

Understanding Cyber Crimes and the Information Technology Act, 2000

Cyber Law · Cyber Crimes

Legal Framework

The Information Technology Act, 2000 is India's primary legislation dealing with cybercrime and electronic commerce. It provides legal recognition for electronic records and digital signatures, and creates offences for unauthorised access, data theft, and other computer-related crimes.

Common Cyber Offences

- **Section 43** — civil liability for unauthorised access to a computer system, introducing viruses, or damaging data.
- **Section 66** — computer-related offences, covering hacking and data theft, with criminal liability.
- **Section 66C** — identity theft, including fraudulent use of another person's electronic signature, password or unique identification.
- **Section 66D** — cheating by personation using a computer resource (e.g. phishing).
- **Section 67** — publishing or transmitting obscene material in electronic form.

Key Case Reference

Shreya Singhal v. Union of India (2015) — the Supreme Court struck down Section 66A of the IT Act (which criminalised sending 'offensive' messages online) as unconstitutionally vague and a disproportionate restriction on free speech.

Staying Safe: Practical Awareness

- Never share OTPs, passwords, or banking credentials over phone or email, even to callers claiming to be bank officials.
- Report cybercrime promptly at the National Cyber Crime Reporting Portal (cybercrime.gov.in) or the nearest police station.
- Preserve evidence — screenshots, transaction IDs, and message headers — before reporting.