

## **Information Technology Act, 2000**

The Information Technology Act, 2000 (IT Act) was enacted to provide legal recognition to electronic records, digital signatures, and electronic commerce. It also defines penalties and punishments for a wide range of cybercrimes. The Act regulates activities relating to unauthorized access, data theft, hacking, cyber fraud, online abuse, privacy violations, publication of illegal content, and cyberterrorism. Over the years, the Act has been amended to address emerging challenges in cyberspace and improve safeguards for individuals, organizations, and national security.

- **Section 67 – Publishing or transmitting obscene material in electronic form**

This section prohibits the publication or transmission of obscene or sexually inappropriate content online. Punishment includes imprisonment of up to 3 years and/or fine for the first offence, and

up to 5 years for subsequent offences.

- **Section 67A – Publishing or transmitting sexually explicit material**

This section applies to more sexually explicit or graphic content compared to Section 67. The punishment is stricter due to the nature of the material.

- **Section 67B – Child sexually explicit content**

This section prohibits creating, transmitting, searching for, collecting, or distributing sexual content involving children. It is one of the most serious offences under the IT Act and carries stringent punishment, including imprisonment and heavy fines.

- **Section 66A – Sending offensive messages through communication services**

This section formerly criminalized sending offensive or menacing messages online. However, the Supreme Court of India struck down Section 66A in 2015 for violating freedom of speech. It is no longer in force.

- **Section 66C – Identity theft**

This section penalizes the fraudulent use of another person's digital identity, including passwords, digital signatures, and biometric information. It protects individuals from impersonation and data misuse.

- **Section 66E – Violation of privacy**

This section prohibits capturing, publishing, or transmitting images of a person's private areas without consent. It protects individuals from online voyeurism and unauthorized sharing of intimate photographs.

- **Section 66F – Cyberterrorism**

Cyberterrorism involves using computer systems or networks to threaten the sovereignty, integrity, security or safety of the nation. It includes attacks on critical information infrastructure. The punishment can extend to life imprisonment.

- **Section 507 (Criminal intimidation by anonymous communication)**

This section applies when threats or intimidation are issued anonymously or with an attempt to hide the sender's identity. In cyber context, this includes

anonymous threats through social media, email and messaging platforms. It adds up to 2 extra years of imprisonment in addition to the punishment under criminal intimidation.

- **Section 420 (Cheating and dishonestly inducing delivery of property)**

Section 420 deals with cheating with the intention to gain property or money dishonestly. It applies to cyber fraud, phishing scams, financial scams, fake job offers, investment fraud and similar offences. Punishment can extend up to 7 years imprisonment along with a fine.

- **Section 43**

Section 43 deals with unauthorized access to computer systems. It applies when a person accesses, copies, downloads, disrupts or damages computer systems, networks, or data without permission. It also covers introducing malware, damaging databases, or denying access to users.

Unlike Section 66, Section 43 does not require proof of criminal intent; the act itself is punishable.

- **Section 383 – Definition of extortion**

Extortion occurs when a person intentionally puts another in fear of injury and dishonestly forces them to deliver money, property, or valuable security.

- **Section 384 – Punishment for extortion**

Provides imprisonment of up to 3 years, a fine, or both.

These sections apply strongly to cases such as online blackmail, ransom threats and sextortion.

- **Section 65**

Section 65 penalizes tampering with computer source code. It applies when a person intentionally conceals, destroys, alters or causes another to alter any computer source code required to be kept by law. This provision protects the integrity of legally maintained software and system code.

- **Section 120A – Criminal conspiracy**

Defined as an agreement between two or more persons to commit an illegal act.

- **Section 120B – Punishment for criminal conspiracy**

Punishment varies depending on the severity of the intended crime. If the conspiracy is linked to a serious offence, punishment can match the severity of the intended act.

- **Section 121 – Waging war against the State**

Covers acts that threaten the sovereignty or security of India. While traditionally physical, cyber activities aimed at destabilizing government or critical infrastructure may fall under this category. Punishment may include life imprisonment or death depending on the case.

## **Indian Penal Code, 1860**

- **Section 354D (Stalking including cyberstalking)**

Section 354D criminalizes stalking a woman physically or digitally. It includes repeatedly following, contacting or monitoring a woman's online activities despite clear disinterest.

Cyberstalking through social media, emails, or tracking tools falls under this provision. Punishment extends up to 3 years for the first conviction and up to 5 years for subsequent convictions.