Swami Vivekananda Advanced Journal for Research and Studies
Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X Pg. 73-77

Cyber Crime and It's Legal Framework in India

Dr. Kajal Verma
Assistant Professor, Meerut College Meerut ,
Uttar Pradesh

Accepted: 13/04/2026
Published: 14/04/2026 ***DOI: http://doi.org/10.5281/zenodo.19567093***

Abstract

Cyber-crime refers to illegal activities where computers, digital devices, or the internet are used as a tool or target. These crimes often involve unauthorized access, theft, misuse, or sharing of personal and sensitive information. They can lead to damage to reputation, psychological trauma, or physical harm to people. As technology advances and reliance on the internet grows, Cyber-crime has become more common. Women and children are particularly at risk, facing issues like cyber stalking, online harassment, voyeurism, impersonation, and cyber pornography. A major reason for this increasing threat is the lack of digital awareness, tech skills, and cyber-security training among many internet users.

In India, cyber-crime is a significant challenge for law enforcement because of its complicated and international nature. Although India was one of the first countries to adopt cyber laws with the Information Technology Act of 2000, the law has limited scope and does not adequately address many new forms of cyber-crime, especially those impacting women. Cyber-crime is not clearly defined under the IT Act, the IT (Amendment) Act of 2008, or any other Indian law. Instead, cyber-crimes are handled through various provisions in the IT Act, New criminal Laws (i.e., BNS,BNSS,BSA) and other relevant laws.

This paper looks at the changing cyber-security and cyber-crime laws in India, with a focus on laws related to cyber-crime, data protection, and information security. The study shows that India's current legal framework is inadequate due to insufficient coverage, poor implementation, lack of awareness, and overlapping regulations that create compliance issues. The paper highlights the legal framework for cyber-crime in India, its advantages and disadvantages.

Keywords: *Cyber security, IT Act, New Criminal Laws, Data privacy, Cyber-Crime*

Introduction

India is undergoing a swift digital revolution characterized by rising internet usage and a greater dependence on technology in a number of industries, including banking, healthcare, education, and government. Digitalization has increased productivity, accessibility, and creativity, but it has also increased the risk of cyber-attacks and data privacy violations. Cybercrimes like hacking, data breaches, online fraud, and identity theft are becoming more common and sophisticated, which presents significant difficulties for people, companies, and society as a whole. In order to protect sensitive data, safeguard vital information infrastructure, and maintain the stability of the digital ecosystem, a strong and flexible cyber-security legal framework is required at both the national and international levels.

The dynamic and quickly changing nature of digital technologies makes the creation and application of cyber-security laws extremely difficult. Artificial intelligence, blockchain, and quantum computing are examples of technological innovations that constantly change the landscape of cyber threats and frequently make current legal provisions outdated. As a result, there are gaps between legal frameworks and technological realities as legislation finds it difficult to keep up with new forms of cybercrime. The enforcement of cyber security laws is further undermined by the lack of technical know-how, awareness, and efficient coordination among legislators, law enforcement, and the judiciary. Legal effectiveness is further hampered by cyber-security's multi-jurisdictional nature, inconsistent implementation, overlapping regulations, and limited harmonization with international standards.

In addition to these more general issues, women have been disproportionately affected by cybercrime, making gender-based cyber violence a crucial problem. Women are more vulnerable to cyber stalking, online harassment, cyber pornography, impersonation, and other types of digital abuse due to the extensive use of social media and online communication platforms.[1] Victims are frequently discouraged from reporting crimes due to low digital literacy, ignorance, and social stigma, which gives offenders a degree of impunity. India passed the Information Technology Act, 2000 in response to these issues in order to combat cybercrimes and safeguard users, particularly women. But despite institutional and legislative efforts, cybercrimes are still on the rise, underscoring the critical need for stronger enforcement mechanisms, awareness campaigns, and legal reforms to effectively combat cybercrime and guarantee a safe online environment.

Concept of Cyber Crime

Cybercrime is the term used to describe illegal activity conducted through computers, digital devices, or contemporary telecommunication networks like the internet and mobile phones. These crimes are carried out with the criminal intent to cause direct or indirect financial, psychological, physical, or reputational harm to individuals or groups. An individual's right to privacy is frequently violated by cybercrimes, which frequently involve the unapproved access, misuse, disclosure, or publication of private and sensitive data. Through platforms like emails, social networking sites, online forums, and messaging apps, the internet is both a tool and a medium for committing such crimes. Notably, the term "cybercrime" is not defined explicitly in Indian laws, such as the Information Technology Act, 2000. Cybercrime, broadly speaking, refers to any illegal activity that uses computers or the internet as a tool, target, or facilitating medium.[2]

Legal framework for Cyber-crime in India

Cyber-crime specifically provided for under the Information Technology Act, 2000

Section 66C of the information Technology Act, 2000 describes the offence of 'Identity Theft', which involves the fraudulent or dishonest use of another individual's unique identification, like an Aadhar number or a bank account number, password, or a digital, electronic, or electronic accepted digital signatures. Our increasing dependency on electronic platforms has enabled the crime of 'Identity Theft' to attain significant importance as a cyber-crime that not only inflicts a loss but also an emotional loss to an accused. Section 66C has sought to provide information Technology users with a measure of security from the misuse of their information through information Technology in the cyber sphere, as an act of punishment that entails a term of either kind that extends to a maximum of three years including a fine that extends to one lakh rupees. In the case of Suhas Katti v. State of Tamil Nadu (2004)[3], although the main subject matter involved was the harassment and impersonation carried out through online means, the judgment emphasized the aspect of the infringement of another's identity on an online platform.

Section 66D specifically deals with the offence of "Cheating by Personation using Electronic Means." Cheating by personation through electronic means occurs in circumstances where a single individual misleads victims by pretending to be another person, or by knowingly substituting one individual with another in any online transactions and communication. This usually involves online fraud, phishing scams, impersonation, and other similar circumstances. In

[1] DEBRATI HALDER & K. JAISHANKAR, CYBER CRIMES AGAINST WOMEN IN INDIA

[2] Adv. Prashant Mali, IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1.

[3] CC No. 4680 of 2004

Shreya Singhal v Union of India (2015)[4] of India, the gravity of use of electronics for abuse was acknowledged by their Supreme Court in a way indirectly corroborating Section 66D's importance.

Section 66E of the Act revolves around the violation of privacy, i.e., electronic voyeurism. The act criminalizes the intentional capture, publication, or transmission of any image of the private parts of any person without their consent in situations that violate their privacy. The act applies neutrally to all genders and covers the provisions of the Indian Penal Code regarding voyeurism or obscenity. Keeping in mind the current trend of using smartphones or digital technology, this particular act plays an significant role in implementing the privacy of the human body in cyberspace, exposing offenders to prison sentences or fines up to two lakh rupees or both. State of West Bengal v. Animesh Boxi,[5] 2018 – Also known as the Revenge Porn case, in this case, a strong condemnation was given by court on non-consensual sharing of intimate images with a strict notion of punishment, aligning with Section 66E.

Section 66F, which deals with cyber terrorism and was introduced by the Information Technology Amendment Act of 2008, specifically protects against and penalises cyber terrorism. Cyber terrorism involves those who attempt to steal information through unlawful access to critical information infrastructure with an intention that disrupts and/or threatens national integrity, sovereignty, and/or security. This cyber terrorism was brought about because of growing apprehensions regarding cyber and national security, especially after the 11/26 terror strikes. Cyber terrorism is punishable by a lifetime sentence. Kasab v. State of Maharashtra[6], though not falling squarely within Section 66F, flagged the important role played by electronic evidence to show the growing relevance of cyber-related terrorism offences.

Hacking, although not specifically mentioned in any particular section in terms of its own, has specific provisions in Sections 43 and 66 of the IT Act. Section 43 and 66 are related to obtaining unauthorized access to computer systems and data theft, introducing viruses, and damaging computer resources. Section 43 provides compensation through a legal suit, and Section 66 provides punishment by imprisoning a guilty offender for a term extending to three years or a fine extending to five lakhs rupees.

Cyber Pornography and Obscenity: Nevertheless, the Information Technology Act lacks a clear and specific definition of the term "pornography," but the matter of "cyber pornography" embraces the provisions of the Information Technology Act that concern the offense of "obscenity" under Sections 67, 67A, and 67B. Under these sections, the act of publishing or transmitting or causing the transmission of "obscene in an electronic format" will amount to an offense. In the absence of an universally accepted definition of "pornography" and in the interest of mitigating the harm that "obscene matter" poses to the larger interest of the community at large, the courts will be guided by the tests for "obscenity." In the case of Avnish Bajaj v. The State (NCT of Delhi) (2008)[7], which is otherwise known as the 'Bazee.com case,' the Delhi High Court addressed the issue of intermediary liability with respect to the dissemination of 'obscene information,' as well as the extent of 'liability,' invoking the applicability of Section 67. The case is a landmark judgment in the realm of cyber obscenity.

Cyber-crime specifically provided for under Bhartiya Nyaya Sanhita,2023

The Indian Penal Code, 1860 was replaced by the Bharatiya Nyaya Sanhita, 2023 (BNS), which includes a number of clauses that either directly or indirectly deal with cybercrimes. The BNS supplements the Information Technology Act, 2000, which continues to be the main piece of legislation governing cyber offenses, by making acts carried out through electronic and digital means illegal, especially those involving deception, invasions of privacy, sexual offenses, threats to national security, or the distribution of illegal content. Online fraud, phishing scams, phony websites, and impersonation on digital platforms are all considered forms of cheating under Section 318. Cyber cheating is defined as dishonestly inducing the delivery of property or valuable security through emails, social media, or other computer resources. This strengthens the prosecution of online financial fraud in conjunction with Section 66D of the IT Act. Section 319 deals with cheating by personation, which covers pretending to be another person or substituting one person for another and extends to cyber impersonation, including fake social media profiles, fraudulent emails, or online impersonation of officials. Section 336 criminalizes forgery of electronic records, including the creation, alteration, or use of false digital documents with the intent to cause damage or support fraudulent claims, thereby addressing cyber fraud and document manipulation. Section 338 specifically targets forgery for the purpose of cheating, encompassing forgery of emails, online records, or electronic documents to deceive individuals or institutions, and works in tandem with IT Act provisions on data tampering and hacking. Section 354 criminalizes voyeurism, including the capturing, transmission, or publication of images of a person engaging in private acts without consent, making it directly applicable to cyber voyeurism, revenge porn, and unauthorized circulation of intimate images,

[4] AIR 2015 SC 1523
[5] Case No. GR:1587/17
[6] AIR 2012 SC 3565
[7] (2008) SCC ONLINE DEL 688

complementing Section 66E of the IT Act. Section 356 extends defamation to statements made through electronic means, covering online harassment, trolling, and reputation damage via social media, blogs, emails, and other digital platforms. Section 113 addresses act that threaten national security, including cyber-enabled terrorist activities, such as attacks on critical infrastructure, unauthorized access to government systems, or digital acts intended to create fear or disrupt public order, which aligns with Section 66F of the IT Act on cyber terrorism. Finally, Section 61 on criminal conspiracy covers conspiracies executed through electronic communication, encrypted messaging, and online coordination, allowing prosecution of cyber-crimes planned or facilitated digitally. Together, these provisions in the BNS provide a robust framework to complement the IT Act and strengthen legal responses to cyber offences in India.[8]

Cyber Crime under Key Indian Legislations

The Protection of Women from Domestic Violence Act, 2005, addresses cyber-related domestic violence. This includes online harassment, digital surveillance, emotional abuse, and economic abuse. Section 3 broadly defines domestic violence. It includes threats, harassment, non-consensual image sharing, and digital financial control. Sections 17 to 22 offer remedies such as protection orders, residence orders, monetary relief, custody orders, and compensation for cyber abuse. In *Hiral P. Harsora v. Kusum Narottamdas Harsora* (2016)[9], the Supreme Court recognised that digital harassment and online abuse fall within the ambit of domestic violence.

The Protection of Children from Sexual Offences Act, 2012 (POCSO) makes cyber sexual offenses against children illegal. Section 11 involves electronic harassment, online grooming, and sexual communication. Section 12 lays out penalties. Sections 13 to 15 focus on the creation, distribution, and possession of child sexual abuse material (CSAM). Sections 19, 21, 29, and 30 set out reporting obligations and penalize those who do not report. They also allow for presumptions of guilt in cyber cases. In *State of Maharashtra v. Rohit S.* (2019), the Bombay High Court held that sending sexually explicit material to minors online constitutes a punishable cyber offence under POCSO.

The Indecent Representation of Women (Prohibition) Act, 1986, bans indecent depictions of women in digital media. Section 2(c) defines what constitutes indecent representation. Section 3 prohibits indecent advertisements. Section 4 prevents the production and circulation of such content. Section 5 allows for the search and seizure of digital devices. Sections 6 and 7 outline penalties and corporate liability, holding online platforms and publishers accountable

Together, these laws, along with the Information Technology Act, 2000, and Bharatiya Nyaya Sanhita, 2023, create a strong framework to tackle cyber-crimes against women and children in India.

Investigation of Cyber-crime

Risks involved in the investigation of computer crimes are very real, and unlike other crimes, in cyber-crimes, the culprit is rarely present where the crime is being committed, thereby lowering the chances of detection. This is because computer crimes are committed through a virtual space that is unbound by national territory, so that if the culprit is based in a different place, there is no viable way to combat the problem through traditional investigation.

Considering the transnational nature of cyber offenses, the concept of Extra Territorial Jurisdiction also assumes prominence in the context of the territorial jurisprudence of India. Accordingly, the extension of the territorial jurisdiction of India has been provided under Section 1(5) of the Bharatiya Nyaya Sanhita, 2023, corresponding to Section 4 of the IPC. Such provision extends an extraterritorial effect to the offenses that are committed outside the territory of India against a computer located within the territory of India. The larger extension of the territorial jurisdiction and the securing of a wider territorial basis have been provided in the context of the Information Technology Act, 2000, particularly under Section 75. However, the efficacy of the aforesaid provision is subjected to the satisfaction of the condition that the commission of an act within the foreign territory would constitute an offence within that particular territory.

Cyber-crimes can be reported through the registration of the First Information Report under Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, being the codified version of Section 154 of the CrPC. The BNSS has recognized the notion of Zero FIR through the official version of the legislation, where the information can be reported irrespective of the jurisdictions involved. Moreover, information can also be furnished through electronic modes, subject to authentication.

The overall investigation process is governed by BNSS and some specific provisions of the IT Act. According to Section 78 of the IT Act, police officers not below the rank of Inspector can conduct investigations of cyber offences. Also, police officers of the same rank can conduct searches and seizures without a warrant in

[8] Piyush Mishra, Hoax calls to be made cognisable offence, situation sensitive: Aviation Minister, https://www.indiatoday.in/india/story/union-aviation-minister-ram-mohan-naidu-hoax-bomb-threat-callscognisable-offence-perpetrators

[9] AIR 2016 SC 4774

a public place, as prescribed in Section 80 of the IT Act. For gathering evidence from other jurisdictions located outside the country, MLAT, LR, and requests under Sections 112 and 113 of BNSS can be used. Thus, all of the legal provisions described help in the conduct of investigations of cyber offences committed in the country.[10]

Digital Arrest Fraud

A Growing Cyber Threat in India Digital arrest fraud is a new and complex type of cybercrime in India. It presents serious financial and personal risks to victims. In this scam, cybercriminals pretend to be law enforcement officials, like CBI, police, or ED officers, and falsely accuse people of being involved in crimes. They use phone or video calls to create urgency and fear, pushing victims to meet their demands.[11]

Scammers use caller ID spoofing to appear as real government officials. They reach out through WhatsApp, Skype, or other online platforms. Victims face intimidation from false accusations of serious crimes like drug trafficking or money laundering. Scammers present fake documents and setups that look like police stations. Often, victims are told to stay isolated on the call. During this time, scammers may use deepfake videos and fake arrest warrants to build trust. They usually demand immediate payment through gift cards, wire transfers, or cryptocurrency, making it hard to recover lost funds. The scammers may also steal personal information, such as Aadhaar and bank details, for identity theft.

Government Efforts - The Indian Cyber Crime Coordination Centre (I4C), part of the Ministry of Home Affairs, is actively working to stop digital arrest scams. Between January and April 2024, losses from these scams reached ₹120.30 crore. In partnership with Microsoft, I4C has blocked over 1,000 Skype IDs linked to the fraud and has run public awareness campaigns. Additionally, an inter-ministerial committee was created in May 2024 to tackle cross-border cybercrime, especially from Southeast Asian countries like Cambodia. Reporting Mechanism works like Victims can report incidents through the cybercrime helpline (1930), online at cybercrime.gov.in, or by reaching out to local police.

Conclusion

Cybercrime in India has quickly evolved with digitalization. It is now more sophisticated, widespread, and harmful to individuals, organizations, and society. Women and children are especially at risk for cyber threats like online harassment, sexual exploitation, identity theft, and digital stalking. New types of cyber fraud, such as digital arrest scams, show the clever tactics used by cybercriminals. Although India has a strong legal framework—including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Protection of Women from Domestic Violence Act, 2005, the POCSO Act, 2012, and the Indecent Representation of Women (Prohibition) Act, 1986—there are still challenges in enforcement, awareness, and adapting to new technologies.

The changing nature of cyberspace, along with the international reach of crimes and low digital literacy in some groups, makes it hard to prevent, detect, and prosecute cybercrime. Despite these challenges, programs like the Indian Cyber Crime Coordination Centre (I4C), task forces that include various ministries, and international partnerships show that the government is actively working to fight cybercrime and protect its citizens.

To improve India's cybersecurity, a multi-faceted approach is needed. This includes ongoing legal reforms, effective enforcement, public awareness campaigns, and upgrading skills among law enforcement. Only by working together can we reduce cybercrime, protect digital rights, and create a safe online environment for everyone, especially vulnerable groups like women and children.

****

[10] Cyber Crime Cases: Issues, Challenges & Solutions Available on -https://jajharkhand.in/wp-content/uploads/2025/02/Cyber-Crime-web.pdf

[11] Digital Arrest: An Emerging Cybercrime in India - INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES [ISSN 2581-5369] Volume 7 | Issue 6 2024