International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Effectiveness of India's Cybercrime Investigation and Prosecution Framework in Dealing with Cybercrime Cases.

Rachi Rajesh Chavan

Student, Amity University Mumbai

ABSTRACT

Cybercrime primarily consists of actions that use the internet and computers as tools to obtain private information about a person, either directly or indirectly, and to disclose that information on online platforms without that person's consent or in violation of the law with the intention of damaging that person's reputation or causing them mental or physical harm. "Nowadays, a guy may complete all of his needs online, including his educational needs, employment needs, shopping needs, and money needs. A variety of cybercrimes have evolved with the expansion of the internet. This is mostly due to the fact that more than half of internet users have just a basic understanding of how online platforms operate, are uninformed of technical changes, and lack proper training and education. India is one of the few nations that has passed the IT Act 2000 to address issues relating to cybercrimes in order to protect its citizens from being exploited by vicious predators, but this act ignores some of the most serious threats to women's security, and issues involving women are still expanding significantly.

INTRODUCTION

Cybercrimes are defined as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause the victim physical or mental harm, or loss, directly or indirectly, using modern telecommunication networks such as the Internet networks including chat rooms, emails, notice boards and groups and mobile phones."

Cybercrime includes both online and computer activity. The right to privacy is jeopardised when someone's personal information is disclosed or published online with the purpose of physically or mentally harming them.

Whereas "Cyber law" can be defined as the legal concerns associated with the use of communications technology, namely "cyberspace," which is the Internet. An effort is being made to incorporate the difficulties posed by human activity on the Internet with the established legal framework that governs the physical world. To prevent internet-related criminal activity The Information Technology Act of 2000 was passed primarily with the intention of fostering a business-friendly environment for I.T. The acts that have been rendered criminal are listed in the IT Act. Additionally, cybercrimes are now covered by the Indian Penal Code, 1860.

BACKGROUND

The history of cybercrime in India may be traced to the country's development of the internet and digital technologies. An overview of the growth of cybercrime in India is shown below:

1. **Initial occurrences (1990s):**
   India had its first cybercrimes in the early 1990s, which were frequently connected to hacking and unauthorised access to computer systems. Cybercrime was still in its infancy during this time, and the majority of instances were tech-savvy individuals looking for weaknesses on the internet.
2. **2000 Information Technology Act:**
   India's attempts to prevent cybercrime reached a key turning point with the passage of the Information Technology Act, 2000. It added procedures to deal with cybercrimes and gave legal validity to electronic documents and digital signatures. The Act includes sections that dealt with hacking, unauthorised access, data theft, and the penalties associated with these offences.
3. **Evolving Cyber Threats (2000s):**
   As the internet and digital technology adoption grew in India, cybercrimes became more prevalent and diverse. Financial fraud, identity theft, phishing attacks, and online harassment started to affect individuals and organizations. The emergence of social media platforms and e-commerce sites provided new avenues for cybercriminals.
4. **Amendments to IT Act (2008):**
   In 2008, the IT Act underwent significant amendments to address emerging cyber threats more effectively. These amendments expanded the scope of the Act to include new offenses and increased penalties for cybercrimes. The Act also introduced provisions for the protection of sensitive personal data and mandatory data breach notifications.
5. **High-Profile Cyber Incidents (2010s):**
   India faced several high-profile cyber incidents, including data breaches, hacking of government websites, and financial cybercrimes. These incidents highlighted the need for improved cybersecurity measures and prompted increased government attention to cyber threats.
6. **National Cyber Security Policy (2013):**
   India introduced its National Cyber Security Policy in 2013 to strengthen the country's cybersecurity infrastructure and capabilities. The policy aimed to create a secure cyber ecosystem and promote proactive cybersecurity practices.
7. **Growth of Cybersecurity Ecosystem (2010s):**
   The Indian government established various agencies and organizations dedicated to addressing cyber threats, including the Indian Computer Emergency Response Team (CERT-In).Public and private sector collaborations in cybersecurity research, education, and capacity-building initiatives expanded.
8. **Recent Trends and Challenges (2020s):**
   In recent years, India has faced an increasing number of cyber threats, including ransomware attacks, data breaches, and online scams. The COVID-19 pandemic further accelerated digital transformation, leading to heightened concerns about cybersecurity.
9. **International Cooperation:**
   India actively collaborates with other countries and international organizations to combat cross-border cybercrimes and enhance cybersecurity.

INDIAN CYBER LAW

These are the provisions of the IT Act of 2000.

One of this Act's most crucial provisions, Section 66, deals with offences using computers. Hacking is classified as a crime under Section 66. Another issue, data theft, is addressed in Section 43. According to

this clause, stealing data is an infraction that is punished by up to three years in jail, a fine of 5 lakh rupees, or possibly both if it is done dishonestly or fraudulently.

Section 66 of the ITA, 2000 offences

It will be briefly mentioned later under the Shreya Singhal case how Section 66A was declared illegal in 2015.

Information technology and communication equipment theft crimes are included under Section 66B. A fine of one lakh rupees or up to three years in prison are the possible penalties for this offence.

Under this section, Section 66C—identity theft—was addressed. By using an electronic signature, identity theft is possible. Another definition of identity theft is using someone else's password. A fine of one lakh rupees or a sentence of up to three years in jail, or a combination of the two, may be imposed under this provision.

This section addresses the same issues as Section 66D, which defines impersonation as a type of cheating. If someone uses an electronic communication device or other computer resource improperly and deliberately to cheat, they might face up to three years in prison or a fine of one lakh rupees. Unauthorised publication or transmission of a person's private information is a breach of Section 66E of the Privacy Act, among other things. Three years in jail, a fine of two lakh rupees, or both are the possible penalties.

One of the biggest issues with relation to national security is cyber terrorism, which is covered in Section 66F. The Indian armed forces and other significant government institutions are always at risk from cyberattacks. By using expressions like "Intent to threaten," this section implies the consequences of criminal intent. The nation's unity, integrity, security, or sovereignty are also emphasised in this part, and any unlawful access to them must be forbidden.

Obscene images or materials cannot be published or transmitted electronically in accordance with Section 67. The Information Technology (Amendment) Act of 2008's modifications expanded the application of Section 67. In addition to making child pornography unlawful, this clause also made it illegal for intermediaries to keep records.

The prohibition of posting or distributing sexually explicit information in any electronic form is included in Section 67A. Regarding the penalties under this clause, there is a specific meaning. Only the penalties outlined in this section may be invoked when the provisions of Sections 67 and 67A are combined. Section 67B alone is responsible for dealing with child pornography.

Several laws have been changed as a result of the IT Act. Regarding IPC, the ITA 2000 has made changes to a number of parts to maintain its own relevance without the interference of other laws' supplemental legal requirements. Sections 192, 204, 463, 464, 471, and 476, among others, were altered.

Another law that the ITA modifies is the Indian Evidence Act of 1872. A court could only accept physical evidence up until the year 2000. To deal with 2000 electronic records and papers, which were otherwise challenging due to a lack of legislation before 2000, was made easier with the passage of the ITA.

EFFECTIVENESS OF INDIA'S LEGAL FRAMEWORK AGAINST CYBERCRIME

Cyber laws' efficacy is up for debate. Despite the fact that the government has made an effort to provide an appropriate legal framework, user information might still be violated in cyberspace. In reality, the Parliament made a remarkable effort since it even changed a number of laws to conform to the goals of the IT act. Despite all the unique legislation's advantages, there are still certain murky areas that hinder

India's cyber laws' ability to be effective. A challenge is the lack of significant attempts on shared storage of electronic evidence.

In the event of a dispute, the original device could be returned to its owner, who would still be free to use it as they please. Original evidence could have been converted into electronic pieces of evidence, at which point they could have been stored by a dependable third party who could produce the same information contained in the discs and software. Software from other parties, such as the Indian "C-DAC" and "EnCase," will aid in maintaining the original version and a date stamp. As a result, it won't be necessary to retain written records.

Inadequate coverage of a number of new cyber problems the lack of coverage of many developing categories of cybercrime is one of the main reasons Indian cyber laws are failing. India only has one law, and because of its restricted reach, it still only applies in certain circumstances. As a result, a number of issues continue to fall beyond the Act's purview, allowing for its unprecedented growth. Numerous important cybercrimes, such as spam emails, data breaches, copyright violations, cybersquatting to demand money, and ISP responsibility for them have not yet gotten appropriate attention.

Weak enforcement of cyber laws, Shri Pavan Duggal, a Supreme Court attorney and computer specialist, made a crucial point. Even while lawmakers deserve praise for their admirable efforts to close the gap in cyber laws, the goal of the IT Act will not be achieved unless and until the laws are made more technologically neutral and have a more rigorous application over offences included by its scope. It has been noted that the current legal framework is lenient towards cybercriminals. This implies that such laws will never be successful. It is necessary to adjust the severity of the penalty.

The extraordinarily low rate of cybercrime convictions, the likelihood of conviction is a crucial indicator of the application of any legislation. Numerous laws won't be able to address the issue of poor law enforcement. The success of the cyber laws in India will, however, be demonstrated by a high conviction rate. Currently, India's cyber laws are ineffectual due to a low conviction rate. In order to demonstrate the deterrent impact of the existing legislation, the certainty of punishment is more significant than the harshness of a punishment.

RECENT CYBERATTACK CASES HAVE DRAWN CRITICISM.

2004 saw one of the first instances of a conviction in India under Section 67 of the Information Technology Act, 2000. Defamatory, offensive, and repetitious communications were posted on a Yahoo chat group in the 2004 case State of Tamil Nadu v. Suhas Katti [(2004) Cr. Comp 4680]. The victim experienced emotional strain as a result of persistently bothersome phone calls. Many similar instances of cyberstalking and abuse of women (particularly) have been documented throughout the years.

Through the case of Shreya Singhal v. Union of India (AIR 2015 SC 1523), Section 66A of the IT Act, 2000 received attention in 2015. Under Article 32 of the Indian Constitution, a PIL writ petition was submitted in this matter. Since Section 66A was said to be unlawful, the petition called for its repeal. The crux of the claims is that Section 66A of the ITA, 2000 is broad, nebulous, and unclear, rendering its scope incapable of making decisions based on objective standards. Such a broad reading of this Section makes it susceptible to wanton exploitation.

CONCLUSION

In recent years, many cybercrimes have been perpetrated due to the emergence and spread of newly created technology. Cybercrime now poses serious risks to humanity. A nation's social, cultural, and security

aspects all depend on its ability to combat cybercrime. The IT Act, 2000 was passed by the Indian government to address cybercrimes. The IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 are all further revised by the Act. Cybercrime may begin from anywhere in the globe and spread across national borders via the internet, making it difficult to investigate and prosecute these crimes on both a technological and legal level. To combat cybercrimes, international harmonisation efforts, coordination, and cooperation amongst diverse states are necessary. Our primary goal in producing this essay was to inform the general public about cybercrime. We wish to conclude this essay, "A Brief Study on Cyber Crime and Cyber Laws of India," by emphasising that cybercrimes would never be accepted. If you or someone you know is the victim of a cyberattack, please come forward and file a report at the local police station. The criminals will never cease if they don't receive punished for their actions. While India has made significant strides in addressing cybercrime through legislation, awareness campaigns, and cybersecurity infrastructure, challenges persist, including the need for continued investment in cybersecurity measures, skill development, and international cooperation to tackle the evolving cyber threat landscape.

REFRENCES

1. SSN: 0974-5823 Vol. 7 No. 6 June, 2022 International Journal of Mechanical Engineering CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS
2. P-ISSN: 2395-0072 © 2017, IRJET | Impact Factor value: 5.181 | ISO 9001:2008 Certified Journal | Page 1633 A brief study on Cyber Crime and Cyber Laws of India
3. [ISSN 2581-5369] Volume 4 | Issue 2 2021 INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES
4. Cyber Crime in India: An Overview: www.legalserviceindia.com
5. United Nations Manual on the Prevention and Control of Computer-Related Crime (1994)
6. Rohit K. Gupta, India: An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective (2013)
7. Dr V.K. Saraswat (Member), NITI Aayog Report on Cyber Security
8. Sushma Devi Parmar, Cybersecurity in India: An Evolving Concern for National Security (Central University of Gujarat)