Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2026 7(1), 691–697

CYBER CRIME AND INDIAN CRIMINAL JUSTICE SYSTEM: A LEGISLATIVE PROTECTIVE APPROACHES

Mahendra Kumar [1], Dr. Upendra Grewal [2]

[1] Research Scholar, School of Law, IFTM University, Moradabad, India
[2] Assistant Professor, School of Law, IFTM University, Moradabad, India

Received 12 March 2026
Accepted 15 April 2026
Published 27 May 2026

Corresponding Author
Mahendra Kumar,
mahendrakumar318@gmail.com

DOI
10.29121/shodhkosh.v7.i1.2026.8404

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

21st century is a world of advancement of information technology. With the advancement of technology a steep increase in the rate of cyber-crimes has been. In this digital and technology paced age, where Artificial Intelligence and Technology plays a significant role in our daily lives, there is a growing necessity of establishing laws to regulate the online world. Cyber-crime mainly involves activities that use internet and computers as a tool to extract private information of an individual either directly or indirectly and disclosing it on online platforms without the person's consent or illegally with the aim of degrading the reputation or causing mental or physical harm.

As India progresses with its "Digital India" initiative, robust legal frameworks are essential for national and individual protection. Judicial decisions, particularly concerning the Information Technology Act, 2000, illuminate the practical application of cyber laws. Courts have affirmed constitutional protections, including the right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution, within the digital sphere. So the study examines the legal framework established by the Indian government to combat these cyber threats, including the Information Technology Act, 2000, and relevant amendments. The paper also highlights the challenges and shortcomings faced in prosecuting cybercrimes and presents recent high-profile cases as illustrative examples.

Keywords: Information Technology Act, Cyber Crime, Cyber Security, Judicial Interpretation, Cyber Law and Legislative Safeguards in Cyberspace

1. INTRODUCTION

The Internet has developed into an essential part of contemporary life. The emergence of technology has given them the chance to expand their skills and play to their strengths. Because of the world's fast modernization, cybercrime is a criminal activity carried out via computers, the internet, or other similar technologies—is a contemporary and widespread problem. In India, where thieves take advantage of the anonymity offered by technology, it is becoming a bigger menace. Cybercrime includes both standard online crimes and a broad spectrum of illicit behaviours, such as cyber terrorism, cyber stalking, email spoofing, cyber pornography, and cyber-defamation.

Today Information and Communication Technology (ICTs) is ubiquitous, and interest for Internet-empowered innovation has driven PC innovation empowered items. Presently vehicles, structures, power dissemination, transportation, military administrations, coordination's of society are altogether subject to Information and Communication Technology. Mobile innovation, Internet, distributed computing and an advance in systems administration through fourth and fifth era innovation has welcomed everything on the laptop[1].

India has seen an unparalleled surge in cybercrimes, which range from financial fraud and data breaches to cyber terrorism, cyber bullying, and online harassment. These crimes put people's privacy, financial security, and mental health at considerable risk, endangering national security. India has implemented a comprehensive legal framework, including the Indian Penal Code (IPC), the Information Technology Act of 2000, and other pertinent laws and regulations, to counter this rising danger. The complexity of cybercriminals, the requirement for extradition agreements and international collaboration, and the deficiency of cyber forensic skills within law enforcement agencies are some of the obstacles to successfully prosecuting cybercrimes within Indian jurisdiction.

The study suggests a multipronged strategy to improve India's response to cybercrime, which includes bolstering the current legislative framework, modifying it to address changing threats, and improving cyber forensic skills inside law enforcement organizations. It also highlights how crucial it is to raise awareness of cyber security issues among people and organizations, encourage global cooperation through agreements and partnerships, and highlight public-private partnerships as a crucial means of strengthening cyber security protocols and enhancing incident response.

What is Cyber Crime?

There is no exhaustive definition of cyber-crimes. It could cover activities which basically offend the human sensibilities, for example, hacking and child pornography. Cyber-crimes may include any criminal act dealing with computers and Internet. This may also include traditional crimes committed through Internet, like Internet frauds, when the computers and internet are used as tools to commit an act which is otherwise an offence. Cybercrimes can be defined as:

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones" [2].

A broad definition would be any crime committed that involves the use of a computer. In the current times, this would mean just about every crime committed, should a criminal use a computer to keep track of robberies he has committed or the drugs he has sold. [3]

A computer crime defined by the U S department of Justice's "As an illegal act requiring knowledge of computer Technology for its perpetration, investigation or prosecution". However, the definition is not exhaustive as there are many acts, which can be called abusive activities concerning the computer but they are often not clearly illegal. Moreover, most of the cyber-crimes are committed via internet but the definition has no reference to it.

Cyber-crimes can be plainly defined as "Crimes directed at a computer or computer system" But the complex nature of cyber-crimes cannot be sufficiently expressed in such simple and limited term[4]

The Organization for Economic Co-operation and Development (OECD) recommended the working definition of cybercrime "computer related crime is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data." [5]

Cybercrimes involves illegal activities carried out using computers, networks, or the internet. Some common types include: [6]

- Hacking and Unauthorized Access – Breaking into computer systems and databases.

- Identity Theft and Data Breaches – Misuse of personal data for illegal gains.
- Cyber Terrorism – Disrupting national security through digital means.
- Online Harassment and Cyber bullying – Defamation, threats, and stalking on social media.
- Deep fake and AI Crimes – Manipulating digital content for misinformation or fraud.

2. LEGAL FRAMEWORK FOR CYBERCRIME IN INDIA

2.1. INFORMATION TECHNOLOGY ACT, 2000 (IT ACT)

The cornerstone of cybercrime regulation in India is IT Act, 2000 which is amended in 2008 to address emerging threats. It is the most important law in India that deals with the digital crimes or cyber-crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) and which is recommended by the General Assembly of United Nations by a resolution dated 30 January 1997". [7]

Important provisions of the Information Technology (IT) Act 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company. [8]

Statutory provisions under the IT Act, 2000 are as follows:

1) **Section 66: Hacking with computer system, data alteration etc:** Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking (up to 3 years imprisonment and/or fine up to ₹5 lakh).
2) **Section 66A: Sending offensive messages through any communication services:** (struck down in 2015 in Shreya Singhal v. Union of India[9] for violating free speech).
    - Any information or message sent through any communication services this is offensive or has threatening characters.
    - Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.
    - Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages.
3) **Section 66C: Identity theft:** Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime (up to 3 years imprisonment and/or fine up to ₹1 lakh).
4) **Section 66D: Cheating by personation by the use of computer's resources:** Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

5) **Section 66E- Privacy or violation:** Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.
6) **Section 67:** Publishing or transmitting obscene material electronically (up to 3 years for first offense, 5 years for subsequent offenses, with fines).
7) The IT Act also empowers authorities to intercept, monitor, and decrypt data under **Section 69** for national security and public order.

2.2. THE BHARATIYA NYAYA SANHITA, 2023

Introduces several new provisions related to cybercrimes:

1) **Section 163:** Identity theft, deepfake, and misuse of AI-based content.
2) **Section 198(3):** Cyberstalking, revenge porn, and cyberbullying.
3) **Section 222:** Cyber terrorism, fake news propagation, and IT infrastructure attacks.

2.3. BHARATIYA NAGARIK SURAKSHA SANHITA, 2023 (BNSS)–

The BNSS, 2023, modernizes criminal procedure, particularly in cybercrime investigations. Key provisions include:

1) **Section 176:** Digital evidence collection from social media and electronic records.
2) **Increased Detention Periods:** Cybercrime suspects can be detained for up to 90 days (previously 60 days).

2.4. BHARATIYA SAKSHYA ADHINIYAM, 2023

The **BSA, 2023,** modernizes the rules for admissibility of digital evidence:

1) **Section 61:** Recognizes digital evidence, including block chain-based records.
2) **Section 63(2):** Removes strict certification requirements under Section 65B (earlier mandatory).
3) **Section 64:** Allows courts to accept electronic evidence without **a certificate from the producer**, if verified by forensic experts.

2.5. PREVENTION OF MONEY LAUNDERING ACT, 2002

Prevention of Money Laundering Act, 2002 applied to cybercrimes involving financial transactions, like crypto currency fraud.

2.6. PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT (POCSO), 2012

Addresses cybercrimes like online child sexual abuse material (CSAM).

2.7. DATA PROTECTION LAWS

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** regulates data processing and imposes obligations on entities to prevent data breaches, indirectly supporting cybercrime prevention.

3. JUDICIAL APPROACHES TO CYBERCRIME

The intangible character of cybercrime, which is perpetrated in the virtual world of online, creates special difficulties for law enforcement. In contrast to traditional crimes, there is no physical presence, no physical evidence like fingerprints or eyewitnesses, and the methods, like sniffer dogs or forensic evidence, that are employed to discover traditional crimes are frequently unsuccessful. Conventional techniques of enquiry and gathering evidence are therefore insufficient in situations involving cybercrime.

The Supreme Court of India, in State of **Punjab and Others v. M/S Amritsar Beverages Ltd. and Others**[10] emphasized the complexity of dealing with cybercrimes and the gaps in the current legal framework. The court acknowledged that the internet has introduced new challenges that were not anticipated by traditional laws. It noted that while the Information Technology Act, 2000[11] (amended in 2008), provides for various types of cybercrimes and their corresponding penalties, it fails to address all the challenges faced by law enforcement officers, particularly those lacking the scientific expertise required to handle such cases.

The apex courts have further expanded the scope of IT Act provisions to cover new forms of cybercrime. For instance, in **State of Tamil Nadu v. Suhas Katti (2004)** [12], the first conviction under the IT Act, the court applied Section 67 to convict the accused for posting obscene content online, setting a precedent for tackling cyber obscenity.

A landmark case in India that drew significant attention to the issue of cybercrime is the **Shreya Singhal case,** [13] which addressed the constitutional validity of Section 66A of the Information Technology Act, 2000. The Supreme Court examined the clause in this case after two people were detained in Palghar, Mumbai, for allegedly making insulting Facebook posts regarding the closure of Mumbai after the passing of a political figure. The case brought up significant issues regarding how to strike a balance between internet content control and free expression. In the end, the Supreme Court declared that Section 66A was unconstitutional because it infringed upon the Indian Constitution's Article 19(1)(a) guarantee of freedom of speech and expression.

The Shreya Singhal case serves as an example of how the courts are changing their strategy to uphold basic rights in cyberspace while striking a balance with the necessity to control harmful online activity. The court's recognition of the value of cyberspace as a forum for free speech is reflected in the decision, which holds that people have the same constitutional rights online as they have outside. The vague and subjective language of the section—using terms like "grossly offensive" or "menacing"—was criticized for being overly broad and susceptible to misuse.

In its 2015 verdict, the Supreme Court held that Section 66A violated Article 19(1)(a) of the Constitution, which guarantees the right to freedom of speech and expression. The Court observed that the provision lacked procedural safeguards and had a chilling effect on free speech in the digital domain.

By declaring the section unconstitutional, the Court established a strong precedent for protecting online expression and limiting arbitrary state action in cyberspace. The judgment is often cited as a cornerstone in India's digital rights jurisprudence and has helped clarify the legal boundaries of permissible speech on the internet.

In **SMC Pneumatics v. Jogesh Kwatra (2001),** [14] the Delhi High Court addressed email defamation, recognizing the need to adapt traditional laws to digital contexts.

With addressing Data Privacy and it breaches in **Justice K.S. Puttaswamy v. Union of India (2017),** [15] the Supreme Court recognized the right to privacy as a fundamental right, influencing cybercrime cases involving unauthorized data access. Delivered by a nine-judge bench in 2017, the ruling came in the context of a challenge to the Aadhaar biometric identification system but has had far-reaching implications for data protection, digital surveillance, and individual autonomy. The Court laid down the principles of legality, necessity, and proportionality as the benchmarks for any action that interferes with an individual's privacy. This judgment significantly affects the operation of Section 69 of the IT Act, which empowers the government to intercept and monitor digital communications.

In the post-Puttaswamy legal environment, any surveillance or data collection must be justified by law and subject to reasonable procedural safeguards. Although the judgment does not directly strike down any provision of the IT Act, it has placed substantial constitutional constraints on the exercise of state surveillance powers and emphasized the need for a comprehensive data protection law. It has also strengthened the case for judicial review of executive actions in the digital domain.

In **Vishaka v. State of Rajasthan (1997),** [16] (though it is not a cybercrime case) the Supreme court's approach to workplace harassment influenced guidelines for addressing cyber harassment. The judiciary has taken a proactive stance in cases of cyber stalking, revenge porn, and online harassment. Under POCSO, courts have imposed stringent penalties for online child exploitation, as seen in cases involving CSAM distribution on platforms like WhatsApp or the dark web.

Cybercrimes often involve cross-border elements, complicating evidence collection. Indian courts have relied on **Mutual Legal Assistance Treaties (MLATs)** and provisions under the IT Act to secure electronic evidence. In **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)** [17] the court considered the requirement of a certificate under Section 65B and for the cybercrime prosecutions, reaffirmed strict compliance of certificate for digital evidence

In another case State **(NCT of Delhi) v. Anurag Singh Bains (2021)** [18] the court held that if the applicant harassed by Cyber stalking and online harassment than court should considered and recognized WhatsApp chats and social media posts as valid evidence.

4. RECENT DEVELOPMENTS AND JUDICIAL TRENDS

4.1. ADOPTION OF TECHNOLOGY IN COURTS

Justice in cybercrime matters is now more accessible because to the judiciary's adoption of e-courts and virtual hearings. In order to preserve electronic evidence, the Supreme Court's e-Committee has advocated for record digitization. To expedite proceedings, specialized cybercrime courts have been set up in Bengaluru, Delhi, and Mumbai.

4.2. FOCUS ON VICTIM-CENTRIC JUSTICE

In cases involving cyber bullying and revenge porn, courts have placed a strong emphasis on victim compensation and counseling. The Nirbhaya Framework has been expanded in several areas to include victims of cybercrime.

4.3. STRICTER PENALTIES FOR DATA BREACHES

Courts have begun holding businesses responsible for data breaches after the DPDP Act was put into effect, as evidenced by lawsuits involving e-commerce behemoths and finance platforms.

4.4. CRYPTO-RELATED CRIMES

Money-laundering laws have been used by the judiciary to combat the increase in cryptocurrency fraud. A proactive stance was demonstrated in 2024 when the Delhi High Court ordered the formation of a task group to look against crypto currency frauds.

5. CONCLUSION

The country's legal system has advanced significantly with the adoption of India's New Criminal Laws, which handle current issues like cybercrimes and adjust to the complexity of the digital era. These revisions aim to promote accountability, openness, and accessibility in the criminal justice system by superseding the Old Criminal Laws. The Information Technology Act, 2000 and its revisions have given criminals a legal foundation for a variety of cyber offences, such as online fraud, hacking, and data theft. However, as technology advances at an accelerated rate, new types of cybercrime emerge that the law cannot keep up with. In order to prevent online crimes, the Indian government must keep revising its cyber laws, making investments in cyber security infrastructure, enhancing digital literacy, and increasing public awareness.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Ajay. (2016). Challenges to Enforcement of Cyber-Crimes Laws and Policy. Journal of Internet and Information Systems, 6(1), 1–12. https://doi.org/10.5897/JIIS2015.0089

Anurag Singh v. State of NCT of Delhi, SLP (Crl.) No. 005023/2022.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, AIR 2020 SC 4908.

Curtis, P. A. (n.d.). Cyber Crime: The Next Challenges Faced by Law Enforcement, While Investigating Computer Crimes in the year 2000 and Beyond. Criminal Justice Institute.

Fatima, T. (2011). Cybercrime. Eastern Book Company.

Halder, D., and Jaishankar, K. (n.d.). Cyber Crimes Against Women in India. Sage Publications India Pvt. Ltd.

Information Technology Act, 2000, as Amended by the Information Technology (Amendment) Act, 2008.

Information Technology Act, 2000. (n.d.). In Wikipedia.

International Journal of Advanced Research in Computer Science and Software Engineering. (2015). [PDF article].

Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1; AIR 2017 SC 4161.

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

Singh, S. D., and Pandey, S. (2025). The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws. International Journal for Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.41627

SMC Pneumatics India Pvt. Ltd. v. Jogesh Kwatra, CS(OS) No. 1279/2001.

State of Punjab and Ors. v. M/S. Amritsar Beverages Ltd. and Ors., AIR 2006 SC 2820.

State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004.

Vishaka and Ors. v. State of Rajasthan and Ors., (1997) 6 SCC 241.

Vishwanathan, S. T. (2001). The Criminal Aspect in Cyber Law in the Indian Cyber Law. Bharat Law House.