Journal of Law and Legal Research Development

Ensuring AI Accountability: The Need for Expedited Oversight Frameworks Based On EU

Janani J

Assistant Professor, Dhanalakshmi Srinivasan University Samayapuram Tiruchirappalli, Tamilnadu, India

Article History

Received: Mar-2024
Revised: Apr-2024
Accepted: Apr-2024
Published: Apr-2024

Keywords

Artificial Intelligence
AI
Accountability
Framework
Risk
EU

Abstract

The inevitability of artificial intelligence (AI) impacting every facet of our life is already evident in many ways. Nations are contending with the prospects and difficulties that AI offers. India has emerged as a frontrunner among South Asian nations in spearheading the promotion and regulation of AI. Nevertheless, it falls far behind nations like China or the United States. This article examines the AI ecosystem in India, including the risks and problems it encounters, as well as the ethical concerns it must address. Ultimately, it analyses the need for a comprehensive framework based on the EU regulation for a better control and regulation.

Corresponding Author:
Janani J
Assistant Professor, Dhanalakshmi Srinivasan University Samayapuram Tiruchirappalli, Tamilnadu, India
Jananij.sol@dsuniversity.ac.in

1. INTRODUCTION

India is currently developing policies that concentrate on the rising field of artificial intelligence (AI). Regardless of the reader's location, it is crucial to evaluate the geographical impact of growing AI sector, and ambitious governmental efforts in the field of AI. Despite the efforts of existing policy processes to promote the rapid advancement of AI for economic growth and societal benefit, there is a prevailing trend in India and other jurisdictions to provide a law in AI. This trend involves the recognition of the limitations and risks associated with data-driven decisions, which are often considered after the development and implementation of AI applications. This article contends that it is crucial to consider the technological constraints of AI systems during the policy development phase. Furthermore, the social and ethical issues that occur as a result of these limits should be considered when determining the goals of policy processes. The framework suggests a method for facilitating this debate by examining the three primary phases involved in implementing machine learning (which is the most widely used subset of artificial intelligence methods) - the data stage, the model stage, and the application stage. This research is set in the context of India's existing AI policy environment and utilizes the suggested framework to address the continuing sectoral concerns in India. In order to impact the current policy discussions in the nation, this study focuses on the possible dangers that result from making judgments based on data, both in general and specifically within the Indian context. This article delves into the need for framework in AI related ethical, legal and technological issues. Artificial intelligence means an algorithm to a collection of encoded methods that are used to convert input data into the desired output by performing specified computations. The technique is a precise and systematic process that does not rely on human intuition or guessing. AI, or artificial intelligence, is the capacity of computers to demonstrate intelligent behavior. Artificial intelligence may be categorized into three main forms. Artificial superintelligence refers to the concept that computers have the ability to exceed human intelligence, social abilities, and scientific understanding in several fields. The second concept

refers to artificial general intelligence. This pertains to the objective of computers demonstrating intelligence in many areas, striving to be, at the absolute least, on par with human intellect. Artificial narrow intelligence (ANI) is the third kind of intelligence, where computers are capable of demonstrating human-like skills in specific and limited areas. In this article, the term AI will specifically refer to ANI[1]. Machine learning is a subset of AI methods that is now the most effective and popular. It involves the capacity of a system to improve its performance on a job over time. The term Data plays a crucial role in the majority of machine learning applications. Machine learning developers train combinations of algorithms using training data. The process of machine learning is iterative, meaning that it requires an ongoing analysis of models and the adjustment of training data and learning algorithms to optimize for success, as defined and established by developers[2]. The concern that arises mostly in AI systems that are less transparent, where a particular choice, action, or lack of action is impacted by several factors, such as the training data, algorithms, methods, training settings, and deployment environment. Various entities may participate in each stage of the development and deployment process. The decision-making process in self-learning systems may be influenced by the deployment environment. The challenge of assigning blame under existing frameworks of accountability and legal redress is complicated by the 'many hands problem' that is often associated with sophisticated computer systems. The first stage of a civil lawsuit is determining the cause of action. However, the complexity of an AI system, along with many interrelated elements influencing individual judgments, creates challenges in identifying errors and assigning responsibilities[3].

The main issues that are identified are

- AI systems are impacted by an intricate network of choices during their existence.
- The deployment environment also has an impact on the ability of self-learning AI.
- Allocating responsibility for the negative consequences resulting from a particular action is a difficult task.

Artificial intelligence systems heavily depend on extensive training data, and the use of an individual's personal data inevitably raises significant privacy problems. The absence of sufficient privacy measures may allow technology to completely document and analyse an individual's personal life without their permission or awareness, causing considerable damage to their interests by ignoring their choices for data use[4]. The damage may be either financially, such as the theft of an individual's credit card information, or emotional, when an individual's personal facts become the topic of public conversation. The 'Societal concerns' section has also analyzed instances of the influence on democratic institutions. AI heavily depends on data for training, which can include personal and sensitive information (PII). This raise concerns such as the risk of entities using personal data without explicit consent and the possibility of extracting potentially sensitive information from the system's outputs. The security issues in AI systems originate from their dependence on data and the conditions in which they are designed and deployed. Certain assaults specifically target machine learning systems and impact various stages of the machine learning development process. Adversarial machine learning attacks exploit weaknesses in the machine learning model, resulting in potentially detrimental outcomes in the actual world.

2. THE AI ACT'S AIM TO REGULATE AI DEVELOPMENT AND DEPLOYMENT

The European Parliament formally passed the EU Artificial Intelligence Act ("AI Act") on March 13, 2024, with a substantial majority of 523-46 votes in favor of the legislation. The AI Act is an innovative and autonomous law that regulates AI, making it the first of its type globally. It has great significance for the European Union. The main purpose of the AI Act is to provide clear standards and obligations for developers and implementers of AI technology for specific uses of AI. Concurrently, the regulation seeks to reduce administrative and financial burdens on companies, including small and medium-sized enterprises (SMEs). The AI Act ensures the creation of trust among Europeans in the capacities of AI. While most AI systems pose little or no risk and have the potential to resolve many societal issues, there are some AI systems that have inherent vulnerabilities that must be acknowledged and mitigated to avoid undesirable outcomes. For example, it is often difficult to determine the underlying reason for an AI system's decision-making process or prediction, as well as the resulting action it takes.

The proposed rules will include the following

- Examine the distinct hazards that arise specifically from the implementation of artificial intelligence (AI) applications;
- Enforce a ban on the use of artificial intelligence (AI) methods that are considered to have unacceptable hazards.
- Identify a collection of applications that pose a high risk.
- Define clear and unequivocal standards for artificial intelligence (AI) systems used in high-risk applications;
- Outline the specific obligations of persons or organizations involved in the creation and provision of high-risk artificial intelligence applications.
- Prior to using or offering an AI system for sale, it is important to carry out a compliance assessment. After the

[1] *Aayog, N. I. T. I. (2018). National Strategy for Artificial Intelligence. Niti Aayog, 46. See https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf*

[2] *Gillespie T (2014) The relevance of algorithms. In: Gillespie T, Boczkowski PJ, Foot KA (eds)* Media Technologies: Essays on Communication, Materiality, and Society. *Cambridge, MA: MIT Press, pp. 167–193.*

[3] *https://stanford.library.sydney.edu.au/archives/sum2010/entries/computing-responsibility/#2.2.1*

[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012 (Supreme Court August 24, 2017). Retrieved from https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf Google Scholar*

AI system is available for purchase, it is necessary to establish mechanisms for ensuring compliance.

- Establish a hierarchical structure of governing bodies at both the European and national levels.

The European Union considers the AI Act to be a vital element of its legal structure and indispensable for the operation of the EU. More precisely, the European Union aims for the AI Act to emulate the impactful consequences of the General Data Protection Regulation (GDPR), sometimes referred to as the 'Brussels effect', by exerting a substantial influence on global markets and practices. Additionally, it seeks to function as a potential blueprint for other regions interested in implementing AI regulations. However, the story does not end here. Over the next months and years, the AI Act will undergo further clarification and expansion via the introduction of new EU laws, namely implementing and delegated acts that will need approval from the EU Commission. The European Union is currently modifying the EU Product Liability Directive to harmonize it with the EU AI Act. In addition, they have introduced a new directive known as the EU AI Liability Directive, aimed at facilitating consumer access to compensation for any harm caused by artificial intelligence. In addition, EU officials have stated their aim to develop further, more precise legislation regarding AI after the EU elections in June 2024. An issue that may be prioritized is the regulation of artificial intelligence (AI) use within the realm of employment. Although the AI Act now addresses certain areas of AI use in employment, EU authorities have emphasized the need for further legislation to provide more extensive regulation in this domain. Furthermore, considering the controversial issues and concerns related to copyright and AI, it is expected that the European Union would pass legislation to address copyright issues in the realm of artificial intelligence. Organizations, whether they are inside or outside the EU, particularly those engaged in "unacceptable" and/or "high-risk" applications and industries, must acquaint themselves with the complex regulatory structure, with the EU AI Act serving as the central focus[5].

3. ARTIFICIAL INTELLIGENCE LIABILITY

In addition, the new Product Liability Directive was formally enacted by the European Parliament on March 12, 2024, in conjunction with the AI Act. This directive implements precise alterations to the current EU legislation and processes, allowing consumers to pursue reparation for damages resulting from defective goods. The objective is to guarantee that the regulation efficiently governs new technologies such as AI. Under the EU Product Liability Directive, manufacturers of defective products are primarily responsible for compensating consumers. The revisions made to this EU Directive stipulate that an "AI system provider" as defined in the AI Act is classified as a "manufacturer" in accordance with the Directive. Therefore, according to the AI Act, the primary responsibility for any harm caused by AI systems is with the supplier of the AI system. The EU Directive significantly reduces the evidential standards for customers who are dealing with advanced or 'blackbox' AI goods. This implies that buyers no longer have difficulties in identifying product flaws caused by the intricate technical or scientific nature of the product. The Council will now formally endorse the Directive, which will then be published in the EU Official Journal. The new requirements will apply to products that are brought to the market 24 months after the Directive is implemented, in accordance with the national laws of EU Member States.

4. AI IN IMPLEMENTATION

Noncompliance with the EU AI Act may result in regulatory fines up to a maximum of 7% of the company's worldwide sales, as well as possible litigation and damage to the company's reputation. The implementation of the AI Act mostly takes place at the national level of EU Member States, with the exception of general-purpose AI models, which are enforced by the European AI Office. The establishment of the European AI Office was formally initiated by a decision by the Commission on January 24, 2024, before the enactment of the AI Act. In addition, the EU AI Act has created an AI Board with the power to supervise the consistent enforcement of the EU AI Act throughout the European Union. The AI Board is accountable for duties such as providing suggestions and opinions, establishing codes of conduct/practice, and establishing technical standards. Once the AI Act has been formally accepted, it will need formal endorsement from the Council in order to be enacted as law. The AI Act is anticipated to be enforced by late April or early May of this year. Once the AI Act comes into effect, it will not be immediately enforceable. Instead, it will experience a slow and staged transition and implementation period. Once 24 months have passed since its implementation, the AI Act will be fully enforceable. Nevertheless, there are certain instances that deviate from this chronological sequence. Prohibitions on banned practices will be implemented 6 months after they become effective, regulations on codes of conduct will be implemented 9 months after they become effective, regulations on general-purpose AI will be implemented 12 months after they become effective, and obligations for high-risk systems will be implemented 36 months after they become effective[6].

5. AI AND THE NEED FOR FRAMEWORK IN INDIA

India has made attempts to keep pace with the rapid growth of artificial intelligence (AI). However, the existing legislation is fragmented, consisting of guidelines and principles that have been influenced by or borrowed from global practices. Additionally, the Information Technology Act, which is over twenty years old, does not adequately address the digital advancements that have occurred since its enactment. India is

[5] *EU Formally Adopts World's First AI Law, MARCH 21, 2024 https://datamatters.sidley.com/2024/03/21/eu-formally-adopts-worlds-first-ai-law/*

[6] *Coeckelbergh, M. Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability. Sci Eng Ethics 26, 2051–2068 (2020). https://doi.org/10.1007/s11948-019-00146-8*

developing the Digital India Act, 2023 to regulate AI and digital technology, with the aim of addressing the negative aspects of these technologies and creating an environment that promotes future digital breakthroughs in the nation[7]. In August 2017, the Union Ministry of Commerce and Industry established an Artificial Intelligence Task Force with the objective of integrating AI into India's Economic, Political, and Legal frameworks. The aim is to develop a systemic capability that will enable India to become one of the leading economies in the field of AI. Considering the broad perspective of AI as a large-scale solution to socio-economic problems, their paper in March 2018 listed 10 industries in India that are relevant for AI. These sectors include manufacturing, financial technology (FinTech), agribusiness, health, technology for individuals with disabilities, national security, environment, public utility services, retail and consumer interactions, and education. The study had a special objective of determining the government's involvement and the potential of AI to address large-scale challenges. One of the recommendations is to create a central organization called the National Artificial Intelligence Mission, which would be responsible for coordinating all AI-related efforts in India[8]. Although the research identifies the variables that facilitate the mainstream acceptance of AI and identifies government institutions and ministries that may support its expansion, it does not adequately discuss the ethical, social, and technological constraints that underlie the usage of AI technology. Although the paper briefly touches upon privacy and data security, it fails to adequately address the specific data-related challenges posed by AI. When considering ethics and social safety, the Task Force recognizes the difficulties associated with sharing data and allowing other parties to access it. Although it briefly mentions data privacy problems, it overlooks the tendency of data-driven decision-making to reinforce and worsen previous prejudice and discrimination. The possibility for algorithmic systems, especially those with good intentions, to have unequal effects on vulnerable and underprivileged people is also overlooked. This absence is also evident in the sectoral analysis conducted by the Task Force. One of the issues in the FinTech business is the ability to predict market demand and find a balance between scaling operations and fostering innovation. The potential impact of the widespread adoption of FinTech on those who are at the fringes of data collecting and technological inclusion is completely disregarded. Of particular concern is the disregard for the influence of AI technologies on the exercise of basic rights, as well as the inclusion of 'autonomous surveillance and combat systems' without acknowledging the serious implications these technologies have on privacy and freedom of speech. The objective of the Task Force's work is to provide clarity on the future trajectory of AI policy development in India. The primary advantage of this product is in its emphasis on accessibility technology. Nevertheless, the absence of legal, policy, and civil society involvement in this process is evident in the superficial (at most) ethical and social examination of India's AI environment[9]. The National Institution for Transforming India, often referred to as 'NITI Aayog', is a government-operated think tank that has been assigned the responsibility of formulating a comprehensive national strategy on artificial intelligence (AI) to guide the government's initiatives in this field. To enhance economic efficiency in India, NITI Aayog collaborated with Google in May 2018 to provide training and support to start-ups aiming to create and incorporate AI-driven solutions into their business models. In late May 2018, NITI Aayog signed a declaration of intent with ABB India to prepare important sectors of the Indian economy for a digitalized future and harness the potential of artificial intelligence, big data, and connectivity. The NITI Aayog, in a discussion paper published in June 2018, outlines the primary objective of a national AI policy as the use of AI to drive economic growth, promote social development and inclusivity, and serve as a hub for growing and developing economies. The job of NITI Aayog goes beyond only suggesting a policy approach; it also include the implementation and deployment of such policies. The National Strategy surpasses existing AI policy processes in two fundamental respects. Initially, it accepts that the adoption of AI has mostly been motivated by business interests so far, and underlines the need of finding a middle ground between limited definitions of financial effect and the broader societal benefits. Furthermore, it acknowledges that AI applications should be appreciated for their gradual, rather than claimed revolutionary, benefit in different industries[10]. Although there are no comprehensive rules governing artificial intelligence (AI) in India, particular laws are applicable to the use of AI in different sectors. The Security Exchange Board of India, which serves as the security markets regulator in India, has formulated rules specifically addressing algorithmic decision-making for individuals interested in wealth management and algorithmic trading.

6. CONCLUSION

With the implementation of data protection regulations in India, it is crucial to carefully examine the possible difficulties posed by Artificial Intelligence (AI). One possible option is for India to impose a fiduciary duty of care on the data fiduciary towards the data principal. The Data Protection Board of India has the potential to acknowledge the principles of data protection by design and default. It is necessary to investigate technical solutions, such as developing Artificial Intelligence (AI) systems that have built-in rights like the Right to rectification and the Right to be erased, regardless of the specific kind of AI.122 Codes of Practice should be used to establish data protection requirements for the utilization of Artificial Intelligence (AI) in certain areas. India should implement measures to safeguard the

---

[7] *Marda V. 2018 Artificial intelligence policy in India: a framework for engaging the limits of data-drivendecision-making.Phil.Trans.R.Soc.A376:20180087.http://dx.doi.org/10.1098/rsta.2018.0087*

[8] *Marda, V. (2018). Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), 20180087.*

[9] *Artificial Intelligence Task Force. See https://www.aitf.org.in/*

[10] *Sharma YS, Agarwal S. 2018 Niti Aayog to come out with national policy on artificial intelligence soon. The Economic Times.*
See https://economictimes.indiatimes.com/news/economy/policy/niti-aayog-to-come-out-with-national-policy-on-artificial-intelligence-soon/articleshow/63387764.cms.

rights of data subjects against automated decision-making, including includes profiling. The EU offers valuable lessons in terms of granting individuals the ability to challenge AI judgments, the right to seek human involvement, and the right to avoid being subjected to automated decision-making that impacts them. Data protection rights must be safeguarded throughout the whole processing life-cycle of Al - both during the development phase of Al and also during its utilization for decision-making purposes. Throughout different phases of processing, it is necessary to have competent human supervision to guarantee the protection of rights and prevent any detrimental consequences for persons. Transparency is necessary to tell the data principal about the algorithm's logic, the extent of data processing, and the legal justification for processing at different stages. While safeguarding data privacy is crucial, it is equally important to avoid impeding the progress of Artificial Intelligence (AI) research. Artificial intelligence has inherent advantages that can contribute to the advancement of civilization. Hence, it is essential to strike a nuanced equilibrium between safeguarding privacy and ensuring data security, all the while facilitating the advancement of Artificial Intelligence (AI).

7. CONFLICT OF INTEREST

Conflict of interest declared none.

8. REFERENCES

1. European Parliament Resolution. 2017. EP Resolution with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Available at: http://www.europarl.europa.eu/
2. de Almeida, P.G.R., dos Santos, C.D. & Farias, J.S. Artificial Intelligence Regulation: a framework for governance. *Ethics Inf Technol* **23**, 505–525 (2021). https://doi.org/10.1007/s10676-021-09593-z
3. Khemani D. (2012). A perspective on AI research in India. *AI Magazine*, 33(1), 96–98.
4. NASSCOM. (2018). *Artificial intelligence primer*. New Delhi. Retrieved from https://community.nasscom.in/wp-content/uploads/attachment/nasscom-ai-primer-2018.pdf
5. NITI Aayog. (2018). *National strategy for artificial intelligence: #AIforAll*. New Delhi: Government of India. Retrieved from https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf