iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79889

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Legislation's Control on Cyber Crime in India

Daksh Khera[1], Shivansh Grover[2], Farmaan Sapra[3], Yogita Thareja[4]
Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India

Abstract: ***The exponential growth of digital technologies in India has led to a parallel rise in cybercrime, posing serious threats to individuals, businesses, and national security. Legislative measures play a crucial role in defining, preventing, and punishing cyber offences. This paper critically examines the legal framework in India, primarily focusing on the Information Technology Act, 2000, along with other supporting laws. It also analyses landmark judicial decisions and recent real-world cybercrime cases (2023–2025). The study identifies gaps in the current legal system and suggests reforms to strengthen cybercrime control through legislation.***

I. INTRODUCTION

India's transition into a digital economy has significantly transformed communication, commerce, and governance. However, this digital expansion has also created opportunities for cybercriminal activities such as online fraud, identity theft, hacking, and cyber terrorism. Cybercrime differs from traditional crime due to its borderless nature, anonymity, and reliance on technology. As a result, traditional legal systems are often inadequate to address these challenges. Legislative intervention is therefore essential to regulate cyberspace, ensure accountability, and protect digital rights.

II. CONCEPT AND NATURE OF CYBER CRIME

Cybercrime refers to unlawful activities conducted using computers, digital devices, or networks. These crimes may involve unauthorized access to systems, theft of sensitive data, or disruption of services.

Key characteristics of cybercrime include:

1) Anonymity: Criminals can hide their identity
2) Global reach: Crimes can be committed across borders
3) High speed: Attacks can occur within seconds
4) Technical complexity: Requires specialized knowledge

III. NEED FOR LEGISLATIVE CONTROL OF CYBER CRIME IN INDIA

The necessity of cyber laws in India arises due to several factors:

1) Increasing dependence on digital platforms
2) Lack of physical evidence in cyber offences
3) Growing incidents of financial fraud and data breaches
4) Need for protection of personal and organizational data

Before the enactment of cyber laws, India lacked a structured mechanism to address such crimes, making prosecution difficult.

IV. LEGISLATIVE FRAMEWORK IN INDIA

A. Information Technology Act, 2000

The backbone of cyber law in India is the IT Act, 2000. It provides legal recognition to electronic records and establishes a framework to deal with cyber offences.

Key features:

- Legal recognition of digital signatures
- Definition of cyber offences
- Establishment of penalties and compensation
- Facilitation of e-governance

B. IT Amendment Act, 2008

The amendment expanded the scope of the IT Act by:

- Introducing stricter penalties
- Recognizing electronic signatures
- Addressing emerging cyber threats
- Including provisions for data protection

C. *Other Supporting Laws*

Cybercrime control in India is not limited to the IT Act. Other laws include:

- Indian Penal Code (IPC) / Bharatiya Nyaya Sanhita (BNS), 2023
- Indian Evidence Act (electronic evidence admissibility)
- Digital Personal Data Protection Act, 2023

These laws complement the IT Act and strengthen the legal framework.

V. ROLE OF LEGISLATION IN CONTROLLING CYBER CRIME

Legislation plays a multi-dimensional role in combating cybercrime:

1) Definition of offences: Clearly identifies cyber activities as criminal
2) Deterrence: Provides punishment to discourage criminal behavior
3) Investigation support: Empowers law enforcement agencies
4) Protection of rights: Ensures privacy and data security

Without legislation, controlling cybercrime would be extremely difficult due to its technical and cross-border nature.

VI. JUDICIAL APPROACH AND LANDMARK CASE LAWS

Shreya Singhal v. Union of India

The Supreme Court struck down Section 66A of the IT Act, holding it unconstitutional due to its vague nature and violation of freedom of speech. This case ensured that cyber laws do not infringe fundamental rights.

K.S. Puttaswamy v. Union of India

The Court recognized the right to privacy as a fundamental right. This judgment significantly influenced data protection and cyber law policies in India.

Anvar P.V. v. P.K. Basheer

This case established the legal framework for admissibility of electronic evidence, making Section 65B certification mandatory.

Avnish Bajaj v. State (Bazee.com Case)

The case clarified the liability of intermediaries and led to better regulation of online platforms.

VII. RECENT CYBER CRIME CASES IN INDIA (2023–2025)

A. *₹400 Crore Export Fraud Case*

Cybercriminals exploited digital identity systems (Aadhaar, PAN) to claim fake export incentives. This highlights vulnerabilities in e-governance systems.

B. *Digital Arrest Scam*

Fraudsters impersonated law enforcement officials and coerced victims into transferring money. This case shows misuse of legal fear and social engineering.

C. *APK Malware Banking Fraud*

Victims were tricked into installing malicious apps, leading to unauthorized bank transactions. This reflects the growing risk of mobile-based cybercrime.

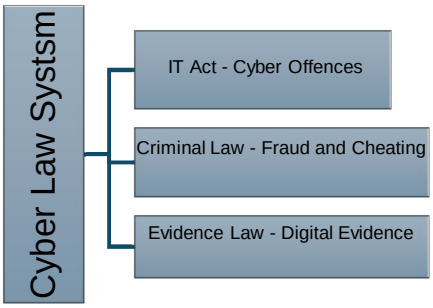
D. *Mule Bank Account Network*

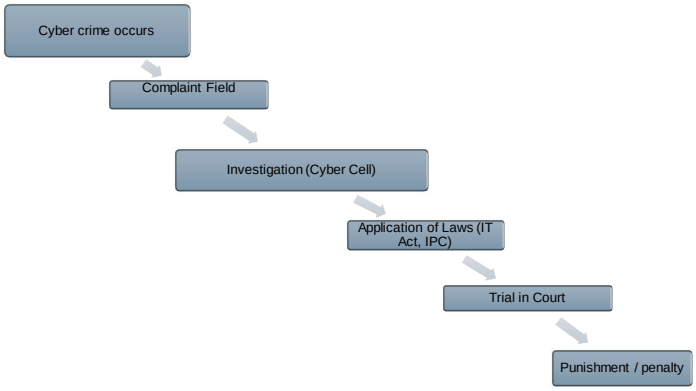
Organized groups used fake or rented bank accounts to transfer illegal funds, indicating the rise of structured cybercrime networks.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

E. Investment and AI-Based Fraud

Fake investment platforms and AI-driven scams resulted in massive financial losses, demonstrating the evolving nature of cyber threats.





Cyber Crime Control Process

Challenges in Cybercrime Legislation

1) Jurisdiction Issues: Difficulty in handling cross-border crimes
2) Technological Advancements: Laws become outdated quickly
3) Lack of Awareness: Citizens often unaware of legal remedies

4) Weak Enforcement: Limited technical expertise in law enforcement
5) Legal Gaps: Emerging threats like AI crimes and cryptocurrency fraud

VIII. SUGGESTIONS FOR IMPROVEMENT

1) Regular amendments to cyber laws
2) Strengthening enforcement agencies
3) Establishment of specialized cyber courts
4) Promotion of public awareness
5) International cooperation in cybercrime control
6) Integration of AI in cybercrime detection

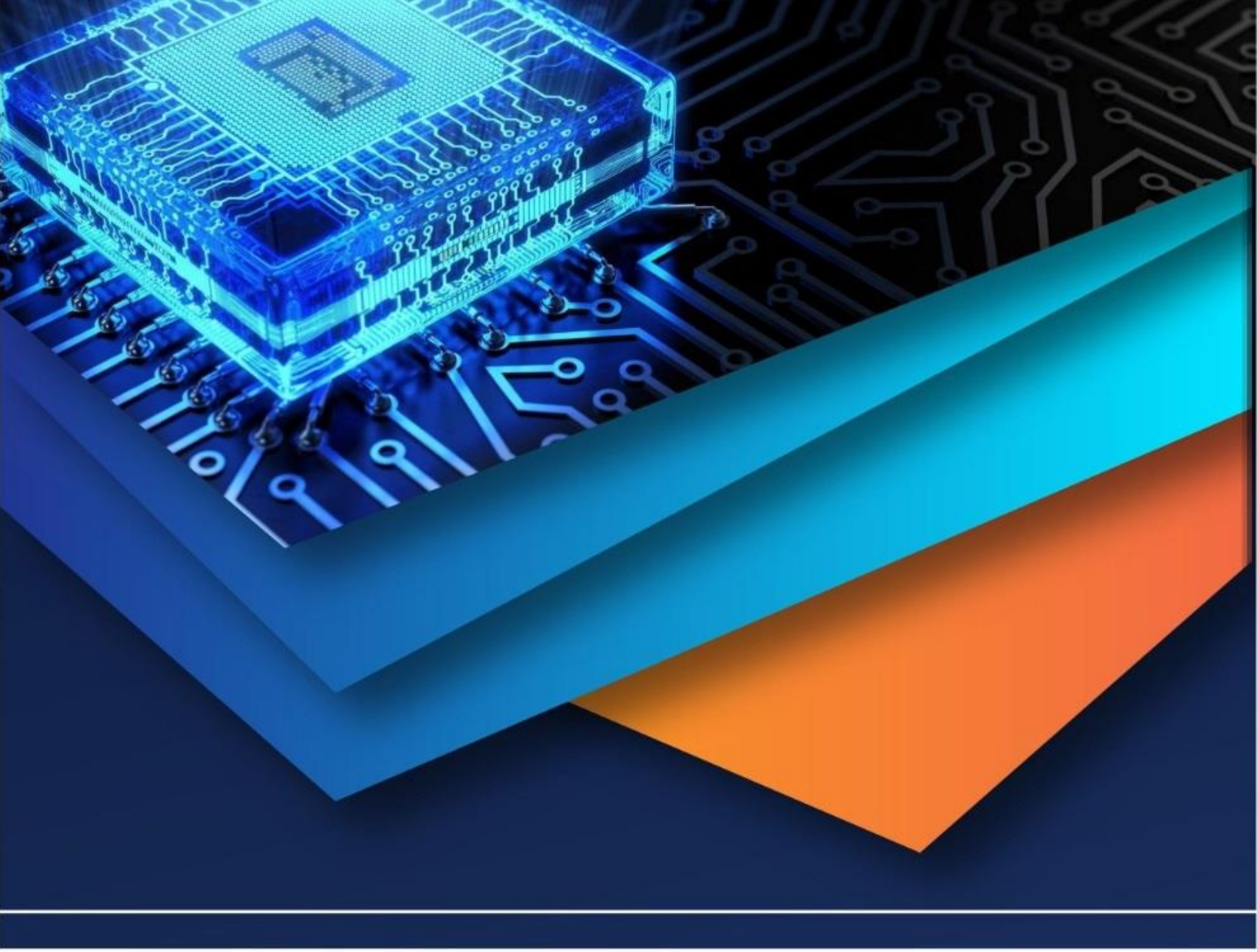
IX. CONCLUSION

Cybercrime represents a significant challenge in India's digital era. While the Information Technology Act, 2000, and related laws provide a strong foundation, rapid technological advancements require continuous updates and improvements.

Judicial interpretations and recent real-world cases highlight both the strengths and limitations of the current system. Effective cybercrime control depends on a combination of robust legislation, efficient enforcement, technological innovation, and public awareness.

REFERENCES

[1] Information Technology Act, 2000
[2] IT Amendment Act, 2008
[3] Digital Personal Data Protection Act, 2023
[4] Supreme Court Judgments (Shreya Singhal, Puttaswamy, etc.)
[5] Research papers on cyber law and cybercrime in India



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY