Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

Cybercrime, Cyber Protection, and Cyber Laws in India

Karthik Vijayanand[a]

[a]CHRIST University, Bangalore, India

Received 23 January 2022; *Accepted* 13 February 2023; *Published* 17 February 2023

One of the fastest-growing fields in the world is cyberspace. Cyberspace is home to both boons and banes to the world. Considering cyberspace in India is inevitably inviting cybercrimes in various forms ranging from hacking and phishing to fraud and cyberstalking. With India becoming the second-largest online market in the world, cybercrime rates in India have been startling to the public. One way to deal with cybercrimes might be by recognizing who is behind cybercrimes in India which usually ranges from hackers to criminal syndicates. People must also be made aware of the cyber laws that exist in the country so that such crimes may be prevented and the criminals may be penalized. Artificial intelligence (AI) is a wing of cyberspace and inseparably a part of it. Further, with the development of the metaverse, cyberspace is sure to flourish. But cyberspace is still prone to cybercrimes through AI and metaverse. Hence, this paper through a doctrinal mode of research, addresses the cybercrimes specifically mentioning AI and metaverse, and laws regarding cybercrimes in India. It also talks about the dependency of the public on technology and aims to establish a relationship between AI, metaverse, and cybercrime and suggests laws that may be developed in the future for covering the loopholes in the law. This paper also suggests ways in which individuals and corporates can protect themselves from cybercrimes. It brings out cyber mitigation ways provided by companies that assess and quantify the risk prone to the data of corporate epitomes.

Keywords: *cybercrime, cyber protection, cyber law, ai, metaverse.*

INTRODUCTION

Cybercrime is an unlawful act where the computer is used as a tool or target to commit an offence in cyberspace. [1] It encompasses activities such as the illegal obtaining of confidential data, unauthorized access to systems, malicious destruction of networks, and exploitation of vulnerable computers.[2] For a simpler understanding, cyber crime can be categorized in two ways:

Computer as a target – the computers are targeted to commit the crime.[3] *E.g.* Hacking, Virus attacks, etc.

Computer as a tool – the computer is used as a weapon to commit a crime.[4] *E.g.* Cyber terrorism, Credit card fraud, etc.

CYBERCRIMES IN INDIA

Cybercrime in India is on the rise and is witnessing an increase in the number of cybercrimes being reported. India was ranked 10th for cyber security in the world according to the 4th edition of the Global Cybersecurity Index 2020[5]. Cybercrimes have increased fourfold in India, in recent years. Cybercrimes in India take many forms, from phishing and fraud to hacking and cyberstalking. The majority of the cyber crimes in India are related to phishing, credit/debit card fraud, and online financial fraud. Cyber accident scams where criminals lure people through fake ads or websites to click on malicious links and download malicious software, and then obtain personal data using it is one of the common cyberspace scams in India.

Hacking, the biggest fear of corporates cannot be overlooked while talking about cybercrimes. Hackers use a variety of malicious software, such as Ransomware, Trojan, and Spyware to steal

[1] 'Information Security Awareness' (*Infosec Awareness*) <https://infosecawareness.in/cyber-laws-of-india> accessed 22 January 2023
[2] *Ibid*
[3] *Ibid*
[4] *Ibid*
[5] 'Global Cybersecurity Index' (*Byju's*) <https://byjus.com/free-ias-prep/global-cybersecurity-index-itu/> accessed 22 January 2023

individuals' data and extort money from them. India is the second largest online market in the world with 560 million internet users. It reported an astonishing 52,974 cybercrime cases across the country in 2021. Cybercrime is a growing problem in India, with criminals using increasingly sophisticated methods to target victims. The country's lack of public awareness about cybercrime and lack of skilled cybersecurity professionals are factors that contribute to this issue. Popular names such as Tata Power, CDSL, and AIIMS (Delhi) which are no less than national critical assets in different sectors have all been hit by cyber attacks in the recent past.

WHO IS BEHIND CYBERCRIME IN INDIA?

Cybercriminals come from various backgrounds and can range from individual hackers to criminal syndicates. There are groups of hackers who use sophisticated software to gain access to confidential data and launch cyber attacks against governments and corporations, as well as individual hackers who use malware or phishing to steal information from their victims. Organized criminal gangs are also using cybercrime as a way of making money, and the proliferation of the dark web and cryptocurrency has enabled them to operate with greater concealment. Though there are cyber laws in India, cybercriminals operate with impunity and keep flourishing. The reason for this could be that the law has not been enforced sufficiently to prevent crime in cyberspace.

LAWS GOVERNING CYBERCRIMES IN INDIA

In India, the Indian Penal Code, of 1860[6] and the Information Technology Act, of 2000[7] are the two legislations that provide for punishment for cybercrimes in India. The Information Technology Act, of 2000 was enacted to provide legal recognition to electronic commerce and transactions. It also provides for punishment for offences like hacking, data theft, cyber terrorism, etc. Some of the sections highlighting cybercrimes from this act are Section 43,[8] Section

[6] Indian Penal Code 1860
[7] Information Technology Act 2000
[8] Information Technology Act 2000, s 43

66,[9] Section 66B,[10] Section 66C,[11] Section 66D,[12] Section 66E,[13] Section 66F[14] , and Section 67[15].[16] The Indian Penal Code, of 1860 provides for punishments for offences like fraud, forgery, identity theft, etc. Some of the sections which provide punishment for cybercrimes from this code are Section 292,[17] Section 354C,[18] Section 354D,[19] Section 379,[20] Section 420,[21] Section 463,[22] Section 465[23] , and Section 468[24].[25]

ARTIFICIAL INTELLIGENCE AND CYBERCRIME

Artificial Intelligence (AI) has been defined in various ways as per different perceptions. The simplest way to define it could be AI is the emulation of human intelligence by machines, particularly computer systems[26]. AI has been adopted across various sectors such as agriculture, healthcare, education, etc.[27] While AI can be used for legitimate purposes, it is also being harnessed by criminals to automate attacks and carry out sophisticated fraud. Cybercriminals are using AI algorithms to perform attacks against victims in cyberspace. AI is used in a variety of cyber activities including but not limited to:

- AI-powered chatbots to carry out phishing and spam attacks[28]

[9] Information Technology Act 2000, s 66
[10] Information Technology Act 2000, s 66B
[11] Information Technology Act 2000, s 66C
[12] Information Technology Act 2000, s 66D
[13] Information Technology Act 2000, s 66E
[14] Information Technology Act 2000, s 66F
[15] Information Technology Act 2000, s 67
[16] *Ibid*
[17] Indian Penal Code 1860, s 292
[18] Indian Penal Code 1860, s 354C
[19] Indian Penal Code 1860, s 354D
[20] Indian Penal Code 1860, s 379
[21] Indian Penal Code 1860, s 420
[22] Indian Penal Code 1860, s 463
[23] Indian Penal Code 1860, s 465
[24] Indian Penal Code 1860, s 468
[25] *Ibid*
[26] Ed Burns, 'What is Artificial Intelligence (AI)?' (*Tech Target*) <https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence> accessed 23 January 2023
[27] *Ibid*
[28] *Ibid*

- Designing and automating malware attacks[29]
- Creating botnets[30]

Through AI, the person being deceived would not even know that he is chatting with an AI-powered system or a real person. Such could be the illegitimate use and capability of AI in cyberspace.

METAVERSE AND CYBERCRIME

One of the most popular platforms for cybercrime in India is the metaverse. The metaverse is a virtual world created and maintained by users. [31] It bridges the gap between physical and virtual interactions and experiences.[32] It can be used for a variety of purposes like social networking, gaming, and shopping. Even decentralized digital currencies such as bitcoin and other cryptocurrencies are a part of the metaverse which has led to a quick expansion in the blockchain industry in recent years laying the groundwork for the economy in the virtual world.[33]India is currently ranked in the fifth position among the top nations driving the metaverse market. According to market projections, India's metaverse market is anticipated to expand at a remarkable CAGR of 37.1% and reach a staggering $758 billion by the end of 2026. This, though an advancement in technology, is also a detriment to society as it also becomes a medium used to commit crimes. The metaverse is frequently used by criminals to commit crimes such as identity theft, phishing, and money laundering.

IS THERE A RELATIONSHIP BETWEEN AI, METAVERSE, AND CYBERCRIME?

The phrase "metaverse" refers to a speculative future version of the internet that integrates and is based on augmented reality, virtual reality, and virtual worlds.[34] The metaverse is

[29] *Ibid*
[30] *Ibid*
[31] Deborah Lovich, 'What Is The Metaverse And Why Should You Care?' (*Forbes*, 11 March 2022) <https://www.forbes.com/sites/deborahlovich/2022/05/11/what-is-the-metaverse-and-why-should-you-care/> accessed 23 January 2023
[32] *Ibid*
[33] *Ibid*
[34] Hanna Hryshkevich, 'How AI and the Metaverse Work Together' (*AI Time Journal*, 2 February 2023) <https://www.aitimejournal.com/how-ai-and-the-metaverse-work-together> accessed 23 January 2023

hypothetical at the moment, but it may one day enable individuals to interact, transact, play, learn, work, and carry out more activities through a centralized virtual experience.[35] The metaverse is not currently existed but is on the verge of being developed shortly.

On the other hand, AI is used to streamline many company processes and helps users find solutions to their problems much more quickly, one of the ways being chatbots.[36] This method of communication shall be used in the metaverse as well. Chatbots can help users in the metaverse by giving them instructions and information about various goods and services, answering their questions, carrying out transactions on users' behalf, taking orders, etc., in addition to their current roles in customer service, marketing, sales, and other areas.[37] For instance, if a user is having trouble finding a particular item, the chatbot can quickly fix the issue by pointing the user in the right direction within the Metaverse.

On keenly observing AI and metaverse, both can be found to be closely interrelated. Both these are inseparably a part of the virtual world. AI can contribute to the Metaverse to become a user-friendly and simple platform. Users will be able to communicate with the Metaverse in their local language and through photos and videos owing to technologies like Natural Language Processing (NLP), speech recognition, computer vision, translation, and augmented reality, which will improve user-metaverse interactions.[38] Another way AI can work with the metaverse is through digital avatars.[39] AI may assist in creating surroundings, speech, and visuals by utilizing NLP, virtual reality, and computer vision to give people realistic avatars that represent them.[40] To add on, by making lifelike avatars, producing fresh digital goods and services, and enabling remote work and collaboration, AI can help the metaverse fulfill its potential. Businesses should use the metaverse as a hub for creativity and innovation, and they should use AI to develop new goods and services that will boost customer satisfaction and offer them a competitive edge.[41] The metaverse has the power to alter the way we live and operate, and AI

[35] *Ibid*
[36] *Ibid*
[37] *Ibid*
[38] *Ibid*
[39] *Ibid*
[40] *Ibid*
[41] *Ibid*

can assist in making this a reality. Briefly put, AI can engage with the Metaverse in a variety of ways, namely through digital avatars, chatbots, interfaces, and more. Artificial intelligence may advance even further, until the arrival of the metaverse, which will open up new prospects for collaboration among various technologies.

As AI and metaverse are technology, any wrong happening through them shall fall under the ambit of cybercrime and be known as cybercrime. Currently, there are no legislations regarding the metaverse as it is yet to become a reality. But once it comes into existence, laws regarding the same can be expected soon. AI can be interpreted to be impliedly a part of cyber law as it is what hackers use to make cyber attacks.

DEPENDENCY OVER TECHNOLOGY

Is dependency on technology and further development of it, in the form of AI and metaverse leading to increased cybercrimes?

The answer to this question might not be a straightforward yes and may involve certain complications. Technological upgradation and development can be a boon till the time it is used within certain circumscribing limits. Development in this ecosystem is to increase the convenience and comforts of society. It is to make the tasks easier through the creation of technologies that can decrease physical labour and alternatively prove effectiveness with minimal scope for error. But even technology needs supervision so that the task can be programmed and performed in the right manner. If technology completely replaces physical labour, then it would lead to a large-scale situation of unemployment and subsequently an end to the human race.

The development of AI-powered robots is one of the inventions of technology. They are capable of performing the tasks of man most efficiently and effectively with hardly any scope for error. They were invented to assist humans in their activities and also are being developed for military purposes. But there are certain incidents where the boon of these robots has turned out to be a bane. One such incident report stated was the death of a 24-year-old worker Ramji Lal at SKH Metals Factory in Manesar, India by the piercing of a factory robot. When incidents such as those

stated above occur, then it must be understood that further technological upgradation in the same domain must happen with utmost care as human life is the most valuable thing in this world and nothing can compensate for such human loss.

DEVELOPMENT OF LAW IN THE CYBERSPACE

According to the incident of Ramji Lal, as stated above, it can be implied that there has been a certain lapse of services and irresponsible manufacturing of the robot by the company which has led to a malfunction of the factory robot, subsequently causing the death of the aforementioned. It can also be observed that Ramji was not taken care of by his employer and there was no preparation in the form of safety equipment mandated to be worn by the factory employees to prevent any malfunction of the robots which might cause harm. From the above, there can be a certain form of liability that can be established over the company manufacturing the AI-powered robots for factories. Liability can take different forms when they are distinguished as intentional or unintentional wrongs in the legal acumen. If it is intentional, then it may amount to murder falling within the ambit of criminal law. But if it is unintentional, then it can be considered to be negligence on the part of the manufacturing company falling within the purview of the law of torts.

With further development coming into existence in legislation governing cyber law, the murder mentioned above which happens through AI-powered robots can as well be considered a cybercrime. But currently, there is no such legislation that talks about murder by AI-powered robots, though in the future there can be scrutiny in this area considering it to be a cybercrime.

HOW CAN ONE PROTECT THEMSELVES FROM CYBERCRIME IN INDIA?

Given the prevalence of cybercrime in India, it is important to take the necessary steps to protect ourselves and our data. Initially, it is necessary to be aware of the different types of cybercrime and to recognize the warning signs of a malicious attack. With the continued growth of the metaverse, we will likely see more instances of cybercrime in this space. There are a few simple things that users can do to protect themselves from cybercrime in the metaverse:

- **Use of a strong and unique password –** A strong password is difficult to guess and contains a mix of upper and lower case letters, numbers, and symbols. Unique means that we should use a different password for each account we have.[42]
- **Keep your software up to date –** Hackers often exploit security vulnerabilities in software to gain access to systems. By keeping our software up to date, we can help to close these vulnerabilities and make it more difficult for hackers to gain access.[43]
- **Be cautious of links and attachments –** Metaverse is full of links and attachments, many of which may be malicious. So we need to be cautious of clicking on links or opening attachments from unknown senders.
- **Use two-factor authentication –** Two-factor authentication adds an extra layer of security to our account by requiring us to enter a code from our mobile phone in addition to our password. This makes it much more difficult for hackers to gain access to our accounts.[44]

To add on, for corporates to be aware of the cyber risks that they are prone to, they may utilize the services of companies that assess the risk of data loss from cyber threats. One such company which performs cyber risk assessment and quantification is Transasia Soft Tech Pvt Ltd. Companies like the previously mentioned, use automated risk modelling to conduct such cyber assessments and quantify risk. Further, this assessment provides a holistic view of the organisation's cyber risk and its ability to withstand a cyber attack. The importance of these companies is yet to reach the crowd at large. But the day is not too far when these companies would become one of the most wanted service providers shortly with the bane that metaverse brings coupled with AI in the future.

CONCLUSION

To wrap things up, cybercrime is a growing problem in India, with criminals using increasingly sophisticated methods to target victims. It is important to be aware of different types of cybercrimes and to take the necessary steps to protect yourself. Knowing the warning signs of a

[42] '4 Things You Can Do To Keep Yourself Cyber Safe ' (*Cyber Security and Infrastructure Security Agency*, 18 December 2022) <https://www.cisa.gov/4-things-you-can-do-keep-yourself-cyber-safe accessed 23 January 2023
[43] *Ibid*
[44] *Ibid*

malicious attack and being proactive in your online behaviour can go a long way in deterring cybercriminals. It is also essential to ensure that your systems are secure and to use strong passwords and two-factor authentication. By understanding the cybercrime landscape in India and taking the appropriate measures, you can make sure that your online experience is secure. Cybercriminals will never go away. But by taking the right precautions, you can protect yourself and enjoy your online experience without worrying about their next attack.