UNCOVERING THE LEGAL CHALLENGES OF CYBERCRIME IN INDIA AND THE NEED FOR A SPECIFIC LEGAL FRAMEWORK

Abeer Rakesh Wasnik*

ABSTRACT

Cybercrime has emerged as a significant global threat, impacting economies, governments, and individuals alike. This research paper aims to uncover the legal challenges associated with cybercrime in India and emphasizes the urgent need for a specific legal framework to effectively combat this growing menace. The paper begins by providing an overview of the escalating rates of cybercrime incidents in India, highlighting the detrimental consequences on the economy, national security, and public trust. It then delves into the current legal landscape, revealing the inadequacies and gaps within the existing legislation. Through an in-depth analysis of the legal challenges faced, this paper explores the complexities surrounding jurisdictional issues, the absence of standardized definitions, procedural hurdles, and the lack of coordination among law enforcement agencies. These challenges not only hinder the successful investigation and prosecution of cybercriminals but also undermine the overall deterrence against cybercrimes. Recognizing the need for a comprehensive legal framework, this research paper proposes key elements that should be incorporated into the legislation to address the specific challenges of cybercrime in India.

INTRODUCTION

Cybercrime is any criminal activity that targets or makes use of a computer, a computer network, or a device that is connected to a network. Cybercriminals or hackers who are motivated by financial gain carry out the majority, if not all, of cybercrime. Cybercrime can be committed by individuals or businesses. Some cybercriminals are well-organized, proficient technically, and use cutting-edge methods. Some are inexperienced hackers. Once in a while, cybercrime means to harm PCs because of reasons other than benefits. These could be political or individual. Cybercrime is a dangerous type of crime that involves digital devices or computers. In this type of crime, a computer can be the target of the crime, a tool of the crime, or contain evidence of the crime. The term "cybercrime" basically refers to any illegal activity that takes place online. There are numerous examples, including identity theft,

*BBA LLB, FIRST YEAR, MAHARASHTRA NATIONAL LAW UNIVERSITY, NAGPUR.

cyberstalking, malware-like viruses, and fraud. Control, prevention, and investigation of cyber activities are crucial to the success of organizations, government agencies, and individuals in today's environment because the majority of information processing relies on information technology. It is impossible to overstate the importance of government and business organizations acquiring and maintaining highly skilled cybercrime experts. Prior, cybercrime was perpetrated principally by people or little gatherings. By and by, it is seen that there are profoundly intricate cybercriminal networks that unite people at a worldwide level continuously to carry out violations. In today's world, cybercriminals are not driven by ego or expertise. Instead, they want to make quick money by using their knowledge. They are making use of their ability to snip, deceive, and exploit people because it is simple for them to make money without having to work hard. Today, cybercrime poses a significant threat.[1]

CYBERCRIME IN INDIA: A FEW CASES STUDIES

a) The Bank NSP Case

In this situation, a bank the executives' student got hitched. Previously, the couple exchanged numerous emails using the company's computers. After separating for some time, the woman created fake email addresses, such as "Indian bar affiliations," and sent messages to the child's unknown clients. She did this by using the PC in the bank. After losing many customers, the boy's company filed a lawsuit against the bank. Emails that were sent through the bank's system were held accountable.

b) The Bazee.com case

The Chief Executive Officer of Bazee.com was arrested in December 2004 for selling a CD with offensive material on the website. The CD was also sold out in the Delhi market. The CEO was eventually released on bail after the Delhi and Mumbai police took action.

c) The Parliament Attack Case

This case was handled by the Bureau of Police Research and Development in Hyderabad. The terrorist who attacked the Parliament was found with a laptop. The BPRD's Computer Forensics Division received the laptop that was taken from the two terrorists who were killed by gunfire on December 13, 2001, while the Parliament was under siege. The fake ID card

[1]Ahmad showkat and Naseer Ahmad Lone, 'CYBER CRIME IN INDIA' [2022] <www.researchgate.net/publication/357839318_CYBER_CRIME_IN_INDIA> accessed 20 May 2023.

that one of the two terrorists was carrying with a Government of India emblem and seal and the sticker of the Ministry of Home that they had created on the laptop and affixed to their ambassador car to gain entry into Parliament House were two of the numerous proofs that affirmed the motives of the two terrorists. The three lion emblems were meticulously examined, and the seal was also carefully crafted with a Jammu and Kashmir residential address. Anyway, cautious identification demonstrated that it was totally fashioned and made on the PC.

d) Andhra Pradesh tax case

The owner of a plastics company was detained and given Rs. The Vigilance Department took 22 from his house. They required him to provide evidence regarding the unaccounted cash. The thought individual submitted 6,000 vouchers to demonstrate the authenticity of the exchange, but when cautious investigation of the vouchers and items in his PCs it was unconcealed that all of them were made after the attacks were led. It was kept a secret that the suspect was operating five businesses under the guise of one and using fake and computerized vouchers to hide sales records and avoid paying taxes. As a result, the state businessman's dubious methods were exposed when department officials obtained access to the suspect's computers.[2]

CYBERCRIMES AND DIFFERENT KINDS OF CYBER OFFENCES UNDER INDIAN LAW:

There are two extraordinary highlights of the Web. First of all, a cybercriminal can commit a crime from anywhere in the world because it does not have a specific geographical limit. The second thing that sets it apart is that it gives its users anonymity, which has both advantages and disadvantages. For individuals who utilize this namelessness for putting out their perspective to the world as an aid yet the culprits utilize this obscurity for the commission of wrongdoing it is a plague. As a result, not only do these features make it difficult to enforce the law but also to prevent crime. At present there is no particular regulation that arrangements with digital wrongdoing against ladies. Different regulations can be utilized in the particular case, most ladies don't know about. Women are unaware of their rights or that they exist.

[2]'A brief study on Cyber Crime and Cyber Laws of India' (2017) 04(06) International Research Journal of Engineering and Technology (IRJET) 2395 -0056, <https://southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf> accessed 17 May 2023.

There are numerous regulations in sculptures and guidelines which punishes digital wrongdoing. However, the Information Technology Act (IT Act) of 2000 and the Indian Penal Code (IPC) comprise the majority of the laws. The Indian Penal Code (IPC) is the country's general criminal code that defines offenses and specifies their associated penalties. IPC covers regulations and discipline relating to the actual world and has been officially changed and wisely deciphered to be appropriate for digital crooks. Though the IT Act is a particular code relating to the utilization of data innovation and wrongdoing perpetrated through it.[3]

(a) Cyber-squatting

It occurs whenever someone uses the internet improperly. Usually, to do this, a domain name that looks to be similar to a well-known or well-liked name of a domain, entity, or brand is used. Squatter refers to the perpetrator, while squatted name refers to the name that is used by the offender. By taking advantage of a first mover advantage, the squatter is able to effectively register the domain name that they have illegally taken. The squatter then demands payment from the owner of the well-known brand in return for the domain that was formerly his or hers, and if the owner declines to do so, the squatter then has the legal right to prevent the owner from using those names. This kind of activity interferes with Intellectual Property Rights and in India it interferes with the "Uniform Domain Name Dispute Resolution Policy".

(b) Cyber-terrorism

Barry Collin, a Research Fellow at the California Institute for Security and Intelligence, used the phrase "cyber terrorism" first. He defines cyberterrorism as the fusion of cybernetics with terrorism. When multiple messages concerning the Kashmir conflict were aired on various well-known websites in the nation in 2002, it was believed that Pakistani hackers operating under the direction of one Doctor Naikar were to blame. This was India's first encounter with cyberterrorism strikes. In April 2010 the CBI website was also hacked by Pakistan Cyber Arm.

[3]Rani Supriya and others, 'CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS' (2022) 7(6) International Journal of Mechanical Engineering <https://kalaharijournals.com/resources/JUNE-37.pdf> accessed 19 May 2023.

(c) Data Theft

It happens when someone unlawfully buys or steals material that is forbidden from being made available to the public and is of a confidential nature. Sections 43, 43A, and 66 of the IT Act of 2000 govern the punishment for such violations. The crime is covered by Section 43, and the punishment measures are covered by Sections 43A and 66. In Syed Assifuddin and Others v. The State of Andhra Pradesh and Others, Section 66 was also used.

(d) Hacking

It is a lot more serious infraction, and it is also one of those that is quite simple to do. Generally speaking, hacking refers to any unauthorised use of a computer or electronic equipment, data, or any other type of data accessing or sharing equipment, apps, etc. Because hacking is such a broad area of crime, using someone else's email address without their consent may fall under this category if the owner of that email address accidentally left it in log-in mode on a device. The most often rising offences in India are those involving hacking. The websites of the Ministry of Defence, Jadavpur University, and several other significant websites have all experienced periodic hacking. Under Section 66(2) of the IT Act, hacking has been treated as a crime.

(e) Web-Jacking

When someone unlawfully and violently seizes control of a website from its legitimate owner by cracking the password, they then start changing the information on the website. The genuine owner of the website loses all control over it as a result of such an unlawful take of custody. Such acts are dealt with under Section 65 of the IT Act, 2000, according to Indian law.

(f) Cyber Bullying

Threatening or frightening someone is typically considered bullying. Cyberbullying occurs when such threats or intimidation are made via digital means. Commonly referred to as frequent and intentional harm caused by the use of computers, mobile phones, and other electronic devices, cyberbullying is a problem today. According to Microsoft's 2011 Global Youth Online Behaviour Survey, 53% of children worldwide have experienced cyberbullying at least once during the course of their online presence. India came in third place, behind

China and Singapore, in terms of this type of bullying. Cyberbullying is not officially defined by Indian law; however, it is possible to prosecute such actions under Section 66 of the IT Act of 2000 and its criminal penalties.

(g) Cyber Stalking

Online stalking is the root cause of cyberstalking. This kind of behavior is referred to as "stalking" in the broadest sense by the Indian Penal Code, and it is against the law when a person is constantly being watched by another person. Cyberstalking is carried out using online platforms. It might not appear to be all that bad for any one person in particular, but it might violate the right to privacy, which is now recognized as a fundamental right under Article 21 of the Indian Constitution.

However, the 2013 Criminal Law (Amendment) Act makes internet stalking a criminal offence punishable under Section 354D of the IPC, despite the fact that the Section is gender-specific and only protects female victims against male perpetrators. Despite the fact that there are no specific provisions in Indian law for the handling of cyberstalking, Section 72 of the IT Act can be used as a reference because it addresses violations of confidentiality and privacy. Consequently, reference to Segment 72 of the IT Act turns out to be more significant despite the fact that it isn't explicitly managing digital following for which there could emerge troubles in deciphering this sort of offense from an unbiased viewpoint.[4]

THE NEED FOR A SPECIFIC LEGAL FRAMEWORK

Observing the above analysis, the need for a specific legal framework for cybercrime in India stems from the unique challenges and risks posed by the digital landscape. As technology advances and more aspects of our lives become intertwined with the online realm, the potential for cyber threats and criminal activities grows exponentially. Therefore, it becomes essential to establish comprehensive laws and regulations to effectively combat cybercrime.[5]

The unique nature of cybercrime necessitates a dedicated legal framework. Unlike traditional forms of crime, cybercrime knows no geographical boundaries, making it difficult to trace and prosecute offenders. The intangible nature of digital data and the anonymity provided by

[4]Jayanta Boruah, 'Cyber Crimes and Its Legal Challenges in India' (2021) 2(1) The Journal of Legal Methodology Policy and Governance <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3819497> accessed 19 May 2023.
[5]Nir Kshetri, 'Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future' [2016] <https://doi.org/10.1007/s10611-016-9629-3> accessed 18 May 2023.

the internet create an environment that requires specialized legal provisions to investigate and prosecute cybercriminals effectively. A specific legal framework for cybercrime is crucial for protecting personal and sensitive data. With the increasing reliance on e-commerce, online banking, and digital transactions, individuals and organizations store vast amounts of personal information online. A robust legal framework helps safeguard this data from unauthorized access, theft, or misuse. It establishes guidelines for data privacy, security, and breach notification, ensuring the confidentiality and integrity of personal information.

The need for a specific legal framework arises from the importance of safeguarding national security. Cyber threats can pose significant risks to a nation's security, including espionage, sabotage, and attacks on critical infrastructure. A dedicated legal framework enables the government and law enforcement agencies to address these threats effectively. It establishes preventive measures, response protocols, and mechanisms for information sharing and cooperation between various stakeholders. Such a framework ensures that the country is prepared to handle cyber incidents that may jeopardize national security.

A specific legal framework enhances law enforcement capabilities in dealing with cybercrime. Cybercrime investigations require specialized skills, tools, and techniques. A well-defined legal framework empowers law enforcement agencies by providing legal powers, procedures, and provisions for collecting evidence, investigating cyber incidents, and prosecuting offenders. It also enables international cooperation in fighting cybercrime by establishing mechanisms for extradition and mutual legal assistance. Thus, a specific legal framework for cybercrime in India is necessary to address the evolving challenges posed by the digital landscape. It ensures the protection of personal and sensitive data, safeguards national security, enhances law enforcement capabilities, and fosters international cooperation. By establishing comprehensive laws and regulations, India can effectively combat cyber threats and provide a secure digital environment for its citizens and organizations.

CONCLUSION

This research paper has highlighted the legal challenges posed by cybercrime in India and emphasized the urgent need for a specific legal framework to address them. The unique nature of cybercrime, its potential risks to personal data and national security, and the specialized skills required for investigation and prosecution all underscore the importance of

a comprehensive legal framework. Such a framework will protect personal information, ensure national security, empower law enforcement agencies, and promote international cooperation. By addressing the legal challenges of cybercrime, India can effectively combat cyber threats and create a safer digital environment for its citizens and organizations. It is imperative that policymakers, legislators, and stakeholders work together to establish and implement a robust legal framework to mitigate the growing menace of cybercrime in India.