

An Evaluation of Cybercrime in India

Harjinder Kaur¹, Dr. Rajnish Bishnoi²

¹Student, LL.M, University School of Law, Guru Kashi University, Talwandi sabo,
Bathinda, Punjab, India

²Assistant Professor, HOD, University School of Law, Guru Kashi University, Talwandi sabo,
Bathinda, Punjab, India

Abstract

Cyber-crime, in its contemporary manifestation, is no longer limited to isolated instances of identity theft, phishing, or financial fraud. It has evolved into a sophisticated, organized and often state-supported phenomenon capable of destabilizing national infrastructure. Modern cyber threats include cyber terrorism, cyber espionage, ransomware attacks targeting critical information infrastructure, large-scale data breaches, disinformation campaigns and hybrid warfare tactics.¹ These activities demonstrate that cyberspace is no longer a peripheral domain of criminal activity but a strategic battleground where power, influence and sovereignty are contested.

Globally, cyber-attacks on power grids, healthcare institutions, financial networks and government databases illustrate the devastating consequences of digital insecurity. In the Indian context, incidents involving data leaks, ransomware attacks on hospitals, breaches of financial systems and attempts to infiltrate defence communication networks underscore the gravity of the threat.²

Keywords: Cybercrime, defence .terrorism, attacks and data-leaks

1. Introduction

Meaning of Cybercrime

cyber-crime and national security within the changing security environment of the digital age. It begins by discussing the traditional concept of national security, which historically focused on territorial integrity and military defense and then explains how security has expanded to include cyber and digital threats. The chapter examines the idea of cyberspace as the fifth domain of warfare and distinguishes between cyber warfare and cyber-crime. It also analyses concepts such as digital sovereignty, strategic autonomy, hybrid warfare and information warfare. Finally, the chapter highlights the importance of critical infrastructure protection and cyber deterrence in maintaining national security and strategic stability.

¹ Pradeep Kulshrestha, Ritu Gautam & Anita Singh, *Cyber Crime, Regulation and Security: Contemporary Issues and Challenges* (Libertatem Media Private Limited, 2022) pp. 7-17.

² Pradeep Kulshrestha, Ritu Gautam & Anita Singh, *Cyber Crime, Regulation and Security: Contemporary Issues and Challenges* (Libertatem Media Private Limited, 2022) pp. 7-17.

Research Methodology:

This research adopts a doctrinal and analytical methodology to examine cyber-crime as a national security risk in India. The doctrinal approach involves a systematic analysis of primary legal sources, including the Information Technology Act, 2000, relevant provisions of the Indian Penal Code, the Digital Personal Data Protection Act, 2023 and other security-related statutes. Judicial pronouncements, government notifications, policy documents and cybersecurity guidelines will also be examined to assess the scope, interpretation and effectiveness of existing legal mechanisms. The analytical component will evaluate cyber-crime statistics, government reports and national security assessments to understand trends, patterns and the scale of digital threats.

Legal Policy Framework under Cyber Crime

The legal framework governing cyber-crime in India and its role in addressing digital threats. It begins with the constitutional foundations of cyber regulation, particularly the balance between freedom of expression under Article 19 and the right to privacy under Article 21. The chapter then analyses the Information Technology Act, 2000, which serves as the primary legislation dealing with cyber offences and electronic governance. It further discusses the role of criminal laws, including the Indian Penal Code (now replaced by the Bharatiya Nyaya Sanhita) and the Unlawful Activities (Prevention) Act, in addressing cyber-related crimes and terrorism. The chapter also evaluates the Digital Personal Data Protection Act, 2023 and significant judicial interpretations and landmark case laws shaping cyber jurisprudence in India. Article 21 also intersects with cybersecurity concerns related to digital identity systems, biometric databases and government surveillance programs. As digital governance initiatives expand, the State must ensure that technological innovation does not compromise individuals' privacy and dignity.

In conclusion, the constitutional framework of India plays a vital role in shaping cyber regulation and addressing the challenges posed by cyber-crime. Articles 19 and 21 provide the legal foundation for balancing digital freedom, privacy and national security. Judicial decisions such as *Shreya Singhal v. Union of India*³, *Anuradha Bhasin v. Union of India*⁴ and *Justice K.S. Puttaswamy v. Union of India*⁵ have significantly influenced the evolution of cyber law by protecting fundamental rights in the digital space. At the same time, recent legislative developments such as the Digital Personal Data Protection Act, 2023 demonstrate the State's efforts to create a modern regulatory framework for data protection and cybersecurity.

INFORMATION TECHNOLOGY ACT, 2000

The rapid expansion of information technology and internet usage in India during the late 1990s created a need for a legal framework capable of regulating electronic transactions and addressing cyber-related offences. In response, the Government of India enacted the Information Technology Act, 2000, which came into force in October 2000. The Act represents the first comprehensive legislation in India dealing

³*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁴*Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

⁵*Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2017) 10 SCC 1.

with cyber law, electronic governance, digital signatures and cyber-crime. It was later amended through the Information Technology (Amendment) Act, 2008 to address emerging cyber threats, strengthen data protection provisions and introduce new cyber offences.

The Information Technology Act forms the backbone of India's cyber regulatory framework and operates alongside other statutes such as the Indian Penal Code, 1860, the Digital Personal Data Protection Act, 2023 and the Bharatiya Nyaya Sanhita, 2023. It provides both civil and criminal remedies for offences committed through digital systems and establishes mechanisms for electronic governance and cybersecurity management.⁶

Objectives and Scope

The primary objective of the Information Technology Act, 2000 was to provide legal recognition to electronic transactions and facilitate the growth of e-commerce and digital communication in India. Prior to its enactment, Indian law largely relied on traditional legal frameworks that did not adequately recognize electronic records or digital signatures. The Act therefore sought to create a legal infrastructure enabling secure electronic communication and online business activities.

One of the key objectives of the Act is the legal recognition of electronic records and digital signatures. Sections 4 and 5 of the Act provide that electronic records and digital signatures shall have the same legal validity as paper-based documents and handwritten signatures. This provision greatly facilitated the development of e-governance initiatives, online banking, electronic contracts and digital documentation.

Another important objective is the prevention and punishment of cyber-crimes. The Act introduces several offences relating to unauthorized access to computer systems, data theft, hacking, identity theft and online fraud. These provisions were designed to protect individuals, businesses and government institutions from cyber-attacks and digital exploitation.⁷

The Act also promotes electronic governance by enabling government departments to accept electronic filings and issue electronic documents. This has significantly contributed to the development of digital public services such as online tax filing, digital identity systems and e-courts.

The scope of the Information Technology Act extends beyond India through the principle of extraterritorial jurisdiction. Section 75 provides that the Act applies to offences committed outside India if the computer system or network affected is located in India. This provision is particularly important in cyber-crime cases, where attackers often operate across international borders.

⁶ Ravi Shankar & Tabrez Ahmad, "Information Technology Laws: Mapping the Evolution and Impact of Social Media Regulation in India," 41(4) *DESIDOC Journal of Library & Information Technology* 295–301 (2021).

⁷ T. N. Srinivasan & Anne Krueger, "Information-Technology-Enabled Services and India's Growth Prospects [with Comment and Discussion]," in *Brookings Trade Forum* (Brookings Institution Press, 2005).

Growth of Digital infrastructure of Cyber Offences

The Information Technology Act contains several provisions that criminalize different forms of cyber misconduct. These offences primarily fall under Chapter XI of the Act and address both individual and institutional harms caused through digital technologies.

Section 43 of the Act deals with unauthorized access to computer systems and networks. It provides civil liability for acts such as downloading data without permission, introducing computer viruses, damaging computer systems or disrupting services. The provision allows victims to claim compensation for damages caused by such actions.

Section 65 criminalizes tampering with computer source documents. Any person who knowingly conceals, destroys or alters computer source code required to be maintained by law may face imprisonment or fines⁸. This provision is particularly relevant for cases involving software manipulation or deliberate alteration of system programs.

Section 66 deals with computer-related offences such as hacking and unauthorized access when committed with dishonest or fraudulent intent. It converts the acts listed in Section 43 into criminal offences punishable with imprisonment or fines.

The Act also addresses identity theft and online impersonation. Section 66C penalizes fraudulent use of electronic signatures, passwords or unique identification features. Section 66D criminalizes cheating by personation through computer resources, a provision commonly applied in cases involving phishing scams, online banking fraud and social media impersonation.

Another significant provision is Section 66E, which deals with violation of privacy. It criminalizes the capture, publication or transmission of images of a person's private areas without consent.⁹ This provision addresses issues such as voyeurism, hidden camera recordings and online harassment.

Section 67 and related provisions regulate obscene or sexually explicit material in electronic form. These provisions impose penalties for publishing or transmitting obscene content, particularly material involving children.

Powers of Government Surveillance

The Information Technology Act also grants certain powers to the government to monitor, intercept and control digital communications in the interest of national security and public order.¹⁰ These provisions aim to enable law enforcement agencies to prevent cyber-crimes, terrorism and other threats arising from digital networks.

Section 69 of the Act authorizes the central government to intercept, monitor or decrypt information generated or transmitted through computer resources if it is necessary for reasons such as national

⁸ Basu, Arindrajit. "India's Cyber Resilience: Strategy, Financing and Collaboration." *Asia Policy* 20.2 (2025): 10-24.

⁹ Basu, Arindrajit. "India's Cyber Resilience: Strategy, Financing and Collaboration." *Asia Policy* 20.2 (2025): 10-24.

¹⁰ Basu, Arindrajit. "India's Cyber Resilience: Strategy, Financing and Collaboration." *Asia Policy* 20.2 (2025): 10-24.

security, sovereignty of India, public order or prevention of crime. Service providers and intermediaries are required to assist government agencies in carrying out such interception.

The constitutional validity of Section 69A was upheld by the Supreme Court in *Shreya Singhal v. Union of India*¹¹, where the Court recognized that the provision contained procedural safeguards and therefore did not violate freedom of speech.

Another important case related to digital privacy is *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹², where the Supreme Court declared the right to privacy as a fundamental right under Article 21 of the Constitution. This judgment has significant implications for government surveillance powers under the IT Act because any interception or monitoring must now satisfy the tests of legality, necessity and proportionality.

While surveillance powers are essential for national security and crime prevention, they must be exercised carefully to prevent misuse and protect individual liberties. The increasing use of digital technologies by both governments and private entities has intensified debates regarding data protection, privacy and accountability.

Judicial Interpretation and Case Law

Indian courts have played a significant role in clarifying the application of criminal laws to cyber offences. One of the landmark cases in this area is *Shreya Singhal v. Union of India*¹³, in which the Supreme Court struck down Section 66A of the IT Act on the ground that it violated the constitutional guarantee of freedom of speech and expression. The Court emphasized that restrictions on online speech must meet the standards of reasonableness under Article 19(2) of the Constitution.

Another important case relating to digital privacy is *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹⁴, where the Supreme Court recognized the right to privacy as a fundamental right under Article 21. This decision has significant implications for cyber law, particularly in relation to surveillance, data protection and government access to digital information.

Courts have also addressed issues relating to electronic evidence. In *Anvar P.V. v. P.K. Basheer*¹⁵, the Supreme Court clarified the evidentiary requirements for electronic records and emphasized the need for certification under Section 65B of the Evidence Act. This judgment continues to influence the treatment of digital evidence under the new Bharatiya Sakshya Adhiniyam.

¹¹*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹²*Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2017) 10 SCC 1.

¹³ *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

¹⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

¹⁵ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

Conclusion

The rapid growth of digital technologies and social media platforms has fundamentally transformed the way individuals communicate, express opinions and participate in public discourse. In the modern digital era, social media has become one of the most influential mediums for the exercise of freedom of speech and expression. While it has significantly expanded opportunities for democratic participation and information sharing, it has also raised complex legal, social and regulatory challenges.¹⁶ The present study examined the relationship between social media and freedom of speech and expression, with a particular focus on the constitutional framework, emerging cyber laws and the broader implications of digital communication in contemporary society.

Freedom of speech and expression is widely recognized as a fundamental human right and a cornerstone of democratic governance. In India, this right is constitutionally protected under Article 19(1)(a) of the Constitution, which guarantees the freedom of speech and expression to all citizens. However, this freedom is not absolute and is subject to reasonable restrictions under Article 19(2) in the interests of sovereignty and integrity of the state, public order, decency, morality and other specified grounds. The evolution of digital platforms has complicated the application of these constitutional principles, as online communication often transcends geographical boundaries and operates within privately owned digital ecosystems.¹⁷ As a result, the regulation of online speech requires a delicate balance between protecting individual freedoms and preventing the misuse of digital platforms.

¹⁶ Basu, Arindrajit. "India's Cyber Resilience: Strategy, Financing and Collaboration." *Asia Policy* 20.2 (2025): 10-24.

¹⁷ Basu, Arindrajit. "India's Cyber Resilience: Strategy, Financing and Collaboration." *Asia Policy* 20.2 (2025): 10-24.