legal frameworks must consider the level of responsibility that should be assigned to the programmer, vendor, and service provider based on their individual levels of awareness and the actions they have done to reduce known risks.

3. Strict Liability Offences: Programmer Accountability

The developer has primary responsibility when AI algorithms are deemed accountable for strict liability breaches. Legal assessments concentrate on the programmer's authority over the AI's functioning and conformity to preset guidelines.

When talking about the nuances of developer taking responsibility, arguments around what constitutes a culpable developer may come up. To make compliance with laws better, it is

[22] Gyandeep Chaudhary, ARTIFICIAL INTELLIGENCE: THE LIABILITY PARADOX, (Sept. 2, 2020), https://www.ili.ac.in/pdf/gyc.pdf.

 [ISSN 2581-5369]

important to consider who should make the decision to hire someone without the necessary training—the management, the programme developer, the expert source, or the developer.

To put it briefly, figuring out who is accountable for AI crimes requires closely examining the specific model that the crime is committed under. In addition, understanding the intricate web of liability that each model entails necessitates ongoing legal discussion to establish clear guidelines for holding the user, programmer, product seller, and service provider, among others, accountable. The dynamic and adaptable legal landscape that deftly negotiates the complexity of technology breakthroughs and their legal ramifications is necessary given the growing nature of artificial intelligence.

VIII. CONCLUSION

Current domestic and international law no longer recognises artificial intelligence (A.I.). If these rules are not followed, AI cannot be held accountable for any potential harm. As per Article 12 of the New York Convention, the onus of accountability for all actions and conversations that transpire within a system rest with the organisation that programmes artificial intelligence. This concept is based on the direct liability model proposed by Hallevy, where strict liability models limit the behaviour of the AI system while leaving other actors unaffected. This shows that intelligence is a tool.

Considering the AI-as-Tool perspective, strict or vicarious liability for damages caused by the AI system becomes more feasible. However, establishing a sufficient burden of evidence poses challenges due to the intrinsic functioning of AI systems, including autonomous decision-making. Differentiating between damage resulting from a product defect and harm caused by AI actions is complicated, given the automated and evolving nature of AI systems. This liability model becomes valuable only when legislators have a clear understanding of how to adapt existing laws or formulate new ones to address the accountability of AI systems, especially as their impact on human lives continues to grow.

Recent research indicates that as AI systems advance, reaching the transition between "Artificial Narrow Intelligence" (ANI) or weak AI and "Artificial General Intelligence" (AGI) or strong AI, the construction of explainable models becomes more achievable. Such models could significantly contribute to understanding and resolving AI-related issues. To effectively regulate AI systems, specific responsibility rules adhering to legal principles such as vicarious liability, product liability, and strict liability must be developed. Ultimately, the feasibility of developing AI systems with legal personhood hinges on the establishment of a comprehensive legislative framework.

 [ISSN 2581-5369]