LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 2

2024

GROWTH OF ARTIFICIAL INTELLIGENCE (AI) IN THE INDIAN LEGAL SYSTEM AND ITS IMPACT ON CYBER TERRORISM IN INDIA

Ayushi Verma[1]

I. ABSTRACT

"*Artificial Intelligence is not a substitute for human intelligence; it is a tool to amplify human creativity and ingenuity*" **- Fei-Fei-Li (American Computer Scientist)**
AI is a new leading-edge innovation. It is currently restructuring various realms. Traditional methods have been replaced after the unification of AI in different sectors particularly the integration of AI in the Indian legal system. AI has proved helpful in Cyber Space by curbing Cyber threats and ensuring Cybersecurity. The present research study is devoted to how ***"Artificial intelligence"*** has grown in the Indian Legal System. It deals with the use of AI in Cybersecurity. It also traces the present legal framework with regard to AI and Cyberterrorism in India.

II. KEYWORDS

Artificial Intelligence, Cyberterrorism, Cybersecurity, Law, Information Technology Act

III. INTRODUCTION

The rise of "***Artificial Intelligence***" (AI) has been in vogue in the current age of technological revolution. It is a speedily evolving field in almost every industry and profession. It is transforming sectors like healthcare, the economy, and entertainment. Likewise, AI is having a great impact on the legal industry. It has become easier for law students, advocates, and everybody in the legal profession to access any information and to find anything in a short span of time which was earlier impossible to reach.

[1] The Law School, University Of Jammu

 (ISSN: 2583-7753)

AI systems have been installed for better productivity. Everything has its own pros and cons which cannot be avoided. As AI technology continues to develop, people are required to know the balance of its benefits along with the greater risks. AI also benefits the "***Cybersecurity***". The major issues that have been encountered with the growth of AI are the threat of ***"Cyberterrorism" and "Cybercrimes".*** All internet users are the victims of ***"Cyberterrorism" and "Cyberattacks".***

Nearly 20% of internet users were victims of cyber threats in the first quarter of 2024[2]. These Cybercrimes lead to continuous violation of privacy rights. Therefore, there is a dire need to combat these Cybercrimes in order to[3]Protect the privacy rights of an individual. There is a need to combat these crimes as there is s continued violation of the privacy rights of an individual.

IV. RESEARCH OBJECTIVES

- To inspect the growth of AI in the Indian legal industry.
- To explain the correlation between AI and "*Cyberterrorism*" (Pros and Cons of AI in cybersecurity).
- To scrutinize the legal structure in India with regard to AI in terms of "*Cyberterrorism*".

V. RESEARCH QUESTIONS

- How is AI unified into the Indian legal system?
- How does AI benefit to counter the leading risks of "*Cyberterrorism*"?
- How is AI responsible for other "*Cyberattacks*"?
- What do the laws in India provide with regard to AI and *Cyberterrorism*?

[2] The Hindu Bureau, "20% Indian Users Fell Victim to Cyber Threats in the First Quarter of 2024, Finds Study" (The Hindu, May 20, 2024) <https://www.thehindu.com/sci-tech/technology/20-indian-users-fell-victim-to-cyber-threats-in-the-first-quarter-of-2024-finds-study/article68196110.ece> accessed August 16, 2024

[3] The Hindu Bureau, "20% Indian Users Fell Victim to Cyber Threats in the First Quarter of 2024, Finds Study" (The Hindu, May 20, 2024) <https://www.thehindu.com/sci-tech/technology/20-indian-users-fell-victim-to-cyber-threats-in-the-first-quarter-of-2024-finds-study/article68196110.ece> accessed August 16, 2024

VI. RESEARCH HYPOTHESES

- The growth of AI in the Legal Industry in India intensifies the fruitfulness of law enforcement agencies. It becomes easier for law students and lawyers to do any task shortly.
- The AI in law also helps to combat the rising incidents of "*Cyberterrorism*" in India. These technologies are more efficient in preventing "*Cyberterrorism*" rather than previous methods.
- The use of AI in order to prevent "*Cyberterrorism*" also introduces other kinds of risks in Cyberspace. AI is often misused for Cyberattacks also.
- Furthermore, there is no specific law concerning the use of AI in terms of "*Cyberterrorism*".

VII. RESEARCH METHODOLOGY

The research methodology adopted in this paper is strictly doctrinal in nature. It is library-based research. This is a model method for theoretical study. In this research sources such as statutory materials, doctrines, legal articles, legal writings, and case studies are used.

This research is comprised of identification, gathering, and evaluation of these sources. The only object is to obtain logical conclusions and to provide an understanding of the legal questions that are being studied.

VIII. LITERATURE REVIEW

- Human work has been displaced by Artificial Intelligence. AI can do anything that a human can do by application of knowledge. The beginning of AI has brought a revolution, especially in the legal Industry. It helps in research and analysis which is hard for lawyers and legal experts. This technology can be known as Time Saviour.
- Cybercrimes such as Cyberterrorism have been in the news in recent times. AI has done a magnificent job in the field of cybersecurity. By its deployment threats can be detected easily.

- AI also attracts many cyber threats and other vulnerabilities. "***If it is a boon, it is also a bane".*** Many terrorists have committed cyberterrorism by misusing AI. They have operated many planned attacks such as the 26/11 Mumbai terror attack (Case: ***Mohammed Ajmal Amir Kasab v. State of Maharashtra)***
- India has no particular legislation for the regulation of AI. But its inference can be found in legislations like ***the IT Act, 2000, the UAPA Act, 1967, the DPDP Act, 2023***, and frameworks like the ***National Strategy for Artificial Intelligence (NSAI), 2018, National Cyber Security Policy, 2013.***

IX. ARTIFICIAL INTELLIGENCE (AI)

AI is a discipline of computer science that helps to perform the tasks that generally require human intelligence. It is also known as machine learning.

A. Types of AI

- **Narrow AI:** This kind of AI is weak and only designed for a particular task.
- **Generative AI:** This kind of AI is strong. This is designed in such a way that it understands the problem, applies the knowledge, and gives the required result. This works in the same way a human does.

B. Growth Of Artificial Intelligence In Indian Legal Industry From Traditional Legal Practices To AI Unification

AI has reformed and revolutionized all sectors across the world including India. Due to digitalization, it has influenced the legal sector in both positive and negative manner. Indian legal system is known for its complex nature.

In the past days, the approach used by legal experts and lawyers was manual in order to do legal research. This was done by consulting a lot of books, commentaries, statutes, etc. Now with the passage of time, AI technologies are being integrated into this legal sector in order to save time and avoid laborious work.

Various databases and tools are being created for law students and legal experts to make their research easier. Some of them are ***CaseMine, NearLaw, SpotDraft, IndianKanoon***, etc.

Following are fields that provide how AI helps lawyers and law students in day-to-day life:

- **Automated Legal Research:** AI is a timesaver. Law practitioners can automate all kinds of legal research with the help of AI apps and databases. This will help to increase their productivity.
- **Prediction Technology:** With the help of AI legal experts can access any kind of knowledge and analysis and can make predictions on their basis more accurately.
- **Mode of Expedition**: As AI can solve any kind of problem and give the required result within seconds, this helps to expedite legal proceedings in countries like India which have dilatory judicial systems having a lot of pending cases.
- **Creation and review of contracts:** Contract creation is one of the most time-consuming works. AI can create contracts automatically by giving the proper commands. This will be beneficial in providing accuracy to the work. This will lower the chances of mistakes. Also, contracts can be reviewed by various AI tools.
- **Virtual legal proceedings:** Apart from drafting and researching, proceedings have started to take place on online platforms. This helps to resolve cases in a more efficient manner.

C. Examples Of Application Of AI In The Indian Legal System

- **SUPREME COURT OF INDIA:** There is an overburdening of pending cases in the '*Supreme Court of India*' and consequently, the Justice gets delayed. Many steps have also been taken in the past time but nothing happened. Recently, an AI-based portal ***"SUPACE" (SUPREME COURT PORTAL FOR***

ASSISTANCE IN COURT EFFICIENCY) was launched by the *Chief Justice of India.* The aim of this portal is to provide legal assistance to the judges.

- Another AI portal that is being used by the Supreme Court of India is ***" (SUPREME COURT VIDHIK ANUVAAD SOFTWARE).*** This system helps to translate the judgments into regional languages. Supreme Court of India is ***"SUVAS" (SUPREME COURT VIDHIK ANUVAAD SOFTWARE).*** This system helps to translate the judgments into regional languages.
- **Case:** *Jaswinder Singh v. State of Punjab*[4] In this case, a bail petition was rejected by the court on the basis that the accused was involved in brutal assault as alleged by the prosecution. In this case, the court requested a wider perspective on bail provision by the use of ***ChatGPT.*** This was only a reference.
- **Initiative Taken By The Maharashtra Government:** Recently, an AI database *"**MahaOnline**"* is launched by the Maharashtra Government. This app was launched in cooperation with NIC (National Informatics Centre). This AI tool is a type of bot that provides legal assistance.
- **Use of AI in Delhi NLU:** The NLU Delhi has also introduced the use of AI systems and tools in academics for legal study. Students are provided with systems like ***"ROSS", "LexisNexis", and "Kira systems".*** These systems help to make legal research easier. Influenced by ***"ROSS Intelligence"*** which is mostly used in the United States, India has also introduced tools like IBM Watson's AI for legal experts and law students.

X. NEXUS BETWEEN "AI" AND "CYBERTERRORISM

With the revolution of technology, the risks of Cyber threats and Cyberterrorism are becoming more prevalent. The same is the case with the growing abilities of AI. The relationship between AI and Cyberterrorism is multidimensional. AI is contributing to Cybersecurity in both negative and positive aspects.

[4] Jaswinder Singh v. State of Punjab (2022) 2 SCC 84

A. Cyber Security: Meaning

Cyber Security refers to the policy of *defending computers, and computer resources.* It aims to prevent Cyberattacks and lessen their impact.

B. Cyberterrorism: Meaning

*The term **'Cyberterrorism'** was coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. Its use became prevalent during the 9/11 attack*[5].

The Federal Bureau of Investigation (FBI) defined cyber terrorism as: *"Previously planned, politically motivated attack against information, computer systems, computer programs and data that result with violence against targets that are not military (civilian) by the sub-national groups or secret agents"*

It refers to carrying out violent and disruptive activities through the use of the internet which are threats to human life. This is done by using:

- Malicious software
- Phishing
- Computer worms
- Viruses, etc

C. Cyberterrorism in India

Some of the most terrifying incidents of Cyberterrorism to which India fell prey because of the misuse of digital technology are:

- URI attack
- Pulwama attack
- 26/11 Mumbai attack

Cyber Criminals execute their malicious propaganda over the internet in Cyberspace. It was remarked by the defense minister Rajnath Singh that now the enemy does not

[5] Plotnek JJ and Slay J, "Cyber Terrorism: A Homogenized Taxonomy and Definition" (2021) 102 Computers & Security 102145

need to enter through the borders. They use malicious software and the internet and operate everything only by sitting *in their Home Country*.

XI. ROLE OF ARTIFICIAL INTELLIGENCE IN CURBING CYBERTERRORISM AND CYBER CRIMES: PROS OF AI

AI is doing a great job in the field of Cyber Security by offering significant advancements. AI helps to prevent Cyber Crimes such as Cyberterrorism.

- **Threat Detection:** An ordinary person cannot detect any kind of cyber risk in their company. Every year hackers and cyber criminals carry out crimes and terrorism for one or the other reasons. But AI has helped to get rid of these crimes and terrorism. AI is an expert in pattern identification by using predictive analytical approaches in various databases. This approach can help in the field of Cyber Security to detect threats. AI can analyze the incidental history and recognize the patterns which will help to detect any kind of threat earlier and prevent any kind of cyber-attack in the future.
- **Analysis of user's behavior:** AI can study the behavior of the user and their activities to detect threats. This will help to prevent any kind of suspicious action by Cyber terrorists.
- **Machine learning Models:** Various Machine learning models are designed. They are designed in such a way that they have datasets that can track any kind of malicious activity. They block these patterns in real-time which helps to mitigate the threats.
- **Natural language processing:** There are also AI-driven systems known as ***Natural language processing (NLP).*** These systems analyze the unstructured data such as text from different sources like social media, reports, etc. This helps to provide more insight into upcoming threats.
- **Automatic responsive technology:** AI systems have the installation of predefined responsive protocols. They are created in such a way that they have the capability to block upcoming attacks with the help of such tools.

XII. CHALLENGES AND VULNERABILITIES INTRODUCED BY AI IN CYBER SECURITY: CONS OF AI

Since AI helps to counter cyberterrorism and other kinds of cyber-attacks. On the other hand, there are many vulnerabilities and risks that are born by the use of AI in the context of Cybersecurity.

- **Cyber Attacks powered by AI**: Many terrorists misuse AI technologies and tools to fulfill their malicious propaganda. They use AI to carry out the crimes in the most organized ways. For instance: Malware is created by the use of AI, AI can be used to automize the identification of risks, and It can be used to create advanced phishing attacks.
- **Deepfakes and disinformation**: Many people use AI in a worse manner than they create deepfakes and disseminate wrong information throughout social media. These are the gadgets that are being used by cyber terrorists nowadays and anyone can be a victim of this trap.
- **Data privacy and security:** One of the major concerns with the use of AI is data privacy and security. Cyber criminals misuse AI to hack anybody's electronic devices which is the infringement of their privacy and personal rights.
- **Threats to AI systems:** Cyber criminals are deploying methods to manipulate AI systems that exploit them so that they will not be able to prevent cyber-attacks.
- **Bias and Errors:** Apart from the advancement of AI, its results can be biased and full of errors because of its trained data, which may overlook the threats.
- **Poisoning of data**: A lot of data for training is required in machine learning. Cyber terrorists or criminals can inject malicious data into these training datasets. This will automatically provide an advantage to cyber terrorists.

XIII. CASE LAW

Mohammed Ajmal Amir Kasab v. State of Maharashtra[6]

This case law was related to the 26/11 Mumbai terror attack. This attack was a lively example of Cyber Terrorism. In this attack, terrorists used sophisticated technology for the coordination of the attacks. The Supreme Court laid down the emphasis on the need for stringent laws and technological measures for the prevention of Cyber Terrorism. The Court underlined the future role of Artificial Intelligence in the domain of Cyber Security.

State of Uttar Pradesh v. Arif Khan[7]

In this case, Arif Khan was convicted under UAPA and IPC and was given the punishment of life imprisonment. He was convicted because he was involved in the terrorists' activities. He developed an AI-based bot by the use of which he was trying to deploy the youth into terrorist organizations.

XIV. LEGAL FRAMEWORK IN INDIA FOR THE REGULATION OF AI IN TERMS OF CYBERTERRORISM

Currently, there is no specific law that deals with Artificial Intelligence in the context of Cyberterrorism. But it is regulated by various existing laws and policies indirectly.

A. Information Technology Act, 2000 (IT Act)

This is the primary legislation for the protection of data.

Section 66[8] Deals with "Computer-related offenses". It provides that:

- *"If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both."*

[6] Mohammed Ajmal Amir Kasab v. State of Maharashtra (2012) 9 SCC 1
[7] State of Uttar Pradesh v. Arif Khan (2022) SCC Online SC 1084
[8] The Information Technology Act, 2000, s. 66

Section 66F[9] The IT Act deals with punishment for Cyberterrorism. According to this section:

- *"Anybody who has the intention to threaten or strike terror in people by denying access to the computer, by accessing the computer without any authorization, by introducing any contaminant in the computer, and by this act causes death or is likely to cause death to any person or causes damage to the property of any person.*
- *Anybody who intentionally accesses any computer resource and by such conduct accesses any data or information which is restricted because of the security of the State or foreign relations and information so obtained causes any injury or is likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offense, or to the advantage of any foreign nation, group of individuals.*
- *shall be liable for the offence of cyber terrorism and such person shall be punishable with imprisonment which may extend to imprisonment for life".*

IT Act does not mention AI in express words. But AI systems used in the activities of Cyberterrorism can fall under the purview of this particular section.

For instance, AI algorithms that are used to launch any advanced cyber-attack will fall under this section.

- **Section 67B** deals with "*Punishment for publishing or transmitting of material depicting children in the sexually explicit act, etc., in electronic form*"[10].

B. Unlawful Activities (Prevention) Act, 1967 (UAPA)

This is an anti-terrorism law.

Section 15[11] The act defines terrorist attacks which also covers cyberterrorism. In addition to this, it also covers the acts of Cyberterrorism done by using AI systems to disseminate misinformation and hate propaganda.

[9] The Information Technology Act, 2000 (Act 21 of 2000), s.66F
[10] The Information Technology Act, 2000, s. 67B
[11] The Unlawful Activities (Prevention) Act, 1967, s. 15

Section 16[12] of the act provides ***"Punishment for terrorist acts"***

- If the terrorist act resulted in the death of any person, he shall be punished with death or imprisonment for life, and shall also be liable to fine
- In other cases, such a person shall be punished with imprisonment for a term not less than five years which may extend to imprisonment for life, and shall also be liable to fine.

C. The Digital Personal Data Protection Act, 2023

The DPDP Act aims to protect personal data in the age of digitalization. This Act applies to fully or partly automated processing of personal data. While this does not expressly mention AI. However, the definition of processing and automation is wide to include the processing of personal data by using AI.

- **Section 2(b)**[13] provides that: **"***Automated means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data"*
- **Section 2(x)**[14] Provides that: **"***Processing in relation to personal data means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction*".

D. National Strategy for Artificial Intelligence (NSAI), 2018

This policy was released in 2018 by NITI Ayog. This framework provides a comprehensive policy for the development and implementation of Artificial Intelligence (AI) among various sectors. Although this policy does not link AI with

[12] The Unlawful Activities (Prevention) Act, 1967, s.16
[13] The Digital Personal Data Protection Act, 2023, s.2(b)
[14] The Digital Personal Data Protection Act, 2023, s.2(x)

Cyber terrorism in a direct manner but aims to address security concerns like Cyber threats. NITI Ayog introduced seven responsible AI principles which are:

- safety & dependability
- equality
- inclusivity and non-discrimination
- privacy and security
- transparency
- accountability and
- the protection and reinforcement of positive human values.

E. National Cyber Security Policy, 2013

This policy was introduced by MEITY. This policy was implemented to secure the cyber ecosystem, enhancing E-Governance services, protection of information infrastructure, prevention of challenges posed by Artificial Intelligence, etc.

F. Advisory issues by "The Ministry of Electronics and Information Technology"

MEITY is a government body constituted for the regulation of internet-related issues.

Recently, it has issued two advisories for the regulation of Artificial Intelligence.

- **1st advisory:** The first advisory was issued on 1st March. This advisory has the work to ensure that all the intermediaries and digital platforms must comply with the terms of the "***Intermediary Guidelines and Digital Media Ethics Code, 2023".*** The advisory also came up with unreliable AI models.
- **2nd advisory:** The second advisory was released on 15th March. This replaced the previous advisory. This expands the repercussions for non-compliance with the guidelines given under the ***IT Act, of 2000.***

There are also other frameworks like the *National Investigation Agency Act, 2008, and Police Powers and Responsibilities Rules, 2020.*

XV. FUTURE DIRECTIONS: POLICY RECOMMENDATIONS

In today's digital era, the use of AI in every sector is increasing. There are still loopholes in its use. There is a need to strengthen the use of AI, especially in blocking and resisting Cyber threats. Following are some of the policy recommendations, so that AI can work in a more effective manner:

- **Specific legislation for AI**: There shall be particular legislation for AI use in the ambit of Cybersecurity. This will help to ensure more transparency and accountability. Also, ethics shall be laid down and compulsory provisions for its adoption shall be made so that its misuse can be avoided.
- **Regulatory body:** A permanent regulatory body shall be established which shall address the AI deployment in Cybersecurity. Also, to ensure that all AI systems are in compliance with the laws.
- **AI risk management system**: A system shall be developed so that all the risks and damages can be assessed earlier due to the development of AI systems.
- **International cooperation**: International Cooperation and agreements with regard to the use of AI shall be strengthened so that Cyberterrorism can be prevented even globally.

XVI. CONCLUSION

The use of AI kept evolving in every field of society. It has made the task of law enforcement agencies easier to detect any upcoming threat. It has proved useful in combatting Cybercrimes like cyberterrorism more efficiently. There are many lacunas in its use. On one side AI helps to curb cyber terrorism and on the other side, it also leads to other cyber risks.

In India, proper legislation and a regulatory body shall be created to avoid any trouble in the future. In addition to this, people should rely less on AI systems and tools. If there is continuous reliance on these advanced technologies, the human mind will become inactive which will lower their critical thinking and reasoning.

XVII. REFERENCES

- The Information Technology Act, (2000).
- The Unlawful Activities (Prevention) Act, (1967).
- The Digital Personal Data Protection Act, (2023)
- The National Strategy for Artificial Intelligence (NSAI), 2018
- The National Cyber Security Policy, 2013
- Mohammed Ajmal Amir Kasab v. State of Maharashtra (2012) 9 SCC 1
- State of Uttar Pradesh v. Arif Khan (2022) SCC Online SC 1084
- Prabhu, A. (2023, August 12). Artificial intelligence in the context of the Indian legal profession and judicial system. *Bar and Bench - Indian Legal News*. https://www.barandbench.com/columns/artificial-intelligence-in-context-of-legal-profession-and-indian-judicial-system
- *Analysing AI and The Digital Personal Data Protection Act 2023*. (n.d.). Khaitan & Co. https://compass.khaitanco.com/analysing-ai-and-the-digital-personal-data-protection-act-2023
- Mishra, P. K. (2024, February 27). Law and AI, legal framework and challenges, AI-powered tools, General Data Protection Regulation (GDPR). *Live Law*. https://www.livelaw.in/lawschool/articles/law-and-ai-ai-powered-tools-general-data-protection-regulation-250673
- The Hindu Bureau. (2024, May 20). *20% of Indian users fell victim to cyber threats in the first quarter of 2024, finds study*. The Hindu. https://www.thehindu.com/sci-tech/technology/20-indian-users-fell-victim-to-cyber-threats-in-the-first-quarter-of-2024-finds-study/article68196110.ece
- *AI in cybersecurity: Pros and Cons*. (n.d.). SecOps® Solution. https://www.secopsolution.com/blog/ai-in-cybersecurity-pros-and-cons

- Dandge, P. S., Dawre, U. I., & Shirshikar, R. F. (2023, December 25). *Artificial intelligence in cyber security*. Auricle Technologies Pvt., Ltd. https://www.researchgate.net/publication/377962451_Artificial_Intelligence_In_Cyber_Security