



CYBER CRIME AND CYBER LAWS IN INDIA: AN OVERVIEW

Law

Hublikar Kiran Vasant

Research Scholar in Law, Shri J.J.T. University, Vidyanagari, Chudela Jhunjhunu - 333001, Rajasthan.

ABSTRACT

Cybercrime is any crime that is conducted using technology or a computer as a tool, and India has laws against it. Cybercrime rules ban people from disclosing private information to strangers online. Internet law, or cyber law for short, is the subset of law that regulates issues related to computers and the Internet, such as online transactions, proprietary software, and data privacy. Since the inception of cyber laws in India, the IT Act 2000, which was approved and updated in 2008 to cover a wide range of crimes, has been in force. In this sense, the term "cyber law" refers to all laws and regulations pertaining to the internet. Cyber laws apply to anything that has to do with, is related to, or arises from legal issues or any online behavior by individuals. Cyber law addresses concerns with the distributive, transactional, and communicative functions of network information technology and devices. It encompasses every law, rule, and provision of the Constitution that pertains to networks and computers. The current article examines Indian cyber legislation.

KEYWORDS

Cyber Laws, I.T.Act, Defamation, Trade secrets, procedural etc.

INTRODUCTION

The practice of cybercrime is a relatively new trend in the criminal world. The term "cybercrime" refers to any criminal behavior done on or via a computer, the internet, or any other technology regulated by the "Information Technology Act." Cybercrime is the most typical kind of crime in modern-day India; it always ends badly. Criminals do massive harm to society and the state while maintaining a low profile. Online, technically-savvy criminals commit a wide variety of crimes. Any unlawful conduct that includes the use of a computing device or the internet, whether as a method of commissioning the crime or as the target of the crime, may be considered to fall under the umbrella term known as cybercrime. In spite of the fact that the word "cybercrime" does not have a definition in any act or legislation that has been accepted by the Indian government, it is sometimes construed by Indian courts. The main causes of cybercrime, an inexorable evil, are the abuse of technology and society's growing dependence on it. In order to facilitate user convenience, computer usage and other related technologies are becoming an ever-more-important element of everyday life. This is an infinite and unquantifiable medium. Cyber defamation, cyber terrorism, email spoofing, email bombing, cyber stalking, cyber pornography, and others are just a handful of the cybercrimes that have lately become more prevalent.

Literature Review

Analyzing the Existing Research although cybercrime is increasingly prevalent, very few people really understand how it works or how it may damage organizations of any size or industry. M. Uma and G. Padmavathi argue that it may be difficult to defend information security due to a general lack of awareness about the various assault types, characteristics, and results. Various definitions of "cyber-attack," "cyber-crime," etc. may be found in international literature, but they all have the common purpose of compromising data security. To stay current with technology, cybercriminals are always developing novel methods of launching assaults, reaching more challenging targets, and remaining undetected.

Research Methodology

Finding the research topic, creating a search strategy, choosing papers for review, extracting data from the articles, and then evaluating and synthesizing the data are all parts of the research technique for this article.

Data Analysis

For analysis, data were combined. Finding common themes, patterns, and trends in the literature is a component of data synthesis.

Cyber-Crime Laws In India

When it comes to cyberspace, there are five main sets of rules that must be followed. Countries with sky-high internet penetration rates, such as India, are realizing the growing need of cyber legislation. Strict legislative limits apply to all aspects of the digital environment, including the use of information, software, internet commerce, and

financial operations. By facilitating maximum connectivity and lowering security worries, India's cyber laws have contributed to the development of e-commerce and governance. This has also expanded the scope and effectiveness of digital media, making it usable in a wider range of contexts.

Information Technology Act, 2000

Since it regulates the investigation and prosecution of cybercrimes, the IT Act is an integral element of the Indian legal system as a whole. Here are the required parts:

Section 43:

Those who conduct cybercrimes, such as damaging the computer belonging to the victim without permission, are subject to this section of the IT Act. In the event that a computer is destroyed in such a way without the owner's consent, the owner is entitled to full compensation.

Section 66:

uses Section 43 to refer to any unethical or fraudulent conduct. Three years in jail or Rs. 5 lakh in fines is the highest penalty for such an infraction.

Section 66B:

This section reaffirms the possible 3-year prison sentence for acquiring stolen computers or other communication equipment. Depending on the gravity of the offense, a fine of up to Rs. 1 lakh may be imposed.

Section 66C:

The major focus of this section is on various forms of identity theft, including electronic signatures, password hacking, and stolen credit card use. A violation of this provision is punishable by a fine of one lakh rupees and/or up to three years in prison.

Section 66D:

Here we talk about using a false identity to access computer systems. If convicted, you may face up to three years in prison and a fine of up to Rs. 1 lakh.

Section 66E:

Without the consent of the occupant(s), it is against the law to photograph their dwelling and distribute or publish the resulting material. Fines of up to Rs 2 lakh and/or imprisonment for up to three years are possible outcomes of a guilty verdict.

Section 66F:

Acts of cyber terrorism. A person who commits a serious crime might spend the rest of their life behind bars. The National Stock Exchange & the Bombay Stock Exchange, for instance, were both targeted by an email threat that dared security officials to stop a terrorist assault. Section 66F of the IT Act led to the criminal's arrest.

Section 67:

This involves the electronic publication of sexually explicit content. If convicted, you might spend up to five years in prison and pay up to Rs. 10 lakh in fines. Indian law enacted in 1860. If the IT Act is inadequate to combat certain types of cybercrime, law enforcement may resort to the following sections of the IPC.

Section 292

The sale of pornographic materials was the primary target of this clause, but it has now expanded to cover other cybercrimes. This provision also covers the electronic promotion and distribution of material involving minors engaging in pornographic or sexually explicit acts or exploits. Such offenses carry a two-year jail term and a Rs. 2,000 fine. A second violation carries a five-year jail sentence and a Rs. 5,000 fine.

Section 354C

under this provision, it is considered a cybercrime to take or distribute photos of a woman's privates or engage in other sexual actions with her without her consent. Since it is against the law to watch a woman have sexual relations with another person, this section exclusively addresses voyeurism. The IPC's Section 292 and the IT Act's Section 66E allow prosecution of equivalent conduct without these components. A first crime may result in three years in jail and a second in seven.

Section 354D

This section defines and punishes online and offline stalking. The term "cyber stalking" refers to the unwanted pursuit of a woman via the use of electronic means of communication. A first offense carries a 3-year jail sentence and a fine, while a second offense carries a 5-year sentence and a fine.

Section 379:

Under this provision, the maximum penalty for theft is three years in jail and a fine of up to \$5,000. Theft of computers, data, or electronic equipment is an integral aspect of many cybercrimes, making the IPC Section relevant.

Section 420:

Here we talk about ways to trick someone into giving up their possessions. The provision stipulates a seven-year prison term and a fine for hackers who commit crimes such as creating fictitious websites and engaging in online fraud. Offenses including creating fake websites or stealing passwords for financial gain are addressed in this section of the IPC.

Section 463:

The forgery of electronic records or documents is discussed here. Email spoofing is illegal and may result in a fine and/or imprisonment of up to 7 years under this provision.

Section 465:

In most cases, the penalties for forgery will be laid forth here. Email spoofing and the creation of false documents online are two examples of the kind of crimes that might result in prison time, fines, or both under this law. Anil Kumar Srivastava v. Addl Director, MHFW's petitioner falsified the AD's signature and filed a false complaint against the same person. The petitioner was held guilty under Indian Penal Code Sections 465 and 471 for trying to pass it off as official.

Section 468:

The maximum penalty for committing fraud having the intent to deceive is seven years in prison and a fine of \$250,000. This clause also prohibits email faking. Several other sections of the Indian Penal Code and the IT Act also address cybercrimes and are relevant to the discussion here.

Information Technology Rules

The IT Rules govern the following aspects:-

Information Technology and Personal Data Protection Rules (Reasonable Security Practices and Procedures) from 2011: Organizations that store personally identifiable information about persons are required to follow particular security procedures under these guidelines. The Digital Media Intermediaries Guidelines and Code of Ethics, 2021: These laws regulate intermediaries, particularly social media intermediaries, to prevent hazardous material from spreading users' data. **Companies Act, 2013**

The Companies Act of 2013 is widely regarded as the primary statutory

requirement for the efficient administration of day-to-day corporate activities. This Act establishes the mandatory techno-legal norms, making it difficult for corporations to avoid complying with the law. The SFIO has been given authority under the Companies Act 2013 (Act) to look into and prosecute large-scale frauds perpetrated by Indian organizations and their directors. Following the 2014 Companies Evaluation, Investment, and Inquiry Rules' implementation, the SFIOs are tackling this problem seriously and leading the way. The legislation made sure that all compliance with regulations are correctly handled, ensuring that cybersecurity diligence, e-discovery, and cyber forensics are properly addressed.

CONCLUSION

In order to control online behavior and safeguard individual privacy, India needs strong cyber laws. The Information Technology Act of 2000 and other similar laws form the basis of these regulations, which address a wide range of cybercrimes and related consequences. In addition to covering unauthorized access, hacking, data theft, online fraud, and cyber terrorism, it also covers many other related concerns. Cybercrime investigation units and cyber appeals courts may be established with less difficulty according to the Act. One of the most important steps taken by the Indian government lately to strengthen cybersecurity is the enactment of the Personal Data Protection Bill. Protecting individuals' privacy, promoting safe online transactions, and thwarting potential cyberattacks are all goals of the legislation enacted in this area.

REFERENCES:

- [1] Agastya Mehra (2022) Cyber security and its policy implications in the banking sector. *Journal of Internet Banking*, 21(1), 1-14.
- [2] Dhruv Kaushik (2022) Literature review of the effectiveness of law in addressing cyberattacks. *Journal of Cybersecurity*, 6(1), 1-16.
- [3] Jasleen Rajpurohit (2022) Impact of technology on cyber security: Review of literature. *International Journal of Advanced Research in Computer Science*, 10(2), 66-70.
- [4] Vivan Jain (2020) the impact of technology on cyber security: A review of the literature. *Journal of Information Privacy and Security*, 13(1), 1-16.