



CYBERCRIME AND ITS LEGAL CHALLENGES IN INDIA: A CRITICAL ANALYSIS

Anushka Bhagat*

ABSTRACT

The internet age has become a serious threat when it comes to cybercrime. In India, with the speed at which mobile payments, e-governance, AI, cloud computing, and social media are all taking over, the threat of cybercrimes has grown manyfold. The article discusses the concept of Cybercrime and the Indian legal territorial framework, important judicial orders, challenges in the enforcement of cybercrime, and policy changes. It says that although the Information Technology Act 2000 is the base for regulating cyberspace, the technologies are ever-changing and Legal mechanisms should be continuously tailored to the evolving technologies. The article further analyses the privacy, digital evidence, data protection, and international collaboration to fight cybercrime.

Keywords: Cybercrime, IT Act 2000, Cybersecurity, Digital Evidence, Privacy, Data Protection, Cyber Law.

INTRODUCTION

Digital technology has revolutionised today's world in so many ways. More and more systems used in banking, education, health care, commerce, and government rely on internet-based systems. The following are the impacts of such developments on efficiency; they've created opportunities for creating cybercriminals, too. Cybercrime encompasses crimes involving computers, digital devices, networks, and the communications medium. With this increased reliance on digital infrastructure, cybersecurity has become a key legal or policy issue.

Internet usage is one of the highest in the world among all countries in India.¹ As more and more people transact online and use digital platforms; cyber offences have evolved in

*BA LLB (HONS.), SECOND YEAR, HIDAYATULLAH NATIONAL LAW UNIVERSITY, RAIPUR.

¹ International Telecommunication Union, Measuring Digital Development (2023).

sophistication. Offences are committed using technological weaknesses, poor passwords or user names, social engineering techniques, and data breaches. As such, they will need to continue to adapt to new cyber threats posed by legislators, courts, and regulatory bodies.

CYBERCRIME AND ITS TYPES

Cybercrime is an illegal activity that activities are committed by using a computer or network.² Typical crimes include cyber-stalking, online harassment and abuse, financial fraud, data theft, ransomware attacks, ID theft, and phishing. Of the many particular risks, cyber terrorism and attacks on critical infrastructure are especially significant since they could affect vital public services.³

Phishing attacks are designed to trick people into disclosing confidential information. Hidden among the many types of fraudulent activity based on personal information is the act of identity theft. Ransomware attacks encrypt data and request payment. Using electronic communications to harass or threaten someone. These offences often affect people outside their territory and are thus difficult to investigate and prosecute.

LEGAL FRAMEWORK IN INDIA

The major law regulating digital activities in India is the Information Technology Act, 2000.⁴ This legislation grants legal validity to digital signatures and electronic documentation and also adds some cyber offences to the list of criminal offences. Unauthorised access and damage to computer systems are discussed in Section 43⁵. There are crimes committed over the internet. There's a section of crimes dedicated to computer-related crimes. There are specific provisions on identity theft (Section 66C)⁶ and on cheating by personation on a computer resource (Section 66D).⁷

Criminal laws are also applicable to cyber offences, albeit those laws have not been established specifically for the internet. Fraud, forgery, intimidation, and obscenity through electronic

² Debarati Halder and K Jaishankar, *Cyber Crime and the Victimization of Women* (IGI Global, 2012).

³ Information Technology Act 2000.

⁴ *Ibid.*

⁵ Information Technology Act 2000, § 43.

⁶ Information Technology Act 2000, § 66C.

⁷ Information Technology Act 2000, § 66D.

computers are covered by the Bharatiya Nyaya Sanhita and other laws. CERT-In provides support to address cybersecurity incidents and hereby issues guidelines for organisations.⁸

JUDICIAL APPROACH

Indian courts have contributed greatly to the formation of cyber law. The Supreme Court in Justice K.S. Puttaswamy vs Union of India declared privacy to be a fundamental right.⁹ Its decision had a significant impact on the discussions about cybersecurity, surveillance, and data protection. The Court in Shreya Singhal vs Union of India declared that freedom of speech is paramount in today's digital age and invalidated Section 66A of the Information Technology Act.¹⁰

The decisions show that the principle of balancing security with constitutional freedoms must be built into cyber regulation. Courts keep grappling with issues of intermediary liability and digital evidence, and online expression. These decisions illustrate that the regulation of the cyber sphere must take into account the security interests and constitutional freedoms. Courts keep dealing with issues concerning intermediary liability and digital evidence/online expression.

DIFFICULTIES IN THE FIGHT AGAINST CYBERCRIME

There are several challenges to good cybercrime enforcement. Cyber-criminal activities are frequently international and anonymous. Cyber-criminals may have multiple locations and work anonymously. You can alter, encrypt, or even delete digital evidence. Specialist training and technological resources are needed for the investigation of complex cyber offences by Law Enforcement.¹¹

Even regulatory challenges are complicated by quick technological advances. New risks have been added to AI, cryptocurrency, and deep fakes. A lot of users are not aware of cybersecurity methods and hence are susceptible to phishing and fraud. Not having enough experts to perform a cyber investigation negatively impacts the quality of investigations.

⁸ Indian Computer Emergency Response Team (CERT-In), Directions Relating to Information Security Practices (2022).

⁹ Justice KS Puttaswamy v. Union of India (2017) 10 SCC 1.

¹⁰ Shreya Singhal v Union of India (2015) 5 SCC 1.

¹¹ Convention on Cybercrime (Budapest Convention, 2001).

PRIVACY AND DATA PROTECTION

Personal data is currently amongst the most prominent areas of cyber law. However, many organisations gather and work with extensive amounts of personal data regularly. Issues with data privacy may involve the release of personal, financial, and medical information. Raising trust in the digital system and minimising chances for cyber exploitation through privacy protection.¹² There has been a significant increase in emphasis on discussions around responsible data governance following the establishment of privacy as a fundamental right. Businesses must take reasonable measures to secure information they gather and to hold themselves accountable for the security of any information they might handle.

INTERNATIONAL COOPERATION

Cybercrime is a truly international crime. Enforcement needs thus require a worldwide joint effort. The structural methods of information sharing, mutual legal assistance, extradition, and common standards aid investigations. In ransomware and cyber espionage and in critical infrastructure attacks, collaboration is crucial across international borders.¹³ There is a need for a multi-agency holistic approach to cybersecurity strengthening by governments, civil society, and private organisations. Co-operation on a global scale provides one way of solving problems that cannot be solved by any single State.

RECOMMENDATIONS

India needs to build its own cyber forensic infrastructure, create digital literacy, and build the capability of the institute. There is a need for frequent training in cyber investigations for law enforcement. There is a need for a cybersecurity awareness programme in the curriculum of educational institutions. There are opportunities for public/private partnerships to enhance threat detection and incident response.¹⁴

New technologies, such as artificial Intelligence and systems using blockchain technologies, must be covered by legislative changes. There is a need for increased international involvement and exchange of information with regard to coordinated enforcement.

¹² Digital Personal Data Protection Act 2023.

¹³ Convention on Cybercrime (Budapest Convention, 2001).

¹⁴ Ministry of Electronics and Information Technology, National Cyber Security Policy (Government of India).

CONCLUSION

Cybercrime is one of the big issues of the electronic era. India has laid down a significant legal structure with the Information Technology Act, 2000, and cases of privacy and digital rights. However, technological advances still generate new threats to cyber. A secure digital future requires a multifaceted legal framework, technological advancements, awareness building, and global collaboration.