The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CYBER CRIME AND LEGAL REMEDIES: A CRITICAL ANALYSIS OF THE INDIAN LEGAL FRAMEWORK

~ TRIPTI PAL

ABSTRACT:

The rapid digitization of society has transformed communication, commerce, governance, and social interaction. However, this digital revolution has also generated new forms of criminality collectively referred to as cyber crime. From identity theft and financial fraud to cyber terrorism and online harassment, cyber crime presents complex challenges to traditional legal systems. In India, the Information Technology Act, 2000 (IT Act), along with provisions of the Indian Penal Code and allied legislation, forms the backbone of cyber law enforcement. Judicial interpretation has further shaped the contours of digital rights and liabilities. This article critically examines the concept, categories, and impact of cyber crime; analyses the statutory and constitutional framework governing cyber offences in India; discusses leading judicial precedents; evaluates procedural and remedial mechanisms; and identifies gaps in enforcement. It concludes by proposing reforms to strengthen India's cyber resilience while balancing digital freedom and security.

I. INTRODUCTION:

The digital revolution has fundamentally transformed governance, commerce, communication, and social interaction. With the expansion of internet penetration, mobile banking, e-governance platforms, artificial intelligence, and cloud computing, cyberspace has become an indispensable part of modern life. However, this rapid digitalization has simultaneously given rise to a new spectrum of criminal activities collectively referred to as cyber crime.

Cyber crime is broadly defined as any unlawful act in which a computer, network, or digital device is used as a tool, target, or place of criminal activity. Unlike traditional crimes, cyber offences are borderless, technologically complex, and often anonymous. They challenge territorial jurisdiction, evidentiary norms, and enforcement mechanisms.

India, as one of the fastest-growing digital economies, faces significant cyber threats ranging from online financial fraud and identity theft to cyber terrorism and data breaches. The legislative response primarily includes the Information Technology Act, 2000[1], supported by provisions of the Indian Penal Code, 1860[2], and constitutional safeguards[3].

Judicial pronouncements, particularly *Shreya Singhal v. Union of India*[4], have shaped the constitutional boundaries of cyber regulation. Further, the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[5] has had far-reaching implications for digital governance.

This article systematically examines the concept of cyber crime, statutory and constitutional frameworks, legal remedies available to victims, enforcement challenges, and necessary reforms within the Indian context.

II. CONCEPT AND NATURE OF CYBER CRIME:

Cyber crime refers to unlawful activities committed through digital means, where a computer, network, or electronic device acts as the tool, target, or medium of the offence. With the rapid growth of internet access and digital technology, cyber crime has become a serious threat to individuals, businesses, and governments.

---

[1] The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).

[2] The Indian Penal Code, No. 45 of 1860, Acts of Parliament, 1860 (India).

[3] INDIA CONST. arts. 14, 19(1)(a), 19(2), 21, 32, 226.

[4] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

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

Cyber offences can be broadly classified into three categories: crimes against individuals, crimes against property, and crimes against the state. Crimes against individuals include identity theft, cyber stalking, online harassment, and circulation of defamatory or obscene content, which harm personal dignity and privacy. Crimes against property involve hacking, data theft, ransomware attacks, intellectual property violations, and online financial fraud, affecting economic security. Crimes against the state include cyber terrorism, espionage, and attacks on critical infrastructure, posing risks to national security.

Cyber crimes differ from traditional crimes due to anonymity, borderless operation, speed, and technical complexity. Offenders often hide their identity using advanced technologies, and digital evidence requires expert handling. As technology evolves, cyber criminal methods also change, demanding strong legal frameworks, effective investigation, and international cooperation to address these challenges.

III. TYPES OF CYBER CRIMES:

A. Hacking and Unauthorized Access: Hacking involves unauthorized access to computer systems or networks. Section 43 of the IT Act provides civil liability for unauthorized access, data downloading, or introduction of viruses. Section 66 converts such acts into criminal offences when committed dishonestly or fraudulently.

B. Identity Theft and Impersonation: Section 66C criminalizes identity theft involving fraudulent use of electronic signatures or passwords. Section 66D penalizes cheating by personation using computer resources. These provisions address rising incidents of phishing, OTP fraud, and digital impersonation.

C. Cyber Stalking and Harassment: Cyber stalking involves repeated online harassment or monitoring. Though not explicitly defined in the IT Act, relevant provisions include Section 66E (violation of privacy) and Sections 354D and 509 of the IPC.

D. Cyber Terrorism: Section 66F of the IT Act defines cyber terrorism as acts intended to threaten the unity, integrity, security, or sovereignty of India by disrupting critical information infrastructure. This provision reflects the recognition that cyber attacks may endanger national security.

E. Obscenity and Child Sexual Abuse Material: Sections 67, 67A, and 67B criminalize publishing or transmitting obscene material and child sexual abuse material in electronic form.

F. Financial Cyber Frauds: Online banking fraud, credit card fraud, UPI scams, and ransomware attacks fall under both IT Act provisions and IPC offences such as cheating (Section 420 IPC) and criminal breach of trust.

IV. INTERNATIONAL LEGAL FRAMEWORK:

Cyber crime is not limited by national borders. A person sitting in one country can hack a computer, steal data, or commit online fraud in another country within seconds. Because of this transnational nature, international cooperation is essential to prevent, investigate, and punish cyber offences effectively. The most important international treaty on cyber crime is the Budapest Convention on Cybercrime. Adopted in 2001 by the Council of Europe[6], it aims to harmonize national cyber laws, improve investigative techniques, and promote cooperation among countries through mutual legal assistance. It also promotes cooperation between countries through mutual legal assistance. However, India is not a signatory to this Convention due to concerns about sovereignty and limited participation in its drafting.

Despite this, India cooperates with other countries through Mutual Legal Assistance Treaties (MLATs), which allow sharing of evidence and information during investigations. India also works with Interpol to track and coordinate action against cyber criminals.
Since cyber threats are global, no country can fight them alone. India must continue strengthening international partnerships while ensuring that cooperation respects constitutional principles such as privacy, due process, and protection of fundamental rights.

V. STATUTORY FRAMEWORK IN INDIA: (600 Words)

[6] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Council of Europe).

India has developed a legal framework to deal with cyber crimes through a combination of special cyber laws and traditional criminal laws. The following statutes form the backbone of cyber regulation in India:

India has developed a combined legal framework to deal with cyber crimes through special cyber laws and traditional criminal laws.

A. Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is the primary law governing cyber offences and electronic transactions. It gives legal recognition to electronic records and digital signatures and defines various cyber crimes.

- **Section 43** provides civil liability and allows victims to claim compensation for unauthorized access, data theft, introducing viruses, or damaging computer systems.
- **Section 66** imposes criminal punishment when such acts are done dishonestly or fraudulently.
- **Sections 66C and 66D** deal with identity theft and online cheating, including phishing and impersonation.
- **Section 66F** addresses cyber terrorism and threats to national security.
- **Sections 67, 67A, and 67B** punish online obscenity, sexually explicit material, and child sexual abuse content.

The 2008 Amendment[7] expanded offences, introduced stricter punishments, and strengthened data protection provisions.

B. Intermediary Liability – Section 79

Section 79 provides safe harbour protection to intermediaries if they follow due diligence and remove unlawful content upon receiving a court order or government notice, as clarified in *Shreya Singhal v. Union of India*. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[8] impose additional compliance obligations

C. Indian Penal Code, 1860

[7] Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2009 (India).

[8] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

The IPC supports the IT Act by covering cheating (Section 420), forgery (Sections 463–471), defamation (Section 499), and criminal intimidation (Section 506) when committed online.

D. Indian Evidence Act, 1872[9]

Section 65B requires certification for admissibility of electronic evidence, as made mandatory in *Anvar P.V. v. P.K. Basheer*[10].

E. Digital Personal Data Protection Act, 2023

The DPDP Act[11] regulates personal data processing, requires consent, imposes penalties for breaches, and establishes a Data Protection Board.

Together, these laws aim to prevent cyber offences and ensure safe digital development in India.

VI. CONSTITUTIONAL DIMENSIONS OF CYBER REGULATION: (400 Words)

Cyber laws in India must follow the Constitution, especially Articles 14, 19, and 21. While the government can regulate online activities for public order and national security, such regulation cannot violate fundamental rights. As the internet has become an important space for speech, business, and personal communication, constitutional protection is essential in digital matters.

A. Freedom of Speech and Expression: Article 19(1)(a) guarantees freedom of speech and expression, and this right also applies to online platforms like social media and messaging apps. However, Article 19(2) allows reasonable restrictions for reasons such as national security, public order, decency, and morality.

---

[9] The Indian Evidence Act, No. 1 of 1872, Acts of Parliament, 1872 (India).

[10] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

[11] The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

Section 66A of the Information Technology Act, 2000 punished sending "offensive" messages online. In *Shreya Singhal v. Union of India*, the Supreme Court struck down this section because it was vague and misused. The Court held that online speech enjoys the same protection as offline speech, and any restriction must be clear, reasonable, and within Article 19(2).

B. Right to Privacy: Article 21 protects life and personal liberty. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court declared privacy a fundamental right. This decision is important for issues like data protection and digital surveillance.

The Court stated that any government action involving personal data must be legal, necessary, and proportionate. Thus, cyber regulation must balance national security with the protection of individual privacy.

VII. INTERMEDIARY LIABILITY AND PLATFORM REGULATION:

Section 79 of the IT Act grants safe harbour protection to intermediaries (e.g., social media platforms) provided they observe due diligence and remove unlawful content upon notice.

In **Shreya Singhal v. Union of India**, the Court clarified that intermediaries are required to remove content only upon receipt of a court order or government notification.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[12] impose additional compliance obligations, including grievance redressal mechanisms and traceability requirements for significant social media intermediaries.

VI. LEGAL REMEDIES FOR VICTIMS:

Victims of cyber crime in India have several legal remedies available under different laws. These remedies aim to punish offenders, compensate victims, and protect their rights.

[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E)

1. Criminal Remedies: A victim can file a First Information Report (FIR) at the nearest cyber police station or any police station. Many states have special cyber crime cells to handle digital offences. Once the complaint is registered, the police investigate the matter. If the accused is found guilty, they may face imprisonment, fines, or both under the Information Technology Act, 2000 and the Indian Penal Code, 1860. Criminal remedies focus on punishing the offender and preventing future crimes.

2. Civil Compensation: Under Section 43 of the Information Technology Act, victims can claim monetary compensation for damage caused to their computer systems or data. Complaints can be filed before an Adjudicating Officer appointed under the Act. This remedy is useful in cases involving data theft, hacking, or system damage where financial loss has occurred.

3. Constitutional Remedies: If a cyber crime results in violation of fundamental rights such as freedom of speech or privacy the victim can approach the High Court under Article 226 or the Supreme Court under Article 32 of the Constitution. These writ petitions are especially important in cases involving unlawful surveillance or misuse of state power.

4. Banking Remedies: In cases of online banking fraud or unauthorized digital transactions, victims must immediately inform their bank. The Reserve Bank of India (RBI) has issued guidelines for reporting such frauds. If reported quickly, customers may receive reimbursement of the lost amount.[13]

5. Data Protection Remedies: Under the Digital Personal Data Protection Act, 2023, individuals can file complaints before the Data Protection Board if their personal data is misused or leaked. Penalties can be imposed on organizations responsible for data breaches.

These combined remedies provide both legal protection and financial relief to victims of cyber crime.

---

[13] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017)

VII. CHALLENGES IN ENFORCEMENT:

Even though India has detailed cyber laws, enforcing them effectively remains a major challenge. The following key issues affect cyber crime investigation and prosecution:

1. Lack of Technical Expertise:

- Cyber crimes involve advanced technology such as encryption, malware, and blockchain.
- Many police officers and investigators lack specialized training in digital forensics.
- Without proper technical knowledge, collecting and preserving digital evidence becomes difficult.

2. Low Conviction Rates:

- Cyber cases often depend on electronic evidence, which must meet strict legal standards.
- Delays in investigation and improper handling of digital evidence weaken cases.
- As a result, conviction rates in cyber crime cases remain low compared to traditional crimes.

3. Cross-Border Jurisdictional Issues:

- Cyber criminals often operate from other countries.
- Accessing data stored on foreign servers requires international cooperation.
- Legal processes like Mutual Legal Assistance Treaties (MLATs) take time, causing delays in investigation.

4. Rapid Technological Changes:

- Technology evolves faster than laws and enforcement methods.
- New crimes such as ransomware, cryptocurrency fraud, and AI-based scams emerge frequently.
- Law enforcement agencies struggle to keep pace with these changes.

5. Public Unawareness:

- Many victims do not report cyber crimes due to lack of awareness or fear of social stigma.

- People often do not know how to secure their digital accounts properly.
- Low awareness increases vulnerability to fraud and scams.

6. Weak Digital Forensic Infrastructure:

- Many regions lack advanced forensic laboratories and modern tools.
- Delays in forensic analysis slow down court proceedings.
- Limited infrastructure affects the quality of evidence presented in court.

~To improve cyber governance, India must strengthen institutional capacity by investing in training, upgrading forensic infrastructure, increasing public awareness, and improving international cooperation mechanisms.

VIII. REFORM AND POLICY RECOMMENDATIONS: (300 Words)

To effectively combat cyber crime and strengthen digital governance, India must adopt comprehensive reforms and forward-looking policy measures. The following recommendations can significantly improve the existing system:

- **Creation of a Unified Cyber Crime Code:** Cyber offences are currently spread across different laws like the IT Act and IPC. A single, updated cyber crime code would remove confusion, ensure clarity, and address new crimes such as cryptocurrency fraud and AI-based attacks.
- **Establishment of Specialized Cyber Courts:** Cyber cases involve technical evidence. Dedicated cyber courts with trained judges would ensure faster trials, better understanding of digital issues, and improved conviction rates.
- **Enhanced International Cooperation:** Since cyber crime is borderless, India must strengthen global partnerships through faster legal assistance, data-sharing agreements, and active participation in international forums.
- **Public Digital Literacy Campaigns:** Awareness programs should educate citizens about online safety, fraud prevention, and reporting mechanisms to reduce cyber crime risks.
- **Stronger Victim Compensation Mechanisms:** Simple compensation procedures and dedicated relief funds can help victims recover financial losses quickly.

- **Continuous Technological Training:** Regular training for police, prosecutors, and judges is necessary to keep up with rapidly changing technology.

Ultimately, policy formulation must carefully balance technological innovation with national security and protection of individual rights.

CONCLUSION:

Cyber crime has emerged as one of the most serious legal and governance challenges in the digital era. As India continues to expand its digital infrastructure through online banking, e-governance platforms, and digital communication systems, the risks associated with cyber offences have also increased significantly. From identity theft and financial fraud to cyber terrorism and data breaches, cyber crime affects individuals, businesses, and the State alike.

India has developed a structured legal framework to address these threats. The Information Technology Act, 2000, supported by the Indian Penal Code, the Indian Evidence Act, and the Digital Personal Data Protection Act, 2023, provides both preventive and punitive mechanisms. Judicial decisions such as Shreya Singhal v. Union of India and Justice K.S. Puttaswamy (Retd.) v. Union of India have ensured that cyber regulation remains consistent with constitutional principles, particularly freedom of speech and the right to privacy. These judgments reaffirm that digital spaces are protected by the same constitutional safeguards that apply offline. At the same time, significant challenges remain in enforcement. Issues such as lack of technical expertise, cross-border jurisdictional barriers, low conviction rates, and rapid technological changes limit the effectiveness of existing laws. Therefore, legal reform must be accompanied by institutional strengthening, specialized training, improved forensic infrastructure, and enhanced international cooperation.

Ultimately, India’s approach to cyber regulation must strike a careful balance between innovation and security, and between state interests and individual rights. A coordinated, rights-based, and technologically adaptive legal system is essential to ensure safe digital growth and public trust in the digital ecosystem.

REFERANCE:

- The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
- The Indian Penal Code, No. 45 of 1860, Acts of Parliament, 1860 (India).
- INDIA CONST. arts. 14, 19(1)(a), 19(2), 21, 32, 226.
- *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
- Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Council of Europe).
- Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2009 (India).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
- The Indian Evidence Act, No. 1 of 1872, Acts of Parliament, 1872 (India).
- *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
- The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017)