

CYBER CRIME

REMEDIES UNDER THE IT ACT

Indian Legal Perspective — IT Act, 2000 (Amended 2008)

Bhartiya Nyaya Sanhita (BNS), 2023 & DPDP Act, 2023

Presented by Advocate Vibhav Srivastava
Srinagar, 3rd April 2026



WHAT IS CYBERCRIME?



Cybercrime refers to any criminal activity involving a computer, network, or network-connected device — targeting individuals, organizations, or governments to cause financial, reputational, or national harm.



Narrow Sense

(Computer Crime)

Crimes directly targeting computer systems, networks, and data — e.g., hacking, malware, unauthorized access.



Broader Sense

(Computer-Related Crime)

Crimes facilitated through digital means — e.g., online fraud, cyberstalking, identity theft, cyberterrorism.

LEGAL FRAMEWORK IN INDIA



IT Act, 2000 (Amended 2008)

Primary legislation governing cybercrimes, digital signatures, and electronic transactions in India.

Bhartiya Nyaya Sanhita (BNS), 2023

Replaced IPC; covers online defamation, fraud, threats, and stalking in the digital space.

DPDP Act, 2023

Digital Personal Data Protection Act — governs consent, data processing and fiduciary obligations of organizations.

CERT-In Guidelines

India's nodal cybersecurity body mandates reporting of cyber incidents within 6 hours for critical categories.

CATEGORIES OF CYBERCRIMES UNDER IT ACT



Hacking

Unauthorized access or control over digital systems to manipulate or steal data. (S.66)



Identity Theft

Misuse of Aadhaar, PAN, or bank details for illegal purposes. (S.66C, 66D)



Cyberstalking

Repeated online harassment, monitoring, or intimidation of a person. (S.67 (only if Obscene content involved), BNS S.78)



Online Fraud

Phishing, fake websites, or scam emails to steal OTPs or financial data. (S.66D)



Cyberterrorism

Attacks on critical infrastructure threatening national security. (S.66F)

HACKING & UNAUTHORIZED ACCESS



What Constitutes Hacking?

- Gaining unauthorized access to a computer system
- Modifying, destroying, or stealing data without permission
- Installing malware or spyware on devices
- Bypassing security systems or password protections

Legal Provision

Section 66 — IT Act, 2000

Also: Section 379/380, BNS (theft of data)

Remedies & Penalty

- Imprisonment up to 3 years
- Fine up to ₹5 Lakh, or both
- Compensation under Section 43A for negligent data breach

IDENTITY THEFT & ONLINE IMPERSONATION



Identity Theft — Section 66C of IT ACT

Fraudulently using someone's password, digital signature, or unique identification such as Aadhaar or PAN without their consent.

Online Impersonation — Section 66D OF IT ACT

Cheating by personating another person through computer resource or communication device for financial gain or defamation.

Penalty for both offences: Imprisonment up to 3 years | Fine up to ₹1 Lakh | Or both

CYBERSTALKING & ONLINE HARASSMENT



Persistent online behavior aimed at monitoring, threatening, intimidating, or harassing a person through electronic communication — including social media, email, or messaging platforms.

Section 67, IT Act

Publishing or transmitting obscene or offensive content electronically targeting a victim.

Penalty: 1st offence: 3 yrs + ₹5L fine
 2nd offence: 5 yrs + ₹10L fine

Section 78, BNS 2023

Stalking including cyberstalking — following, monitoring, or repeatedly contacting a person despite disinterest (where the offence involves use of computer resources).

Penalty: 1st offence: 3 yrs imprisonment
 2nd offence: 5 yrs imprisonment

DATA PROTECTION & CORPORATE NEGLIGENCE



Section 43A — IT Act, 2000

When a body corporate fails to use reasonable security practices to protect Sensitive Personal Data (SPDI) and such negligence causes wrongful gain or loss — the company is liable to pay compensation to the affected person.

DPDP Act, 2023 — Key Update

- Organizations (Data Fiduciaries) must obtain explicit consent before processing personal data
- Data breaches must be reported to Data Protection Board and affected individuals promptly
- Penalty for data breach: up to ₹250 Crore per instance
- Every citizen has the right to access, correct, and erase their personal data

CYBERTERRORISM — SECTION 66F



Section 66F — IT Act | Punishment: Life Imprisonment

Acts Constituting Cyberterrorism:

- ! Denying or causing denial of access to authorized computer users
- ! Penetrating computer systems without authorization to obtain restricted state or security information
- ! Introducing computer contaminants into critical systems (power grids, defence, banking, government databases)
- ! Any cyber activity threatening the unity, integrity, sovereignty, or security of India



Common Scam Methods

-  Fake emails/SMS mimicking banks, IRCTC, UIDAI
-  Fraudulent e-commerce or lottery websites
-  Fake job/investment offers via WhatsApp
-  OTP phishing calls posing as KYC agents
-  UPI payment scams using QR codes

Legal Provision

Section 66D — IT Act

Section 318/319 — BNS, 2023 (Cheating by personation where the offence involves use of computer resources.)

Penalty

Imprisonment up to 3 years

Fine up to ₹1 Lakh, or both

Report: cybercrime.gov.in | Helpline: 1930

ADJUDICATING OFFICER — CIVIL REMEDY



Section 46 — Power to Adjudicate

AO has authority to adjudicate any contravention of IT Act provisions and can order compensation up to ₹5 Crores.

Qualification of AO

Must be an officer not below the rank of Director to Government of India, or equivalent officer of State Government.

Section 47 — Factors for Compensation

AO must consider: (a) Amount of unfair advantage gained, (b) Loss caused to person, (c) Repetitive nature of default.

Section 64 — Recovery of Penalty

Penalty or compensation awarded shall be recovered as an arrear of land revenue — enforceable by the Revenue Department.

APPEALS & HIGHER REMEDIES



1

Adjudicating Officer (AO)

Section 46 — Original Complaint

2

TDSAT

Section 48 — Appeal from AO order

3

High Court

Section 62 — Second Appeal

4

Supreme Court

Constitutional Remedy (Article 136)

S.60: Limitation Act 1963 applies | S.61: Civil Court jurisdiction is barred for IT Act contraventions

HOW TO REPORT A CYBERCRIME



1

Gather Evidence

Screenshots, emails, messages, transaction records, URLs, and logs with timestamps. Do NOT delete anything.

2

Report Online

File complaint at cybercrime.gov.in or call helpline 1930. Available 24x7 for financial fraud, women/child safety crimes.

3

File FIR at Police

Visit the nearest Cyber Crime Cell or Police Station. Carry ID proof and all evidence. Request copy of FIR.

4

Seek Legal Advice

Consult a cyber law specialist for civil compensation under Sections 43/43A of IT Act or criminal prosecution.

CYBER INSURANCE AS A REMEDY



Cyber insurance provides financial protection against losses from cyber incidents — including data breaches, ransomware attacks, cyber extortion, and business interruption. Increasingly important under DPDP Act 2023.

First-Party Coverage

- ✓ Direct financial losses from cyber fraud
- ✓ Business interruption due to cyberattacks
- ✓ Data recovery and forensic investigation costs
- ✓ Ransomware payments (where legally permissible)

Third-Party Coverage

- ✓ Legal liability to customers/partners from breach
- ✓ Regulatory fines and penalties (DPDP, CERT-In)
- ✓ Notification costs to affected data subjects
- ✓ PR and crisis management expenses

KEY TAKEAWAYS



IT Act 2000 (A2008) + BNS 2023 + DPDP Act 2023 form India's cyber law framework.



Civil remedies via Adjudicating Officer; criminal prosecution via court and police.



DPDP Act 2023 introduces penalties up to ₹250 Cr for data breaches by organizations.



Always preserve digital evidence before reporting — it is crucial for investigation.



Cyber insurance is a growing financial remedy for both individuals and corporate entities.

THANKYOU