REGULATING ARTIFICIAL INTELLIGENCE UNDER INTERNATIONAL LAW

Krish Gaur, B.A. LL.B., Apex University, Jaipur

ABSTRACT

Artificial Intelligence in today's world becoming a most important part of our daily lives. Today humans are totally dependent on AI for their works including Healthcare, Industry work, Transportation, Customer Service, Finance, Entertainment, Education, Agriculture and etc. However, AI bring various benefits to the people but it also comes with negative ethical, social, and legal drawbacks, which need careful regulation.

The question of regulating AI under International Law has become an urgent issue at both the national and international levels as AI is having negative impacts on people life, as it also comes with significant disadvantages that need to be carefully managed, these include issues like Job Displacement, Bias and Discrimination, Dependency and Overreliance, Limited Creativity and Understanding, Ethical Challenges.

The major negative impact of AI is Loss of Privacy and Security Risks, as AI is having vast amount of personal and sensitive data that can be hacked which leads to increasing risk of leaking data that is the major problem in today's world. As many people has come under this trap of hackers which leads to damage their life. Therefore, there is an urgent need for regulating AI to reduce its negative impacts on people and to ensure that AI is used responsibly, ethically, and safely by reducing potential harms such as privacy violations, bias and promoting international cooperation.

In the course of this article, the author seeks to analysis "the impact of regulating artificial intelligence under international law" as in today's world people are using AI not for the purpose it was made for " helping people or to solve there doubt and to reduce there burden" but it is being used in negative manner, people are getting trapped by hackers, by the misappropriate use of AI, therefore, there is an urgent need to stops these fraud based on AI by regulating AI.

Keywords: Artificial Intelligence, Dependency, Ethical Challenges, Regulations, Legal Drawbacks.

ARTIFICIAL INTELLIGENCE AND ITS DRAWBACKS IN TODAYS WORLD:

Artificial Intelligence or AI, is a mechanism that is programmed to think and learn like humans. It practices in a certain manner that allow computers and systems to perform tasks that require human intelligence and presence, such as giving a detail decision on any topic, give ideas for problem-solving, understanding language and learning from data. AI in today's world playing major roles in various sectors like: Healthcare, Industry work, Transportation, Customer Service, Finance, Entertainment, Education, Agriculture and etc, which traditionally need humans to perform the same. AI is continually evolving and has the potential to shape almost every aspect of human life, from healthcare and business to entertainment and transportation.

Even today in legal field people are dependent on AI for Document Review and Legal Research, Contract Analysis and Drafting, Case Outcome Predictions, Legal Chatbots and Virtual Assistants and etc, but it lags behind Bias and Discrimination, Lack of Human Judgment and Empathy, Loss of Jobs, Lack of Transparency, Privacy Concerns, Difficulty in Handling Complex or Unstructured Data, Security Risks.

While AI offers many benefits, it also comes with significant disadvantages that need to be carefully managed.

1. Loss of Privacy: AI collects vast amount of personal data from apps and websites like "Instagram, Google, Facebook, Twitter" and other online platform on which we shared our personal details, our photos and video, on which we post about our life style, all these personal and sensitive data attract hackers and by the use of deepfake technology they target people with their frauds. As in today's world most of the hackers generate our personal information from these social media apps and use against us, like by editing the photos and videos post by us, leaking our personal details which leads to bank fraud and other problem which cause people financial damages. AI was formed to help people but it is being misused these days and this need to be regulated under international laws.

2. Security Risks: Use of AI generated security risks in several ways as, AI can be used to launch cyberattacks, AI can be use to generate fake video, voices, and images that can be used for scams, identity theft and political manipulation, it can be use for sending fake emails and messages to threatened people, poorly secured AI models can expose sensitive data like financial details and personal details, Autonomous weapons could be hacked or misused.

Some other negative impacts of AI are Job Displacement, Bias and Discrimination, Lack of Human Judgment, Dependency and Overreliance, Limited Creativity and Ethical Challenges.

CASE STUDY: Unusual CEO Fraud via fake Audio Steals US$243,000 From UK Company:

This case highlight that, Deepfake audio fraud is a new cyberattack to steals moneys and personal information, further highlight how AI can be misused by cybercriminals to make scams.

An unusual case of CEO fraud used a deepfake audio[1], an artificial intelligence (AI)-generated audio, and was reported to have conned US$243,000 from a U.K.-based energy company. According to a report from the Wall Street Journal, in March, the fraudsters used a voice-generating AI software to mimic the voice of the chief executive of the company's Germany-based parent company to facilitate an illegal fund transfer. The cybercriminals called the U.K. company's CEO pretending to be the CEO of the parent company. The attackers demanded that an urgent wire transfer be made to a Hungary-based supplier and the U.K. company's CEO was assured of a reimbursement. After the money had been transferred, it was forwarded to an account in Mexico and then other locations, making the identification of the fraudsters more difficult.

In today's world there are so many cases of cyberattack by misusing AI, that is the major cause behind financial, personal, social and political loss of humans now days and there is urgent need to regulate AI as for the reducing fraud by use of AI.

NEED FOR REGULATING ARTIFICIAL INTELLIGENCE:

AI is rapidly developing several risks that can lead to dangerous consequences on people life if not regulated properly, therefore to reduce the amount of fraud by use of AI there is an urgent need to regulate AI.

There is urgent need of policy to reduce Privacy violations as AI technologies often rely on vast amounts of personal data to function effectively and hacker use that personal and sensitive data against the individual to defame and manipulate to gain money, for example: hacker use personal data like photo and manipulate that to gain money that infringe person privacy, As in today's world most of the hackers generate our personal information from these social media apps and use against us, like by editing the photos and videos post by us, leaking our personal details which leads to bank frauds and other negative impacts. There are major Accountability issues with AI decision. If an AI system makes a harmful decision, such as an autonomous car

---

[1] Trend Micro (MX), Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company| Trend Micro (MX) (last visited Jan. 10, 2026).

causing an accident or a loan denial based on biased data, it is unclear who should be held accountable. There are Security risks also as AI can be used to launch cyberattacks, AI can be used to generate fake video, voices, and images that can be used for scams, identity theft and political manipulation, it can be used for sending fake emails and messages to threatened people.

There are various existing policy and framework at international level to regulate artificial intelligence some are,

1. The European Union's AI Act: The European Commission in April 2021, presented the Artificial Intelligence Act[2], which establishes a well-established framework for regulating AI. The AI Act is one of the first attempts to address AI frauds fully in the European Union. The AI Act was focused on effective, fair and transparent work by and it may serve as a model for other country.

2. OECD AI guidelines: The Organization for Economic Cooperation and Development (OECD) produced guidelines for governance of AI[3] followed by 42 countries, including the United States, Japan, and the European Union. The OECD's guiding principles center on promoting fairness, responsibility and openness in AI, which can be helpful for reducing AI based fraud by securing the system under OECD guidelines.

3. The Role of the UN: The United Nation was given a task for developing international ethical framework and regulation for AI to protect people from frauds, like leakage of personal and sensitive data. The United Nations Educational, Scientific, and Cultural Organization (UNESCO) published a global guideline on regulating AI under ethics in 2021[4]. Guidelines stated that AI should uphold equality, privacy, and human rights.

These are some policies adopted by countries to stop fraud by AI, but the question is **Can Global Regulation Work?** The answer is Maybe, but its not going to be easy due to increase number of frauds by hacker on international level, Countries have vastly different priorities when it comes to AI 'while EU focused on privacy but Asian country focus on innovation and economic development' and to regulate AI on international level there is urgent need to implement existing policies globally and from new policy to protect fraud by AI.

---

[2] EU Artificial Intelligence Act, High-level summary of the AI Act | EU Artificial Intelligence Act (last visited Jan. 10, 2026).
[3] OECD.AI, AI Principles Overview - OECD.AI (last visited Jan 10, 2026).
[4] UNESCO, Recommendation on the Ethics of Artificial Intelligence | UNESCO (last Visited Jan 10, 2026).

FUTURE OF REGULATING AI UNDER INTERNATIONAL LAWS:

As AI taking place in nearly every aspect of society today and influencing peoples political, personal, social and economic life, the future of regulating AI under international laws is becoming a critical concern focusing on the increase amount of fraud by AI like bank fraud, leaking personal and sensitive data of people, fraud call, manipulating photos and video posted by people on social media, all these fraud impact individual privacy and distress them. The rapid growth of AI presents both significant opportunity and risk. To reduce these challenges, international collaboration is essential.

With AI increasingly handling personal and sensitive data, significant concerns are emerging regarding human privacy and safety. AI can accomplish tasks more quickly than humans, but it relies on algorithms or utilizes individuals' personal data to enhance work efficiency. Such work processes can result in biased or discriminatory decisions, misuse personal data, or be vulnerable to hacking; thus, robust and explicit laws must be established to safeguard citizens' information. The government must assume the duty of establishing laws and regulations to safeguard individuals in the digital era. The government needs to establish regulations that ensure AI can be used in a clear and accountable manner.

Today, different countries have different policies and approaches to regulate AI, leading to fragmentation and difference in policies, but to avoid conflicts between country based on policy international organizations like the United Nations (UN), Organization for Economic Co-operation and Development (OECD), and World Trade Organization (WTO) should establish frameworks that countries can voluntarily adopt. Policies should emphasis on ensuring that AI systems respect the privacy rights of individuals and Expect regulations to expand to address the challenges posed by AI and big data, including issues of consent, data ownership, and cross-border data flows.

The future of regulating Artificial Intelligence under international laws will likely involve a combination of global standards, ethical guidelines, safety frameworks, and accountability and transparent policy measures. These regulations will need to evolve rapidly to keep peace and stability with technological advancements and address problems related to safety, privacy, equity, and global collaboration.