THE NEED TO EVOLVE A LEGAL REGIME FOR REGULATING THE USE OF ARTIFICIAL INTELLIGENCE IN INDIA

Written by **Dr. Rakesh Chandra**

Academician, Former Civil Servant, LL.M. from B.B A. (Central) University, Lucknow, Ph.D. in Law from Lucknow University, India

ABSTRACT

The use of technology such as Artificial Intelligence permeated into nearly all sectors because of its multiple uses. It is now used in guiding weapons, driving cars, conducting medical procedures, and even writing legal memos. The list is not an exhaustive one. Artificial Intelligence is fast engulfing our day-to-day activities. However, as per the experts, Artificial Intelligence contains the potential for misuse, misleading, threatening, or even bullying individuals. They are of the view that mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war. Moreover, the use of drones in warfare with the help of AI is heading towards dangerous proportions. Further, Generative AI is the real danger since its content can be misleading. Currently, much of the talk about control of AI is centered on self-regulation. The industry, for example, is reliant on self-regulation which is not based on a sound legal base. Therefore, a balance has to be made between technological gains and the harmful effect of AI. In this context, the European Union countries have started working on formulating appropriate legislation to regulate the use of AI. India is also on the way to regulate AI through the prism of user harm. Apart from this, such regulation will have to take into account the constitutional rights to privacy, equality, liberty and livelihood. This paper examines the whole issue of regulating the use of AI through evolving a legal regime, the steps taken so far by the government, and to suggest ways to resolve the issue at hand.

Keywords: Artificial Intelligence, Legal Regime, European Union, Generative AI, Self-regulation.

INTRODUCTION

Artificial Intelligence (AI) is the new buzzword among people around the world. This new technology has shown its enormous potential in almost every field of human endeavour. It has witnessed a manifold increase in its use over the last few years. So much so, that it's now used in guiding weapons, driving cars, conducting medical procedures, writing legal memos though inaccurately, often. This list is not an exhaustive one. As per the experts, AI has the potential to change the way war is waged. In Ukraine war, drones are being deployed to identify, select and attack targets without help from humans and powered by AI. This reflects a new kind of problem for the nation-states-weaponisation of AI. In a paper published in 2022, the United Nations Institute for Disarmament Research, it has been asserted that "What is certain is that the increased adoption of AI will introduce new risks to international security that traditional instruments of risk/incident prevention and management may not be adequate to address."[i] In the year 2022, the world saw the upsurge of Generative AI, also known as Generative Adversarial Networks (GANs). This is a rapidly developing field of artificial intelligence. It has the potential to transform the existing technology in a big way. This technology involves two neural networks, one generative and another adversarial. Both collaborate to generate synthetic data that is not distinguishable from real data. Its significant aspect is the ability to improve existing data sets by generating new, diverse and realistic data. This is helpful in addressing the issues of bias discrimination in algorithms. At the same time, it also improves the overall performance of machine-learning models. Generative AI has vast applications ranging from creating more realistic virtual environments for gaming and augmented reality to generating personalized content for social media and advertising.[ii] Generative AI enables machines in the creation of new content in a way that amounts to mimicking human creativity. It can be useful in generating text and audio, as well as creating new images. Even entire virtual worlds can be created with the help of this technology. Not only this but also, Generative AI can also be used to improve existing AI systems, if provided with more diverse and realistic training data. This can prove to be useful in the field of art, design and entertainment as well as in practical applications like data augmentation and anomaly detection. Overall, Generative AI may significantly impact future technology. In November 2022, the OpenAI start-up, best known for Dall-E, the AI-based text-to-image generator, came up with a new Chatbot called ChatGPT. It is considered to be a monumental step in the advancement of Artificial Intelligence

because of the potential it holds. ChatGPT is based on he company's Language Learning Models (LLM). It can answer "follow up questions," "admit it mistakes, challenge incorrect premises, and reject inappropriate requests". GPT stands for Generative Pretrained Transformer 3, a computer language model that produces human-like text based on inputs, relying on deep learning techniques.[iii]

THE POTENTIAL GREY AREAS OF AI

Every new technology elicits hope and fear, at the same time, among humans. Artificial Intelligence is currently mainstream technology. The balance between technological gains and the harmful effect of AI is a matter of constant debate amongst policymakers, scientists, and the members of civil society. Generative AI poses real danger since its contents can be misleading. On 30th May this year, a statement on AI risk, signed by OpenAI CEO, Sam Altman, Microsoft co-founder Bill Gates and other experts, journalists and policymakers was released by the AI Center for Safety. It specifically stated, "Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war."[iv] That reflects the enormity of the AI revolution. The above statement by Centre for AI Safety (CAIS), endorsed by high-profile tech leaders, was issued just after two weeks after the testimony before the Senate Committee of the United States in which both Sam Altman, along with IBM's Chief Privacy Office Christina Montgomery and AI scientist Gary Marcus, testified on the promises and pitfalls of advances in AI. During the hearing, Mr. Altman urged lawmakers to intervene and place safeguards to ensure the safety of AI systems. He suggested that the Committee should look into a combination of software licensing, and testing requirements for AI models above a certain threshold. Ms. Montgomery urged lawmakers to adopt a "precision regulation approach." This meant establishing rules to govern specific AI use cases as opposed to regulating overall AI. She also pointed out that AI systems must be transparent so that people know they are interacting with AI when they use that technology. AI scientist Gary Marcus pointed out that tools like chat bots could surreptitiously influence people's opinion far greater than social media. And companies that choose what data goes into their Large Language Models (LLM) could shape societies in subtle and powerful ways. He said that "We have built machines that are like bulls in the China shop-powerful,

reckless, and difficult to control."[v] In this context, the speech made by the hon'ble Chief Justice of India, D.Y. Chandrachud, at the 60th Convocation of Indian Institute of Technology, Madras, on Jul 22, this year is worth mentioning here. He said that technology, especially one fostering quicker communication to a large spectrum of audiences such as social media, and artificial intelligence (AI) which has permeated all sectors, should create affordances 'against misuse because human values and individual privacy are of paramount importance.' He contended that "new technology cannot exist in a vacuum" and hence has to be made benign with safeguards for affable use. He further elaborated on the issue by saying that "....Likewise, AI contains the potential for misuse, mislead, threaten, or even bully individuals. Curbing its misuse for harmful purposes will be among the key challenges for you."[vi]

In this context, a group of experts, namely, Timmit Gebru of Distributed Artificial Intelligence Research Institute in California, et al. published a seminal paper on AI, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?". They have listed the following key issues to be dealt with in AI:[vii]

■ Exploitation of workers and massive data theft to create products for the enrichment of few entities;

■ The explosion of synthetic media in the world, which reproduces systems of oppression, and at the same time, endangers our information ecosystem.

■ Concentration of power in the hands of few individuals aggravating social inequalities.

There is no denying the fact that these issues are of deep concern in the Indian scenario.

AI AND THE ETHICAL CONSIDERATIONS

In regard to AI, there is widespread recognition of the fact that product architecture and development or any possible use of this technology should be based on appropriate ethical principles and standards. However, this is not happening in some areas related to the use of AI. For example, coders have already charged violation of copyright against the likes of OpenAI and Microsoft for using their work to create AI tools. Since AI is now encompassing images, and will soon videos, this problem will aggravate in near future.[viii]

SOME INSTANCES OF AI HAZARDS

1. In the last week of March 2023, the Italian government's privacy watchdog temporarily blocked the artificial Intelligence software ChatGPT in the wake of a data breach. The action is provisional "until ChatGPT respects privacy."[ix]

2. Some public schools and universities around the world have blocked the ChatGPT website from their local networks over student plagiarism concerns.[x]

3. With the help of AI, people became successful in generating fake movie trailers with no real actors and having far smaller resources than major Hollywood studios. A search for Wes Anderson on YouTube showed trailers that the renowned director with a distinctive style appears to have made for adaptations of Star Wars, Harry Potter and the Lord of the Rings featuring Bill Murray, Scarlett Johansson, and other stars.[xi]

4. A lawyer named Steven Schwartz was grilled by a judge Kevin Castel of the US district Court during a hearing in New York after the disclosure that this lawyer had created a legal brief for a case that was filled with fake judicial opinions and legal citations by ChatGPT. The judge said he would now consider whether to impose sanctions on Schwartz and his partner. The case involved a man named Roberto Mata, who had presented a suit in the court against the airline Avianca and claimed that he was injured when a metal serving cart struck his knees during the 2019 fight. The respondent, Avianca, asked to dismiss the suit as time barred. Mata's lawyers responded with a 10-page reply citing more than half a dozen court decisions in support of their argument. Avianca lawyers could not trace the cases and the judge Castel ordered Mata 's lawyers to provide copies of the mentioned cases. They submitted a compendium of decisions which were found to be not real. Schwartz said he had posed questions to ChatGPT, and each time it seemed to help with genuine case citations.[xii]

5. In July 2023, one PS Radhakrishnan, was duped by several messages on WhatsApp, with the scammers even using deepfake technology to video call Mr. Radhakrishnan convinces him that the person calling him was a former

colleague in desperate need of money. According to police, the scammers used sophisticated deep fake technology. The National Crime Records Bureau data for the year 2021 showed that a cyber-crime was recorded every 10 minutes somewhere in India. With the easily accessible AI and deep-fake technology, it is only a matter of time that the cyber-crime farms operate across India. Scammers can easily misappropriate the physical likeness of someone, making these crimes with two victims-the one duped and the one whose identity is stolen.[xiii]

6. According to sources, a number of Criminal groups in Delhi are using the anonymity of the dark web to further their nefarious activities. These groups are exploring AI for cybercrimes, including using cryptocurrencies such as Bitcoin to make anonymous transactions, drug trafficking, weapons smuggling, and money laundering, selling stolen data, including credit card details and personal information.[xiv]

7. There has been a tenfold increase in complaints related to morphed images or deep nudes created with the help of advanced tools in India. These cases relate to influences and other public personalities being blacklisted with threats of releasing their deep fake images unless a ransom is paid. In this context, keywords like "Remove Dress AI" and "Deep fake AI tools" have seen an upsurge in searches along with queries on websites like Undress AI, Magic Eraser AI, and Soulgen AI. Another website called Clipdrop AI has witnessed a 4,500 % increase in searches during the same period. These as well other similar sites allow the users to upload a photo of their choice and receive a nude version of that for free or on payment of some cost. Google Trends has classified all these sites as "breakout" searches, which means that they have undergone a "tremendous increase, probably because these queries are new and had few (if any) prior searches."[xv]

AI & THE GLOBAL LEGAL SCENARIO: SOME SIGNIFICANT CONTRIBUTIONS

European Union

In a significant development on May 11, 2023, European Parliament lawmakers initiated the process for comprehensive EU-wide regulations governing AI systems, including ChatGPT. This initiative received resounding support from parliamentary committees focusing on civil liberties and consumer protection. Following this, on June 12, the European Parliament granted approval for the proposed regulations, collectively known as the EU Artificial Intelligence Act (AI Act), designed to address the rapidly evolving landscape of AI technology. Expected to become law in the coming months, this legislation brings several notable features into focus.

Under the AI Act, stringent penalty provisions are introduced, allowing for maximum fines of up to 30 million Euros or up to 6% of a company's total worldwide annual turnover from the preceding financial year, whichever is higher. These regulations also establish harmonized rules for the development and market placement of AI systems within the EU and provide a singular, "future-proof" definition of AI.

In accordance with the new regulations, certain AI practices are expressly prohibited. These include AI systems with the potential to manipulate users through techniques not fully understood, exploitation of children or disabled individuals leading to psychological or physical harm, AI-based profiling that results in social scoring of EU member citizens, and the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes. Exceptions may be granted under specific circumstances with justifiable concrete evidence. The AI Act also addresses the imitation of humans by AI, allowing this only under certain circumstances and with the requirement of disclosure, except for designated authorities.

Specific restrictions are put in place, particularly concerning biometric identification systems, while AI systems posing risks to human health and safety are categorized as 'high-risk.' Clear obligations are imposed on service providers to ensure compliance with these regulations.

Additionally, the legislation paves the way for the establishment of the European Artificial Intelligence Board, comprising representatives from EU member countries and the EU Commission. Importantly, these regulations do not apply to AI systems developed or used exclusively for military purposes, with regulatory sandboxes, basic governance frameworks, supervision, and liability mechanisms to be established by EU member states. This draft legislation marks a significant stride toward bringing AI within the purview of the legal domain, equipped to address the potential hazards of AI technology.

U.S.A.

In the United States, the White House introduced the Blueprint for an AI Bill of Rights in October 2022, as a publication from the White House Office of Science and Technology Policy (OSTP). This blueprint outlines a non-binding roadmap designed to foster responsible AI use. The document elaborates on five core principles aimed at governing the responsible development of AI systems, with a focus on mitigating unintended consequences that could infringe upon civil and human rights. These principles encompass safeguarding users from unsafe or ineffective AI systems, protecting against algorithmic discrimination, ensuring users' data is treated responsibly with built-in protections, providing transparency about AI usage and its impact, and enabling users to opt out and access assistance for problem resolution.

The Blueprint's primary objective is to guide the development, deployment, and use of automated systems to safeguard the interests of the American public. It's important to note that these principles are non-regulatory and non-binding; they do not constitute an enforceable "Bill of Rights" with legislative backing. The document also includes multiple examples of AI use cases that the White House OSTP deems problematic. These examples encompass AI's application in lending, human resources, surveillance, and other domains, with some alignment to the "high-risk" use case framework proposed in the EU AI Act, as observed in a synopsis by

the World Economic Forum. The AI Bill of Rights reflects the foundational principles of American constitutionalism, rooted in robust individual rights and free speech protections.

China

China is in the process of developing its own regulatory regime. In this regard, the Federal Internet Regulator of the country came up with a 20-point draft in the month of April 2023 to regulate generative AI services, which included mandates to ensure accuracy and privacy, prevent discrimination and guarantee protection of intellectual property rights. The draft is expected to be enforced later this year. It requires AI providers to clearly label AI-generated content, establish a mechanism for handling user grievances, and undergo a security assessment before going public. Not only this but also, the A8-generated content must "reflect the core values of socialism". Further, it should not contain anything leading to an overthrow of the socialist system, according to the draft quoted by Forbes.[xvi] The noted legal expert and commentator, Menaka Guruswamy says " China's initial law-making draft intended to regulate AI reveals a two-pronged approach. First, to make the provider responsible for breaking laws that prohibit hate, violence, falsity, or shore up ideology/the state. The language used is broad enough to enable the state to have wide latitude to control providers with stringent punishments. Second, to mandate that the AI product is first submitted to the regulators to ensure that it conforms to the expectations of the state before it is opened to the public. This is clearly screening and censorship in its plainest form. Both prongs are premised on the belief that all AI can be controlled and will never be independent."[xvii] The Chinese draft to regulate AI is an exercise towards evolving a state-controlled AI mechanism which can be more dangerous for the people than the private actors in the field. Any country, by adopting such strategies, can turn into an Orwellian State.

United Kingdom (U.K.)

In U.K., any such effort in lawmaking to regulate AI. Rather, there is a decidedly 'light-touch' approach that is aimed at fostering, and not stifling, innovation in the evolving field of AI.[xviii]

Japan

In Japan too, an accommodative approach has been adopted regarding the development of AI in the country.[xix]

The Indian Scenario

In India, lawmaking to regulate AI is currently not under consideration of the government. According to Information and Technology Minister, Ashwini Vaishnaw, although AI "had ethical concerns and associated risks", it had proven to be an enabler of the digital and innovative ecosystem.[xx] However, the Minister of State for Electronics and Information Technology, Rajeev Chandrasekhar has said that India will regulate AI "through the prism of user harm." He further elaborated that "....This has been our philosophy since 2014..We will not let those platforms harm the digital user in this country and when we allow them to operate, it will be mitigated. Our approach to AI regulation is fairly simple, we w8ll regulate Web3 or any emerging technology, to ensure that the nagrik is protected. "[xxi]

In this context, it is worth mentioning the stand of the Telecom Regulatory Authority of India (TRAI). In a consultation paper titled "Leveraging Artificial Intelligence and Big Data in Telecommunication Sector", the telecom regulator has stated that the Union Government should collaborate with international agencies and other countries to form a global agency for the responsible use of artificial intelligence. It has also recommended setting up a domestic statutory authority to regulate AI in India, through the lens of a "risk-based framework."[xxii] Meanwhile, India's National Programme for Artificial Intelligence, now christened as INDIAai, has been tasked with looking into the regulatory aspects of AI. Consequently, seven working groups have been constituted for this purpose which are likely to submit recommendations for a comprehensive framework governing various facets of AI shortly. Thereafter, the draft will be released for public consultation.[xxiii]

CONCLUSION

Artificial Intelligence is the technology which has influenced the life of human beings in an unprecedented manner. This has become a buzzword in common parlance of everyday life. Undoubtedly, the use of this technology has eased the complexities of life to a great extent. Its use in various fields Including health, industries and commerce, scientific research and many more sectors has produced better and most satisfactory results. The process of its evolution for the benefit of humanity is a continuing process. Unfortunately, at the same time, AI technology has fallen into the hands of some bad actors who are using it to the detriment of the general well-being of the people. Deeply urged by its constant misuse, the Godfather of AI, Geoffrey Hinton has left Google once for all recently. He has warned of dangers lying ahead in this regard. Similarly, Microsoft Chief Economist, Michael Schwarz says that he is confident that AI will be used by bad actors, and it will cause real damage. He has stressed the need to regulate AI. Even the Chief Justice of the Supreme Court of India, Y.V. Chandrachud has also spoken on the same lines. Though there is no reason for being scared, it is necessary to take necessary action to regulate the use of AI by the successive governments. Like any other significant technological advancements, regulations are needed for their proper and justifiable use 8n the interest of mankind. But the laws are needed to award punishment to the bad actors indulging in misusing AI for ulterior motives. Countries like China and the European Union have come up with necessary legislations and in the USA, there is a Blueprint for AI prepared by the White House authorities. But other countries are lacking in this regard. So many dangerous and bad things are happening in countries including India that need to be punished with heavy hands. In the Indian scenario, bad actors have started playing their dirty games affecting innocent people. But our lawmakers seem to be oblivious of these sordid facts. This has to be nipped in the bud. This is the most opportune time to act and bring appropriate laws to regulate AI otherwise it will be too late. India not only needs proper regulations but also stringent laws for punishing the bad actors.

ENDNOTES

[i] Kanika Saxena, Nirmal John & Mugdha Variyar, Speak Up On AI, India, The Economic Times, Jun 11,2023.

[ii] Ibid.

iii Shruti Dhapola, ChatGPT: Bot that promises an AI revolution, The Indian Express, Nov 8, 2022.

iv Kanika Saxena, Nirmal John, & Mugdha Variyar, Speak Up On AI, India, The Economic Times, Jun 11, 2023.

v John Xavier, Are safeguards needed to make AI systems safe?, The Hindu, Jun 4, 2023.

vi Press Trust of India, CJI cautions against tech and AI's misuse, Hindustan Times, Jul 23, 2023.

vii Ibid.

viii Shweta Mulki, An AI-Deal World, The Economic Times, Jan 11, 2023.

ix AP, Italy Privacy Watchdog Blocks ChatGPT, Citing Data Breach, The Economic Times, Apr 1, 2023.

x AP, Italy Privacy Watchdog Blocks ChatGPT, Citing Data Breach, The Economic Times, Apr 1, 2023.

xi Lisa Richwine, Digital doubles, fake trailers: AI worries Hollywood before labour talks, The Indian Express, Jun 2, 2023.

xii The Times of India, Jun 10, 2023.

xiii Editorial, Hindustan Times, Jul 24, 2023.

xiv IANS, Dark Web Groups Exploit AI for Cybercrime Surge, The Economic Times, Sep 4, 2023.

xv Dia Rekhi, The Economic Times, August 3, 2023.

xvi Anil Sasi, Grappling with AI, The Indian Express, May 2, 2023.

xvii Menaka Guruswamy, Chat-bots with socialist values, The Indian Express, Jul 22, 2023.

xviii Anil Sasi, Grappling with AI, The Indian Express, May 2, 2023.

xix Ibid.

xx Ibid.

xxi Liz Mathew, Will bring regulations for AI to keep digital citizens safe: Minister, The Indian Express, June 10, 2023.

xxii ENS Economic Bureau, The Indian Express, Jul 21, 2023.

xxiii Aashish Aryan & Surabhi Agarwal, May 23. 2023.