DIGITAL FORENSICS AND CYBER SECURITY IN THE WORLD OF METAVERSE AND ARTIFICIAL INTELLIGENCE – IN THE CONTEXT OF THE INDIAN LEGAL SYSTEM

Anand Shankar*

ABSTRACT

Digital forensics and cyber security have become increasingly important in the world of Metaverse and Artificial Intelligence as these technologies continue to evolve and shape our digital landscape. Metaverse refers to the concept of a shared virtual space that is accessible to individuals from all over the world, while AI involves the development of intelligent systems that can perform tasks that would typically require human intelligence. As the Metaverse becomes more widespread and AI becomes more sophisticated, the potential for cyber threats and attacks increases, making it crucial to have effective digital forensics and cyber security measures in place. These measures include techniques for detecting and preventing cyber-attacks, as well as methods for investigating and analysing digital evidence in the event of an attack or other security incident. In addition to traditional cyber security threats, such as hacking and malware, the Metaverse and Artificial Intelligence present unique challenges related to data privacy, identity theft, and virtual asset theft. To address these challenges, new technologies and methods are being developed to secure virtual spaces and protect personal information in the Metaverse. Overall, the continued growth of the Metaverse and Artificial Intelligence presents exciting opportunities for innovation and collaboration, but it also requires vigilance and proactive measures to ensure the safety and security of individuals and their digital assets. Digital forensics and cyber security will play a critical role in achieving this goal. This article aims to find out the issues relating to cyber security with the growth of Metaverse and AI and available legal frameworks in India to trace the footprints of cyber criminals for investigation and collection of evidence.

Keywords: Digital Forensics, Metaverse, Artificial Intelligence, Cyber Criminals, Cyber Security, Cyber Attack, Data, Privacy, Identity, Virtual.

*LLM, GALGOTIAS UNIVERSITY, GREATER NOIDA.

HYPOTHESIS

India needs to run fast to strengthen digital forensics and cyber security in the fast-growing digital world. The world of metaverse and artificial intelligence in the Indian legal system will lead to several issues if not dedicatedly focused to improve the protection of digital assets and data, increased accountability of online activities, and improved enforcement of cyber laws.

AN INTRODUCTION

Digital forensics and cybersecurity are two closely related fields that are becoming increasingly important in today's digital age. In India, with the rise of digital technologies, the need for digital forensics and cybersecurity experts has become more pressing than ever before. Digital forensics is the process of investigating digital devices, such as computers, mobile phones, and other electronic storage devices, to gather evidence for use in legal proceedings. It involves collecting, analysing, and presenting digital evidence in a manner that is admissible in court. Digital forensics can be used in a variety of cases, such as cybercrime, intellectual property theft, fraud, and even homicide. Cybersecurity, on the other hand, is the practice of protecting computer systems, networks, and data from unauthorized access, theft, damage, or disruption. Cybersecurity is essential in today's world because of the growing number of cyber threats that organizations and individuals face. Cyber-attacks can result in financial loss, reputational damage, and even national security threats.

In India, digital forensics and cybersecurity have become increasingly important due to the rapid growth of the country's digital economy. India has one of the largest populations of internet users in the world, and this trend is only expected to continue in the coming years. With the increasing adoption of digital technologies, the risk of cyber-attacks and digital crimes has also increased. To address this growing concern, the Indian government has taken several initiatives to strengthen the country's cybersecurity and digital forensics capabilities. In 2013, the Indian government launched the National Cyber Security Policy, which aims to create a secure and resilient cyberspace for the country. The policy sets out several objectives, including developing a secure information infrastructure, creating a workforce of cybersecurity professionals, and promoting cybersecurity research and development. In addition to the National Cyber Security Policy, the Indian government has also established several organizations and initiatives to promote digital forensics and cybersecurity in the

country. The Indian Computer Emergency Response Team (CERT-In) is the nodal agency responsible for responding to cybersecurity incidents in the country. The agency works closely with various stakeholders, including government agencies, private companies, and academic institutions, to improve the country's cybersecurity posture.

The Ministry of Electronics and Information Technology (MeitY) is another key player in India's digital forensics and cybersecurity landscape. MeitY is responsible for formulating policies, developing standards, and promoting research and development in the areas of electronics, IT, and cybersecurity. The ministry has established several initiatives, including the Cyber Swachhta Kendra, which aims to provide free tools and services to Indian citizens to protect their digital devices from cyber threats. The private sector in India has also taken steps to improve digital forensics and cybersecurity in the country. Several cybersecurity companies have established a presence in India, offering a range of services, including threat intelligence, vulnerability assessment, and incident response. The government has also encouraged the growth of the cybersecurity industry by providing incentives for startups and creating a cybersecurity entrepreneurship program. Despite these initiatives, India still faces several challenges in the area of digital forensics and cybersecurity. One of the main challenges is the shortage of skilled professionals in these fields. India has a large pool of IT professionals, but there is a lack of specialized skills in areas such as digital forensics and cybersecurity. This shortage of skilled professionals is a major impediment to the growth of these fields in the country. Another challenge is the lack of awareness among the general public about digital forensics and cybersecurity. Many individuals and organizations in India are not aware of the risks of cyber threats and the importance of cybersecurity. This lack of awareness makes them vulnerable to cyber-attacks and digital crimes.

LAWS RELATING TO DIGITAL FORENSICS IN INDIA

India has several laws and regulations in place to govern digital forensics and cybersecurity. Digital forensics and cybersecurity are crucial for protecting the digital assets of individuals, organizations, and governments. India has a comprehensive legal framework for digital forensics and cybersecurity, which provides a basis for preventing and addressing cybercrimes, protecting personal data, and ensuring cybersecurity in various sectors. In this article, we will discuss the laws and regulations related to digital forensics and cybersecurity in India, along with their sections and provisions:

Information Technology Act, 2000 (IT Act): The IT Act is the primary law that governs cybersecurity and digital forensics in India. It provides for legal recognition of electronic documents, digital signatures, and electronic transactions. It also defines various offenses related to the misuse of computers and networks, such as hacking, unauthorized access, and data theft. The IT Act also establishes the Cyber Appellate Tribunal and Cyber Regulations Advisory Committee to oversee and regulate cybersecurity issues.

Section 43: Unauthorized access to computer systems or data: - This section deals with unauthorized access to computer systems or data. It defines unauthorized access as accessing a computer resource without the permission of the owner or the person in charge of the computer resource. The offense is punishable with imprisonment for up to three years, a fine of up to five lakh rupees, or both.

Section 43A: Compensation for failure to protect data: - This section deals with the compensation for failure to protect data. It states that a person who is negligent in implementing and maintaining reasonable security practices and procedures to protect sensitive personal data shall be liable to pay compensation to the affected person. The compensation shall be paid for any wrongful loss or wrongful gain caused by such negligence.

Section 66: Hacking: - This section deals with hacking, which is defined as unauthorized access to a computer system. It covers offenses such as hacking with the intent to cause damage, hacking with the intent to steal information, and hacking with the intent to threaten national security. The offense is punishable with imprisonment for up to three years, a fine of up to two lakh rupees, or both.

Section 66A: Sending offensive messages through communication services: - This section deals with the sending of offensive messages through communication services such as email, social media, or instant messaging. It covers messages that are grossly offensive, menacing, or false and intended to cause annoyance, inconvenience, danger, or insult. The offense is punishable with imprisonment for up to three years and a fine.

Section 66B: Dishonestly receiving stolen computer resources or communication devices: - This section deals with the dishonest receipt of stolen computer resources or communication devices. It covers offenses such as receiving stolen passwords, access codes, or

communication devices with the intent to use them dishonestly. The offense is punishable with imprisonment for up to three years, a fine of up to one lakh rupees, or both.

Section 66C: Identity theft: - This section deals with identity theft, which is defined as the dishonest use of another person's identity to deceive or defraud someone. It covers offenses such as impersonation, identity fraud, and the use of false identities on social media or email. The offense is punishable with imprisonment for up to three years, a fine of up to one lakh rupees, or both.

Section 66D: Cheating by personation by using computer resources: - This section deals with cheating by personation by using computer resources. It covers offenses such as using a false identity or pretending to be someone else on the internet or social media to deceive or defraud someone. The offense is punishable with imprisonment for up to three years, a fine of up to one lakh rupees, or both.

Section 66E: Violation of privacy: - This section deals with the violation of privacy, which is defined as the capturing, publishing, or transmitting of images of the private parts of a person without their consent. The offense is punishable with imprisonment for up to three years.

Indian Penal Code, 1860 (IPC): The IPC is the criminal law that deals with cybercrimes in India. Section 66 of the IPC deals with computer-related offenses such as hacking, unauthorized access, and damage to computer systems.

The Indian Evidence Act, 1872: The Indian Evidence Act provides rules for the admissibility of digital evidence in court. It defines electronic records and outlines the procedures for their admission as evidence in legal proceedings.

National Cyber Security Policy, 2013: The National Cyber Security Policy outlines India's strategy for protecting cyberspace from threats and attacks. It establishes a framework for information sharing, capacity building, and coordination among various stakeholders in the cybersecurity ecosystem.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: These rules require organizations to implement reasonable security practices and procedures to protect sensitive personal data. They also mandate data breach reporting requirements and penalties for non-compliance.

Reserve Bank of India Guidelines: The Reserve Bank of India (RBI) has issued guidelines for cybersecurity in the banking sector. These guidelines require banks to establish cybersecurity policies and procedures, conduct regular security audits, and report cyber incidents promptly.

Aadhaar Act, 2016: The Aadhaar Act establishes a framework for the unique identification of individuals in India. It also provides for the security and confidentiality of the Aadhaar database, which contains sensitive personal information.

The Indian Computer Emergency Response Team (CERT-In): This is the nodal agency for cyber security in India. It is responsible for responding to cyber incidents, issuing alerts and advisories, and promoting research and development in the field of cyber security.

Thus, India has a comprehensive legal framework for digital forensics and cybersecurity. These laws and regulations provide a basis for preventing and addressing cybercrimes, protecting personal data, and ensuring cybersecurity in various sectors. It is essential for organizations and individuals to comply with these laws to safeguard themselves against cyber threats and potential legal repercussions.

LEADING CASES RELATING TO DIGITAL FORENSICS

There have been several important cases relating to digital forensics in India in recent years. These cases have helped to establish legal precedents and provide guidance on how digital evidence can be used in criminal investigations and court proceedings. In this essay, we will discuss some of the leading cases relating to digital forensics in India.

State of Tamil Nadu v. Suhas Katti (2010): - This case involved the recovery of deleted emails from a computer used by the accused in a fraud case. The emails had been deleted from the computer but were recovered by digital forensics experts using specialized software. The trial court accepted the digital evidence, and the accused was convicted based on the recovered emails. On appeal, the High Court of Madras upheld the trial court's decision, holding that the digital evidence was admissible and reliable. This case established the principle that digital evidence can be admissible in court, even if it has been deleted or tampered with. It also highlighted the importance of using specialized software and techniques to recover digital evidence in a forensically sound manner.

State (NCT of Delhi) v. Navjot Sandhu (2005): - This case, also known as the "Parliament Attack Case," involved a terrorist attack on the Indian Parliament in 2001. The accused were charged with various offenses, including terrorism and conspiracy to wage war against the state. Digital evidence played a key role in the prosecution's case, as several accused had communicated with each other through email and instant messaging. The trial court accepted the digital evidence, and the accused were convicted and sentenced to death. On appeal, the Supreme Court of India upheld the convictions, holding that the digital evidence was admissible and had been properly authenticated. This case was significant because it demonstrated the importance of digital evidence in prosecuting complex cases involving terrorism and other serious offenses. It also established the principle that digital evidence can be admissible in court, as long as it is properly authenticated and meets other evidentiary requirements.

Shreya Singhal v. Union of India (2015): - This case involved a constitutional challenge to Section 66A of the Information Technology Act, which criminalized the sending of "offensive" messages through electronic communication. The petitioner argued that the provision was vague and overbroad, and violated the right to free speech guaranteed by the Indian Constitution. The Supreme Court of India struck down Section 66A, holding that it was unconstitutional and violated the right to free speech. The court noted that the provision was so broad that it could be used to criminalize legitimate speech and expression and that it had a chilling effect on online discourse. This case was significant because it highlighted the importance of protecting free speech and expression online and the need for clear and narrowly tailored laws relating to cybercrime and digital communication.

Anvar P.V. v. P.K. Basheer (2014): - This case involved the admissibility of electronic records as evidence in court. The petitioner argued that electronic records, such as emails and computer printouts, should be admissible only if they are accompanied by a certificate under Section 65B(4) of the Indian Evidence Act, which requires the person producing the electronic record to certify that it was produced by a computer and that it was in proper working order at the time of production. The Supreme Court of India held that electronic records can be admissible in court even if they are not accompanied by a Section 65B(4) certificate, as long as the authenticity and reliability of the record can be established through other means. The court noted that the requirement for a Section 65B(4) certificate should not

be used as a technical hurdle to exclude relevant and reliable evidence. This case was significant because it clarified the admissibility.

State of Tamil Nadu vs Nalini: - The assassination of Rajiv Gandhi, the former Prime Minister of India, in 1991 was one of the most significant events in Indian political history. Nalini was one of the conspirators involved in the assassination, and she was charged under the Indian Penal Code (IPC) and the Terrorist and Disruptive Activities (Prevention) Act (TADA). The prosecution presented digital evidence in the form of emails, floppy disks, and CDs to support their case. The digital evidence was crucial in establishing the link between the accused and the conspirators. The case was ultimately decided by the Supreme Court of India, which sentenced Nalini to life imprisonment.

State vs Gopal Krishna Raju: - Gopal Krishna Raju was the managing director of Satyam Computer Services, one of the largest IT companies in India. In 2009, Raju confessed to a massive financial fraud, which involved inflating the company's earnings by more than $1 billion. The fraud was uncovered through a digital forensics investigation, which revealed that the company had created fake invoices and manipulated its accounting records. The investigation was carried out by the Central Bureau of Investigation (CBI) and led to the arrest of Raju and several other top executives of the company. The case is still ongoing, and Raju is currently out on bail.

Shakti Vahini vs Union of India: - In 2018, the Supreme Court of India ruled on a case involving the use of digital forensics evidence in human trafficking cases. The case was filed by an NGO called Shakti Vahini, which sought to establish guidelines for the collection, preservation, and presentation of digital evidence in such cases. The court issued a set of guidelines, which included the appointment of a forensics expert to collect and preserve digital evidence, the use of digital signatures to ensure authenticity, and the establishment of a chain of custody to ensure the integrity of the evidence.

State vs Ravi Kapoor: - Ravi Kapoor was one of the accused in the 2006 Mumbai train bombings, which killed over 200 people and injured more than 700 others. The prosecution relied heavily on digital evidence in the form of emails, phone records, and chat transcripts to establish the link between the accused and the bombing. The digital evidence was crucial in establishing the identity of the accused and their role in the bombing. Kapoor was convicted and sentenced to life imprisonment.

State vs Ajmal Kasab: - The 2008 Mumbai terror attacks were one of the deadliest terrorist attacks in Indian history. Ajmal Kasab was one of the terrorists involved in the attacks, and he was captured alive by the police. The prosecution presented a vast amount of digital evidence in the form of CCTV footage, phone records, and GPS data to establish the link between Kasab and the attacks. The digital evidence was crucial in establishing the identity of the accused and their role in the attacks. Kasab was convicted and sentenced to death, which was later upheld by the Supreme Court of India.

The Airtel-Spying Case: - In 2010, a hacker group called LulzSec claimed to have hacked into the servers of Indian telecommunications company Airtel. The group released confidential information about Airtel's customers on the Internet. Airtel filed a complaint with the Cyber Crime Division of the Delhi Police, and the police arrested the alleged hackers. The case highlights the importance of protecting sensitive information and the need for robust cyber security measures.

The Niira Radia Tapes: - In 2010, transcripts of phone conversations between lobbyist Niira Radia and various politicians, journalists, and corporate executives were leaked to the media. The conversations revealed unethical and illegal practices in the telecom industry and led to a national scandal. The case highlights the need for digital forensics investigations to uncover evidence of cybercrime.

The Pegasus Spyware Case: - In 2021, a global investigation revealed that Israeli spyware Pegasus was being used to target journalists, activists, and politicians in several countries, including India. The Indian government denied any involvement in the use of the spyware but ordered an investigation into the matter. The case highlights the need for robust cybersecurity measures to prevent the misuse of surveillance technology.

The Noida Double Murder Case: - In 2008, a teenage girl and her family's domestic servant were found murdered in Noida. The case gained national attention, and the police used digital forensics techniques to gather evidence. The police used cell tower location data and call records to track the suspects and eventually solve the case. The case highlights the importance of digital forensics investigations in solving complex crimes.

The Uber Data Breach Case: - In 2016, ride-hailing company Uber suffered a data breach that affected millions of its customers and drivers worldwide. The breach was not reported until a year later, leading to a backlash from customers and regulators. The case highlights

the need for timely reporting of data breaches and the importance of data protection regulations.

The Aadhaar Data Leak Case: - In 2018, a journalist reported that the personal data of over a billion Indian citizens enrolled in the Aadhaar program was available for sale on the Internet. The case led to calls for better data protection regulations and the need for robust cyber security measures to prevent data breaches.

Thus, digital forensics investigations have become increasingly important in India, and they have played a crucial role in several high-profile cases. The courts have recognized the importance of digital evidence in establishing the identity of the accused and their role in the crime. With the increasing use of technology in all aspects of life, the need for effective digital forensics investigations is likely to continue to grow.

RECENT DEVELOPMENT

Digital forensics and cybersecurity have become increasingly critical in India due to the rapid growth of technology and the increase in cybercrime incidents. In this article, we will discuss recent developments in digital forensics and cybersecurity in India.

The National Cyber Security Strategy 2020: - In 2020, the Indian government released the National Cyber Security Strategy, which aims to create a secure and resilient cyberspace in the country. The strategy includes initiatives such as creating a National Cyber Crime Reporting Portal, establishing a National Cyber Coordination Centre, and strengthening the cybersecurity workforce through training and capacity building.

The Personal Data Protection Bill, 2019: - The Personal Data Protection Bill, 2019 is currently under review by the Indian government. The bill aims to protect the personal data of individuals and create a regulatory framework for the collection, storage, and processing of personal data. The bill includes provisions for data protection, consent, and penalties for violations.

The Cyber Crime Prevention Against Women and Children (CCPWC) portal: - In 2020, the Indian government launched the CCPWC portal to address cybercrimes against women and children. The portal provides a platform for reporting cybercrime incidents and offers

support to victims. It also includes a database of offenders and a mechanism for tracking and monitoring cybercrime cases.

The Cyber Swachhta Kendra: - The Cyber Swachhta Kendra is a government initiative launched in 2017 to provide cybersecurity solutions to individuals and organizations. The platform offers free tools such as antivirus software, bot removal tools, and malware analysis tools to help protect against cyber attacks.

The Cyber Forensics Laboratory: - In 2020, the Indian government announced the establishment of a Cyber Forensics Laboratory in Hyderabad. The laboratory will be responsible for conducting digital forensics investigations and providing technical assistance to law enforcement agencies. The laboratory will also offer training and capacity-building programs for digital forensics experts.

The Cyber Coordination Centre: - In 2017, the Indian government established the Cyber Coordination Centre (CCC) to strengthen the cybersecurity infrastructure in the country. The CCC is responsible for collecting, analyzing, and disseminating information on cyber threats and incidents to relevant stakeholders. The center also provides technical support and expertise to law enforcement agencies for cybercrime investigations.

The Cyber Swachhta Kendra Botnet Cleaning and Malware Analysis Centre: - In 2018, the Indian government launched the Cyber Swachhta Kendra Botnet Cleaning and Malware Analysis Centre. The center is responsible for identifying and cleaning infected systems, preventing botnet attacks, and analyzing malware samples.

The Cyber Surakshit Bharat Initiative: - The Cyber Surakshit Bharat Initiative was launched in 2018 to raise awareness about cybersecurity among citizens and organizations. The initiative includes a series of workshops and training programs for students, teachers, and professionals to help them stay safe online.

Digital forensics and cybersecurity are critical areas for India's overall security and development. Recent developments in these fields demonstrate the government's commitment to creating a secure and resilient cyberspace in the country. However, there is still a need for continuous efforts to stay ahead of cyber threats and protect citizens and organizations from cyber attacks.

CONCLUSION

In conclusion, the emerging world of metaverse and artificial intelligence presents both opportunities and challenges in the areas of digital forensics and cyber security. With the increasing use of these technologies, it becomes imperative to ensure the security and protection of data, systems, and networks from cyber threats and attacks. In the context of the Indian legal system, there is a need to develop appropriate laws and regulations to address cybercrime and ensure effective enforcement of these laws. The government and law enforcement agencies must also invest in the necessary resources and infrastructure to strengthen cyber security and forensics capabilities. Moreover, it is crucial to promote awareness and education among individuals and organizations about the importance of cyber security and the potential risks and consequences of cybercrime. The development of a skilled workforce in digital forensics and cyber security is also necessary to address the growing demand for such expertise in the industry. As the world continues to advance technologically, the need for robust digital forensics and cyber security measures will become increasingly important in ensuring a safe and secure digital environment for all.

REFERENCES

The following sources were used to write the above article.

1. **Books and Acts Referred**
   - The Constitution of India
   - The Information Technology Act, 2000
   - The Personal Data Protection Bill, 2018
   - The General Data Protection Regulation, 2016
   - The India Penal Code, 1860
   - The Code of Criminal Procedure, 1973
   - The Indian Evidence Act, 1872
   - The National Cyber Security Policy, 2013
   - The Cyber Appellate Tribunal (Procedure) Rules, 2000
   - The Digital Signature Certificate (DSC) Guidelines, 2015
   - Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
   - Reserve Bank of India Guidelines
   - Aadhaar Act, 2016
2. **Articles on Websites Referred**
   - http://www.cyberlawcollege.com
   - https://www.cyberlawtimes.com
   - https://ncfta.net
   - https://www.dsci.in
   - http://www.cspf.co.in
   - https://www.ccci.ac.in
   - http://www.csrc.in
   - https://www.cert-in.org.in
   - https://cybercrime.gov.in
   - https://nccc.gov.in
   - https://www.legalserviceindia.com
   - https://protenus.com
   - https://criminal.findlaw.com

- https://www.privacyend.com
- https://www.nexusguard.com
- https://www.information-management.com
- https://www.symantec.com
- https://www.forbes.com
- http://www.prnewswire.com
- https://www.juniperresearch.com
- https://www.businesstoday.in
- https://indianexpress.com
- https://www.testbytes.net
- https://economictimes.indiatimes.com
- https://secludit.com
- https://academic.oup.com
- http://www.libraryoflaw.com/
- https://www.researchgate.net
- https://nludelhi.ac.in
- https://www.prnewswire.com