CYBERCRIME AND CRIMINAL LIABILITY IN THE DIGITAL ERA: CHALLENGES AND LEGAL RESPONSES IN INDIA

M. David Ziegan Paul[1]

VOLUME 2, ISSUE 1 (JANUARY-JUNE 2026)

ABSTRACT

The development of digital technology has changed the way people communicate, conduct business, and access information. Crimes such as hacking, phishing, identity theft, cyberstalking, ransomware attacks, and online financial fraud have become common in recent years. These offences not only affect individuals and businesses but also pose serious threats to national security and public infrastructure. Traditional criminal laws were not originally designed to address crimes committed in cyberspace, which created the need for specialized cyber legislation. This paper examines the concept of cybercrime and analyses criminal liability under Indian law, especially under the Information Technology Act, 2000. The paper discusses important statutory provisions, judicial decisions, and constitutional concerns relating to privacy and freedom of speech in the digital environment. It further examines practical challenges faced by investigating agencies and courts, including jurisdictional difficulties, lack of technical expertise, and problems associated with electronic evidence. The paper also highlights emerging concerns involving artificial intelligence, cryptocurrency, and digital surveillance.

The study adopts a doctrinal research methodology based on statutes, judicial precedents, books, journal articles, and government reports. The paper argues that although India has made considerable progress in developing cyber laws, the legal framework still faces challenges in effective implementation. It concludes that stronger institutional mechanisms, technological preparedness, public awareness, and continuous legal reforms are essential to combat cybercrime effectively in the digital era.

Keywords: Cybercrime, Criminal Liability, Information Technology Act, Digital Evidence, Cyber Law, Cyber Terrorism.

[1] M.David Ziegan Paul, *Bharath Institute Of Law.*

INTRODUCTION

The digital revolution has fundamentally altered the structure of modern society. Internet-based services now influence nearly every aspect of human life, including education, healthcare, governance, finance, and business transactions. India has emerged as one of the fastest-growing digital economies, supported by increasing internet penetration, smartphone usage, online banking systems, and digital governance initiatives such as Digital India. While these developments have created new opportunities for economic and technological growth, they have simultaneously exposed individuals and institutions to serious cyber threats.

Cybercrime has become one of the most significant challenges in the contemporary legal landscape. Cybercriminals exploit technological vulnerabilities to commit offences such as hacking, phishing, identity theft, financial fraud, data breaches, cyberstalking, and online harassment. The anonymous and borderless nature of cyberspace complicates investigation and prosecution, making cybercrime a complex issue for criminal justice systems across the world.[2]

India has witnessed a sharp increase in cybercrime incidents over the last decade. Online financial frauds, unauthorized access to databases, ransomware attacks on institutions, and misuse of social media platforms have become increasingly common. High-profile incidents such as the AIIMS ransomware attack highlighted the vulnerability of critical digital infrastructure and demonstrated the urgent need for effective cybersecurity measures.[3] The growth of artificial intelligence, cryptocurrency transactions, and encrypted communication has further complicated the legal and regulatory framework governing cyber offences.

The traditional provisions of criminal law under the Indian Penal Code were insufficient to address offences committed through digital means. In response, Parliament enacted the Information Technology Act, 2000 to provide legal recognition to electronic records and regulate cyber activities.[4] The Act was later amended in 2008 to include stricter provisions relating to identity theft, cyber terrorism, obscenity, privacy violations, and intermediary liability. Judicial decisions have also played an important role in shaping cyber jurisprudence in India, particularly in balancing criminal liability with constitutional rights such as freedom of speech and privacy.[5]

---

[2] JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME 8–10 (2d ed. 2015).
[3] NINA GODBOLE & SUNIT BELAPURE, CYBER SECURITY: UNDERSTANDING CYBER CRIMES, COMPUTER FORENSICS AND LEGAL PERSPECTIVES 25 (2011).
[4] Aparna Viswanathan, Cybercrime and Jurisdictional Issues in India, 12 INDIAN J.L. & TECH. 45, 49 (2021).
[5] Press Trust of India, AIIMS Ransomware Attack Highlights Cybersecurity Concerns, THE HINDU (Nov. 28, 2022), https://www.thehindu.com.

This paper examines the concept and scope of cybercrime, analyses the framework of criminal liability under Indian law, evaluates judicial approaches, and identifies major challenges in cybercrime regulation. It further discusses reforms necessary for strengthening India's cyber legal regime in the digital era.

RESEARCH QUESTIONS

What constitutes cybercrime under Indian law?

How does Indian legislation determine criminal liability in cyberspace?

What are the major challenges in investigating and prosecuting cyber offences in India?

Whether the existing legal framework is sufficient to address emerging cyber threats?

RESEARCH METHODOLOGY

This study adopts a doctrinal and analytical method of research. Primary sources such as statutes, judicial decisions, government reports, and legal provisions have been examined. Secondary sources including journal articles, books, research papers, and online databases have also been referred to for comprehensive analysis.

UNDERSTANDING CYBERCRIME

Cybercrime refers to offences committed using computers, digital devices, or communication networks. In some cases, the computer itself becomes the target of the offence, while in others it acts as a tool for committing the crime.[6] Cybercrime differs from conventional offences because it can be committed remotely and anonymously without physical contact between the offender and the victim.

The nature of cybercrime has evolved along with technological advancement. Earlier cyber offences mainly involved unauthorized access to computer systems or simple hacking activities. However, the expansion of internet services, online banking, social media, and cloud computing has led to more sophisticated forms of digital crime. Today, cybercriminals use advanced technologies to steal financial data, spread malware, commit identity theft, and disrupt computer systems.[7]

Cybercrime may broadly be divided into three categories: crimes against individuals, crimes against property, and crimes against the state. Crimes against individuals include cyberstalking,

[6] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

[7] GODBOLE & BELAPURE, supra note 2, at 28.

online harassment, identity theft, and phishing scams. Crimes against property involve hacking, ransomware attacks, data theft, and intellectual property infringement. Crimes against the state include cyber terrorism and attacks on critical digital infrastructure.

One of the most common forms of cybercrime in India is phishing. Fraudsters send fake emails or create fake websites resembling genuine institutions to obtain confidential information such as passwords and banking credentials. Many individuals become victims because they are unable to distinguish between authentic and fraudulent communication. Identity theft has similarly increased due to unauthorized access to personal information available on digital platforms.

Cyberstalking and online harassment have also become serious social concerns. Women and children are particularly vulnerable to digital abuse through social media platforms. The misuse of private photographs, fake online profiles, and threatening messages has increased substantially in recent years. Such offences affect not only personal safety but also mental health and dignity.

Ransomware attacks represent another major cyber threat. In these attacks, malicious software encrypts digital data and demands payment for restoring access. The ransomware attack on AIIMS disrupted hospital services and exposed weaknesses in cybersecurity infrastructure. These incidents show that cybercrime can have serious consequences for public administration and national security. The investigation of cybercrime presents several practical difficulties.[8] Digital evidence can easily be altered or deleted. Cybercriminals often use fake identities, encrypted communication systems, and virtual private networks to conceal their activities. As a result, tracing offenders becomes extremely difficult for investigating agencies.

EVOLUTION OF CYBER LAW IN INDIA

The increasing use of electronic communication and internet-based services highlighted the need for a specialized legal framework in India. Before the enactment of cyber legislation, offences involving computers were dealt with under traditional criminal laws, which were not equipped to handle technological complexities.

India enacted the Information Technology Act, 2000 based on the UNCITRAL Model Law on Electronic Commerce. The primary objective of the legislation was to provide legal recognition to electronic records and digital signatures while facilitating electronic commerce and e-governance. The Act also introduced provisions dealing with cyber offences and penalties.

[8] Press Trust of India, supra note 4.

The original legislation focused mainly on electronic transactions and digital authentication. However, the rapid increase in cybercrime soon exposed the limitations of the law. Consequently, Parliament enacted the Information Technology (Amendment) Act, 2008 to strengthen cybercrime regulation. The amendment introduced provisions dealing with identity theft, cyber terrorism, privacy violations, and intermediary liability.

Section 43 of the Information Technology Act imposes civil liability for unauthorized access, downloading of data, introduction of computer viruses, and disruption of computer systems. Section 66 converts these acts into criminal offences when committed dishonestly or fraudulently. Section 66C criminalizes identity theft, while Section 66D punishes cheating by personation through digital means.

Section 66E deals with violations of privacy involving unauthorized capture or transmission of private images. Section 66F criminalizes cyber terrorism and recognizes the growing threat posed by attacks on digital infrastructure and national security systems.

The legislation also regulates obscene and sexually explicit online content. Sections 67 and 67B prohibit the publication and transmission of obscene material and child sexual abuse content in electronic form. These provisions aim to prevent online exploitation and abuse.

Another important provision is Section 79, which deals with intermediary liability. Social media platforms and internet service providers are granted conditional immunity if they comply with due diligence requirements and government directions. The role and responsibility of intermediaries have become increasingly important due to the growth of digital communication platforms.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 further expanded the responsibilities of intermediaries by introducing grievance redressal mechanisms and compliance obligations. These developments indicate that cyber governance in India is continuously evolving in response to technological changes.

CRIMINAL LIABILITY IN CYBERSPACE

Criminal liability in cyberspace involves determining responsibility for offences committed through digital technology. Establishing liability in cyber offences is often more difficult than in conventional crimes because cybercriminals frequently operate anonymously and across international borders.

One of the essential elements of criminal liability is mens rea or guilty intention. In cyber offences, intention is usually inferred from digital records, communication history, and technical evidence.

Courts examine the conduct of the accused and surrounding circumstances to determine criminal intent.

The Information Technology Act creates both civil and criminal liability for cyber offences. Section 66 punishes computer-related offences committed dishonestly or fraudulently. Fraudsters often misuse passwords, OTPs, and confidential credentials to gain unauthorized access to bank accounts.

Section 66D addresses cheating through personation using communication devices. Online investment frauds, fake customer care scams, and fraudulent online advertisements are commonly prosecuted under this provision. Such offences have increased significantly with the expansion of digital transactions.

The issue of intermediary liability has become one of the most debated aspects of cyber law. Social media platforms and online intermediaries play an important role in facilitating communication and sharing information. Questions often arise regarding their liability for unlawful content posted by users. Section 79 grants safe harbour protection to intermediaries if they comply with due diligence obligations.

The constitutional validity of restrictions on online speech was examined by the Supreme Court in Shreya Singhal v. Union of India. The Court struck down Section 66A of the Information Technology Act on the ground that it violated freedom of speech guaranteed under Article 19(1)(a) of the Constitution. The judgment emphasized that vague restrictions on online expression are unconstitutional.

Cyber law also intersects with the constitutional right to privacy. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognized privacy as a fundamental right under Article 21 of the Constitution.[9] The judgment has important implications for digital surveillance, data protection, and state monitoring powers.

Corporate liability has similarly gained importance in recent years. Companies handling sensitive personal data may face legal consequences for failing to implement adequate cybersecurity measures. Data breaches affecting financial institutions and healthcare organizations demonstrate the need for stronger corporate accountability in cyberspace.

[9] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

JUDICIAL APPROACH TOWARDS CYBERCRIME

One of the earliest cybercrime convictions in India was State of Tamil Nadu v. Suhas Katti.[10] The accused was convicted for posting obscene and defamatory messages online. The case demonstrated that existing cyber laws could effectively address online harassment and cyber abuse.

The admissibility of electronic evidence was clarified in Anvar P.V. v. P.K. Basheer.[11] The Supreme Court held that electronic records are admissible only if accompanied by a certificate under Section 65B of the Indian Evidence Act. This judgment established important evidentiary standards for digital evidence in criminal proceedings.

The landmark judgment in Shreya Singhal v. Union of India significantly influenced India's cyber jurisprudence.[12] The Court held that Section 66A of the Information Technology Act violated constitutional protections for free speech because its language was vague and susceptible to misuse. The decision reaffirmed the principle that restrictions on speech must satisfy constitutional standards of reasonableness.

In Avnish Bajaj v. State (NCT of Delhi), commonly known as the Bazee.com case, the issue concerned liability of intermediaries for objectionable online content. The case highlighted the difficulties in balancing intermediary responsibility with protection from excessive liability.

Indian courts have increasingly recognized the seriousness of cyber offences. High Courts in various states have repeatedly emphasized the need for stronger cyber forensic infrastructure, trained personnel, and specialized cybercrime investigation units. Judicial observations also indicate concern regarding delays in cybercrime investigation and lack of technological expertise among investigating authorities.

CHALLENGES IN CYBERCRIME REGULATION

Despite legislative developments, India continues to face several challenges in regulating cybercrime effectively. One major issue is jurisdiction. Cyber offences frequently involve multiple jurisdictions because offenders, victims, and servers may be located in different countries. Determining territorial jurisdiction becomes difficult in cross-border cybercrime cases. Existing procedural mechanisms often fail to ensure timely international cooperation.

[10] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Tamil Nadu Dist. Ct. Nov. 5, 2004) (India).
[11] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[12] Shreya Singhal, (2015) 5 S.C.C. at 35.

Another significant challenge is the lack of technical expertise among law enforcement agencies. Cybercrime investigation requires specialized knowledge of digital forensics, encryption systems, malware analysis, and blockchain technology. Many police officers and prosecutors lack adequate training in handling technologically advanced offences.

The collection and preservation of electronic evidence also create practical difficulties. Digital evidence is highly volatile and can easily be altered or destroyed. Improper handling of electronic records may render them inadmissible before courts. The requirement of certification under Section 65B further complicates evidentiary procedures.

The rise of artificial intelligence has introduced new forms of cyber threats. Deepfake technology can be used to create fabricated videos and manipulate public perception. Artificial intelligence systems may also facilitate automated cyberattacks and large-scale phishing operations. Existing laws do not comprehensively regulate such emerging technological threats.

Cryptocurrency-related crimes have similarly increased in recent years. Anonymous digital transactions enable money laundering, online fraud, and financing of illegal activities. The absence of a comprehensive cryptocurrency regulatory framework complicates criminal enforcement.

Underreporting of cybercrime remains another concern. Many victims avoid reporting cyber offences due to embarrassment, fear of reputational damage, or lack of confidence in investigative authorities. Women and children facing online harassment often hesitate to approach law enforcement agencies.

Balancing cybersecurity with constitutional freedoms presents an additional challenge. Government powers relating to interception, surveillance, and online content blocking must be exercised carefully to prevent violations of privacy and freedom of speech. Excessive state control over digital platforms may create concerns regarding democratic accountability.

SUGGESTIONS AND REFORMS

India's cyber legal framework requires continuous reform to address evolving digital threats effectively. First, there is a need for specialized cybercrime courts to ensure speedy disposal of technologically complex cases. Delays in investigation and trial reduce the effectiveness of criminal enforcement.

Second, law enforcement agencies should receive advanced training in digital forensics, artificial intelligence, blockchain investigation, and cyber intelligence. Modern cybercrime requires technical expertise beyond conventional policing methods.

Third, India must strengthen international cooperation mechanisms for cross-border cyber investigations. Cybercrime is a global phenomenon, and effective enforcement requires coordinated international action.

Fourth, comprehensive legislation regulating artificial intelligence, deepfake technology, and cryptocurrency transactions should be introduced. Existing laws are insufficient to address these emerging digital risks.

Fifth, public awareness programs relating to cyber safety and digital literacy should be expanded. Educating citizens regarding phishing scams, online frauds, and data privacy can significantly reduce cyber victimization.

Finally, cyber governance must maintain a balance between national security and constitutional freedoms. Legal safeguards against arbitrary surveillance and censorship are essential for preserving democratic values in the digital age.

CONCLUSION

Cybercrime has emerged as one of the most complex legal challenges of the twenty-first century. India's rapid digital transformation has increased dependence on technology while simultaneously exposing individuals, corporations, and public institutions to serious cyber threats. The Information Technology Act, 2000 and its subsequent amendments represent important steps towards regulating cyberspace and establishing criminal liability for digital offences.

Judicial decisions have significantly contributed to the development of cyber jurisprudence by addressing issues such as electronic evidence, intermediary liability, online speech, and privacy rights. However, the constantly evolving nature of technology continues to create legal and practical challenges. Jurisdictional barriers, lack of technical expertise, inadequate forensic infrastructure, and emerging threats involving artificial intelligence and cryptocurrency complicate cybercrime enforcement.

A strong cyber legal framework requires not only effective legislation but also efficient implementation mechanisms, international cooperation, technological preparedness, and public awareness. India must therefore adopt a balanced and forward-looking approach that ensures cybersecurity without undermining constitutional freedoms. The future effectiveness of criminal justice in the digital era will largely depend on the ability of law to adapt to rapidly changing technological realities.