



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

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER CRIMES AGAINST INDIVIDUALS: LEGAL REMEDIES UNDER INDIAN LAW

- *Mudit Vikaram Singh*

INTRODUCTION

Computer do not commit crime.¹ However, the computer hand in hand with internet has given to birth to a new generation of crime. In such computer crime, the role of human hand is less while the major activities are carried out by the automated machines. While the Internet is the wonder gift of science to mankind, it has at same time become a haven for criminals. The manipulation of employees, the compromising of email, and the hacking of accounts and the increasing number of social media platforms are collectively giving a never before boost to the world of cyber-crime.² Not only this, the monetary gains or the crime produced in this filed have surpassed other crime, there was risking of life and limb or of reputation, but the increasing number of social media platforms and the ease to reach millions at the click of buttons has led to a cyber-crime economy.

Cybercrime may additionally usually be understood as an unlawful act wherein a laptop, conversation tool, or computer network is used to devote or facilitate an offence.³ Not like conventional crimes, cybercrimes can be committed remotely and can involve perpetrators, victims, digital proof, and service carriers placed in unique jurisdictions. Not like conventional

¹ Donn B. Parker, a retired guru, however, anticipates a day of “Automated Crime” when a software package will be available which when put to use will automatically select the victim anonymously commit the crime and remove the evidence of its commission from the computer. Donn B. Parker, “Automated Crime “ in Cyber crime

[International Conference Course Book] (Oceana Publications, Washington DC 1997).

² Web Crime statistics: Total complaints filed in 1993 (1.7 per day), it went up from a total of 971 (2.6 per day) in 1994 to 1494 in 1995, to 4322 in 1996, to 12,775 in 1997, to 47,000 in 1998 and to almost 1, 00,000 squarely with immense cyber security steps so much so that the cyber security market is anticipated to reach \$300 billion by 2024 (2019 Press Release by Global Market Insight Inc.)

³ National Cyber Crime Reporting Portal, Learn about Cybercrime, Government of India, <https://www.cybercrime.gov.in/Webform/CrimeCatDes.aspx>.

crimes, cybercrimes can be committed remotely and can contain perpetrators, sufferers, digital evidence, and carrier vendors placed in one-of-a-kind jurisdictions.

In India, cybercrime is broadly speaking addressed via the information Technology Act, 2000 (“IT Act”), at the side of the Bharatiya Nyaya Sanhita, 2023 (“BNS”), Bharatiya Nagarik Suraksha Sanhita, 2023 (“BNSS”), Bharatiya Sakshya Adhiniyam, 2023 (“BSA”), and the data era (intermediary hints and virtual Media Ethics Code) guidelines, 2021 (“IT regulations”)⁴.

COMMON CYBER CRIMES AGAINST INDIVIDUALS

Cybercrime in opposition to individuals can take several bureaucracy. Online monetary fraud consists of phishing, fraudulent banking transactions, impersonation, and deceptive digital fee schemes. Identity-related offences might also contain the misuse of passwords, electronic signatures, or other unique identity functions. The IT Act specially addresses identification theft below phase 66C and cheating via personation the usage of a computer aid under section 66D.⁵

Privacy-related offences are also extensive. Section 66E of the IT Act penalizes the intentional or understanding seize, publication, or transmission of photos of a person's non-public place without consent, concern to the statutory requirements.⁶ Similarly, Sections 67 and 67A deal with the publication or transmission of obscene and sexually explicit material in electronic form⁷.

Cyberstalking, threats, dishonest, forgery, intimidation, and different conduct may additionally moreover attract provisions of the BNS. The BNS acknowledges digital information in provisions coping with offences which include forgery, making the cutting-edge criminal regulation relevant to behavior involving digital documents and digital information.⁸

⁴ Information Technology Act, No. 21 of 2000, **India Code**, <https://www.indiacode.nic.in/>; Bharatiya Nyaya Sanhita, No. 45 of 2023, **India Code**, <https://www.indiacode.nic.in/>; Bharatiya Sakshya Adhiniyam, No. 47 of 2023, **India Code**, <https://www.indiacode.nic.in/>

⁵ Information Technology Act, No. 21 of 2000, sec 66C–66D, India Code, India Code, <https://www.indiacode.nic.in/>.

⁶ Id. sec 66E.

⁷ Id. sec 67, 67A.

⁸ Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 335–337, India Code, India Code, <https://www.indiacode.nic.in/>. The BNS came into force on July 1, 2024.

LEGAL REMEDIES UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act stays the predominant law specifically handling laptop-related offences in India. Section 43 presents for compensation in situations regarding unauthorized get entry to, downloading, introducing contaminants, adverse laptop structures, or disrupting pc networks. Where such conduct is finished dishonestly or fraudulently, section 66 presents crook liability.⁹

For individuals whose credentials had been misused, section 66C is especially applicable. It covers fraudulent or cheating use of another character's digital signature, password, or other unique identification function. Section 66D addresses dishonest via personation thru a conversation device or pc aid.¹⁰

Sufferers may additionally have treatments concerning privacy and sexually express cloth underneath Sections 66E, sixty seven, and 67A. These provisions are particularly relevant where illegal digital content material is circulated via web sites, messaging services, or social-media platforms.

CONCLUSION

Cybercrime in opposition to individuals requires a coordinated prison reaction because a single incident may additionally involve criminal liability, privateness rights, economic loss, digital evidence, and middleman responsibilities simultaneously. Indian regulation offers more than one remedies through the IT Act, BNS, BNSS, BSA, and the IT policies.

For victims, well timed reporting and cautious upkeep of evidence are specifically vital. The country wide Cyber Crime Reporting Portal and helpline 1930 offer critical mechanisms for reporting cyber offences, whilst crook court cases and other legal remedies may also comply with relying upon the character of the offence. As era keeps to adapt, effective enforcement will depend no longer most effective on noticeable criminal provisions but also on technically sound investigation, dependable digital evidence, and powerful cooperation amongst victims, regulation-enforcement agencies, financial institutions, and digital structures.

⁹ Information Technology Act, No. 21 of 2000, sec 43, 66, India Code, <https://www.indiacode.nic.in/>.

¹⁰ Id. sec 66C–66D.