

# Cyber Crime

# History

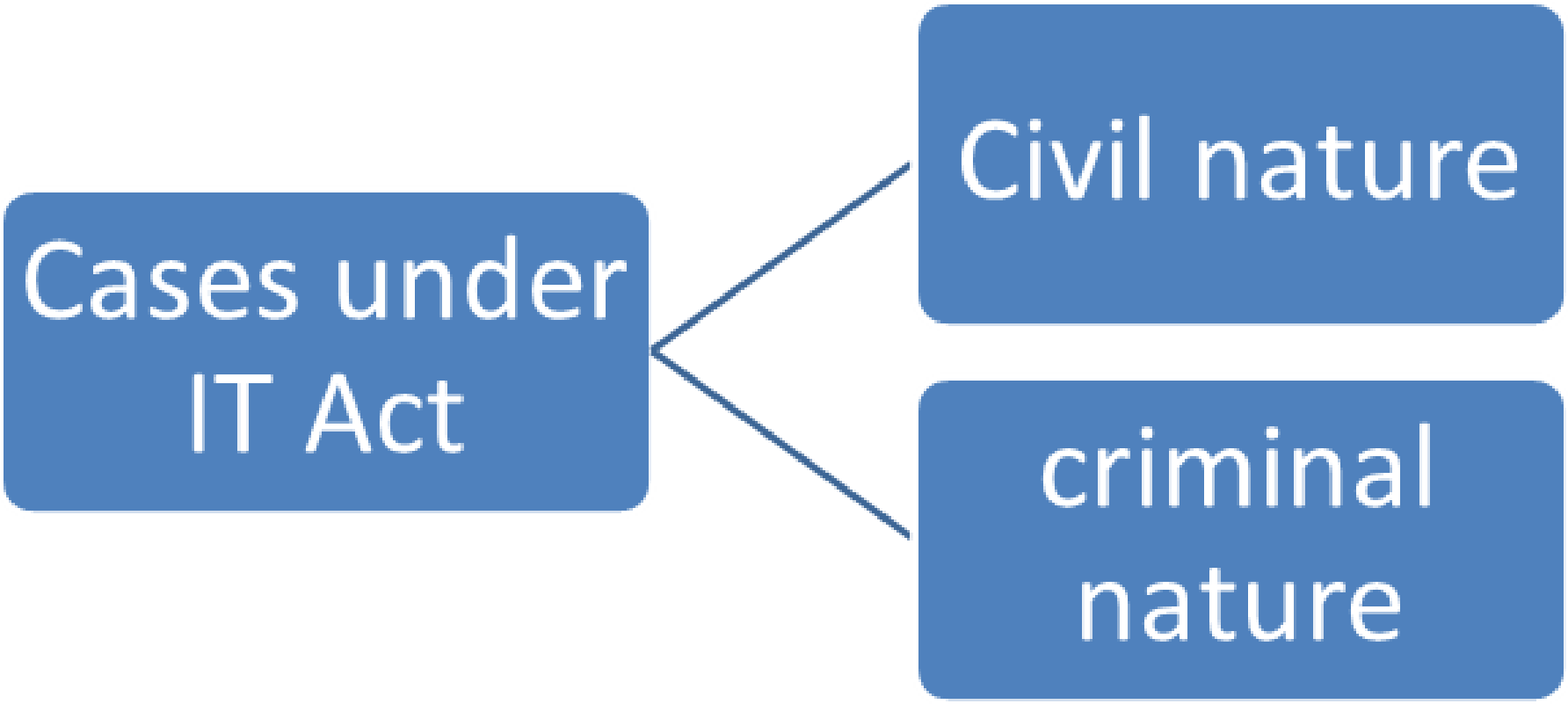
- 2nd Five year Plan
- Rajiv Gandhi Government
- Pre 2000
- 2000-2010
- 2010-2020
- Post 2020


X calls Y and abused over phone. Is it a cyber crime?



# Law

- IPC
- IT act-2000 & 2008
- IT rules 2011 & 2021


Cases under IT Act
Civil nature
criminal nature

**Short title, extent, commencement and application.—(*1) This Act may be called the Information Technology Act, 2000.***

*(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.*

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY Sl. No. Description of documents or transactions

1. A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881).

2. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882).
3. A trust as defined in section 3 of the Indian Trust Act, 1882 (2 of 1882).
4. A will as defined in clause (*h) of section 2 of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called.*
5. Any contract for the sale or conveyance of immovable property or any interest in such property.

# IT ACT, 2000 –MAJOR PROVISIONS



- **Extends to the whole of India**

(Section 1(2))

- **Electronic contracts will be legally valid**

(Section 10A )

- **Legal recognition of digital signatures**

(Section 3 )

- **Security procedure for electronic records and digital signature**

(Section 16 )

- **Appointment of Controller of Certifying Authorities to license and regulate the working of *Certifying* Authorities**

(Section 17 of the Act for purposes of the IT Act )

**43. [Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–**

(a) accesses or secures access to such computer, computer system or computer network 7[or computer resource]; UNAUTHORISED ACCESS

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; DATA THEFT

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; VIRUS

- (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; DAMAGE
- (e) disrupts or causes disruption of any computer, computer system or computer network; E-Mail Bombing
- (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; DoS Attack

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; ABETMENT

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network; INTERNET THEFT

1[(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; DATA DIDLING

(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;] SOURCE CODE

43A. Compensation for failure to protect data.– Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

46 Power to adjudicate. -

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, [51] [direction or order made thereunder which renders him liable to pay penalty or compensation] the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

[52] [(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore: Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court.]

(2) The adjudicating officer shall, after giving the person referred to in sub- section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

# IT ACT, 2000 –MAJOR PROVISIONS (Contd..)



- Certifying Authorities to get License from the Controller to issue digital signature certificates

(Section 2)

- Various types of computer crimes defined and stringent penalties provided under the Act

- Appointment of Adjudicating Officer for holding inquiries under the Act

(Section 46)

- Establishment of Cyber Regulatory Appellate Tribunal under the Act

(Section 48 )

# IT ACT, 2000 –MAJOR PROVISIONS



- Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court

(Section 57)

- Appeal from order of Cyber Appellate Tribunal to High Court

(Section 62)

- Act to apply for offences or contraventions committed outside India

(Section 75 (1) and (2))

- Network service providers not to be liable in certain cases

- Power of police officers and other officers to enter into any public place and search and arrest without warrant

(Section 80)

- Constitution of Cyber Regulations Advisory Committee to advise the Central Government and the Controller

(Section 88)

**65. Tampering with computer source documents.– Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.**

*Explanation.–For the purposes of this section, ―computer source code‖ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.*

**66. Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.**

*(a) the word —dishonestly‖ shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);*

"Dishonestly".--Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

*(b) the word —fraudulently‖ shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).*

"Fraudulently".--A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

66B. Punishment for dishonestly receiving stolen computer resource or communication device.–Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66C. Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D. Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E. Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

**66F. Punishment for cyber terrorism.–(*1) Whoever,–***

*(A)with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by– DOS Attack, Virus or Unauthorised Access.*

*(B)knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,*

commits the offence of cyber terrorism.

67. Punishment for publishing or transmitting obscene material in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

**67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.–Whoever,–**

*(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or*

*(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or*

*(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or*

*(d) facilitates abusing children online, or*

*(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,*

**67C. Preservation and retention of information by intermediaries.–(*1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.***

*(2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.]*

# BAZEE.COM

- An obscene MMS video was listed for sale on the website www.bazeee.com (now www.ebay.in) ("**Website**"). Though the Website had requisite filters to detect such listings, this listing was not tracked.
- The item was first listed on the evening of November 27, 2004 on the Website and deactivated only two days later i.e. on 29 November, 2004 after a complaint was lodged. In the meantime, a few sales took place through the Website.
- Upon investigation by the Crime Branch of Delhi, Ravi Raj, Avnish Bajaj, the managing director of the Website, and Sharat Digumarti, the manager of the Website, were held responsible for handling the content on the Website. They were listed as the accused on the charge sheet.

- Section 292 of the IPC deals with obscenity, and states that a figure or any object shall be deemed to be obscene if it is lascivious or appeals to the prurient interests such as to tend to deprave and corrupt a person. Further, the section makes it an offence to distribute, import, export, exhibit, advertise, etc. obscene content by means of traditional *print* media
- Section 294 of the IPC makes it an offence to do any obscene acts, or utter obscene words or songs in public places to the annoyance of others.
- Section 67 of the IT Act makes it an offence to publish or transmit obscene content in *electronic* form.
- Thus, the difference between Section 292 of the IPC and Section 67 of the IT Act is that while the latter criminalizes the transmission of obscene content by electronic means, the former criminalizes the dissemination of obscene content through conventional print media, such as through writings, drawings, books or pamphlets

# SECTION 85 IN THE INFORMATION TECHNOLOGY ACT, 2000

- **Offences by companies**.–(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

- Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

- **Section 79 of the IT Act** provides **immunity to intermediaries (for example, websites like Facebook) for any illegal content posted by third parties**.
- Under this section and the Information Technology (**Intermediaries Guidelines**) 2011, if an intermediary receives **'actual knowledge' of any illegal content posted on it, it is obligated to remove such content within 36 hours**.
- On failing to do so, the intermediary will lose its immunity from being sued. Illegal content under this section is much broader than that under Section 69A. It can include, for example, content that is offensive, obscene or defamatory.

- In the case of Section 79, the court upheld its validity, but with a few changes. Formerly, the 'actual knowledge' received by an intermediary under this section could come from anywhere, be it the government, a court, an NGO or a person. For example, a Facebook user reporting offensive content will be taken as giving Facebook 'actual knowledge', imposing the obligation to remove the offending content within 36 hours. **The court changed this and interpreted 'actual knowledge' to be received only when the takedown request is accompanied by court order or government direction**. If on receiving a court order, the intermediary fails to remove the content within 36 hours, then it will lose the immunity granted to it under

# Shreya Singhal Case

1

Section 66A

2

Section 69A

3

Section 79

# Supreme Court strikes down Sec 66A of IT Act

Provides power to arrest a person for posting allegedly 'offensive' content on websites

**Punishment: Up to 3 years in jail**

> The public's right to know is directly affected by section 66A of the IT Act
>
> –Supreme Court

## The Track

**2012:** First PIL filed by law student Shreya Singhal seeking amendment in Section 66A, after two girls- Shaheen Dhada and Rinu Shrinivasan were arrested in Palghar in Thane district as one of them posted a comment against the shutdown in Mumbai following Shiv Sena leader Bal Thackeray's death and the other 'liked' it.

**May 16, 2013:** Apex court advisory- a person, accused of posting objectionable comments on social networking sites, can not be arrested without police getting permission from senior officers like IG or DCP

**February 26, 2015:** Apex court reserves its judgement in the matter

**March 18, 2015:** A boy arrested for allegedly posting on Facebook objectionable comments against senior Samajwadi Party leader Azam Khan



## To remain enforced with certain restrictions

**Section 69A:** Provides power to issue directions to block public access of any information through any computer resource

**Section 79:** Provides for exemption from liability of intermediary in certain cases

PTI GRAPHICS


MOBILE NETWORK
FIXED NETWORK
NEXT GENERATION NETWORK
LAWFUL INTERCEPTION
2G
2G NETWORK
3G
3G NETWORK
4G
4G NETWORK
INTERCEPTION
GATHERING
STRONG
ANALYSING
MONITORING

**1885:** The Indian Telegraph Act remains one of the major laws regulating government monitoring of information today, along with the Information Technology Act, 2000. The British-era law allowed the Raj to control and restrain telegraph communications during their rule. Section 5 of the Act allows both central and state governments to intercept messages 1) in "public emergency" or in the interest of "public safety" and 2) in interest of sovereignty and integrity of India, security of the State, friendly relations with foreign states, public order, and prevention of incitement to the commission of offence. It also creates a Review Committee to oversee interception orders.

# SECTION 69 IT ACT

- 69. **Power to issue directions for interception or monitoring or decryption of any information through any computer resource**.– (1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

•**Rule 4 of the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009** provides that 'the competent authority may authorise an agency of the Government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose specified in sub-section (1) of Section 69 of the Act'.

- Each case of interception, monitoring, decryption is to be approved by the competent authority i.e. **Union Home secretary**. These powers are also available to the competent authority in the State governments as per IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.

- **69A. Power to issue directions for blocking for public access of any information through any computer resource**.–(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, **direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource**.

- **69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security**.–(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise **any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource**.
- (2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

- 72. **Penalty for Breach of confidentiality and privacy**.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

- 72A**. Punishment for disclosure of information in breach of lawful contract**.–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.]

# ATTEMPT OF CYBER CRIME

- 84-C : Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

**DIGITAL SIGNATURES MAKE IT POSSIBLE TO IDENTIFY SPECIFIC DOCUMENTS, WHEREAS ESIGNATURES DEMONSTRATE THE INTENT OF A SIGNATORY TO BE LEGALLY BOUND BY THE TERMS WITHIN A SPECIFIC DOCUMENT.**

# ELECTRONIC SIGNATURES

# DIGITAL SIGNATURES

## Overview



**An electronic signature** is a digital form of a wet ink signature. It is **100% legal**ly binding and secure.



**Digital signatures** rely on the Public Key infrastructure. They can be verified which provides authenticity to the document.

**Electronic signatures** are easy to implement into existing processes and are considered equivalent to handwritten signatures.

**Digital signatures** include the identity of the signer in terms of a **digital signing certificate** issued to the signer by **Certifying Authority (CA).**

**Electronic signatures** do not require any kind of signing certificate.



To get **digital signatures** on the documents, the signer must have the digital signing certificate from an **issuing CA.**



**Electronic signatures** can easily be stored for long term archival.



**Digital signatures** safeguard all the sensitive data generated by private key and public key making the whole process **fully secure.**




# Functions



**Who signed** the document



**What document** was signed



**Intent and consent** of the sender and signer



**Secure sensitive data**
(User Authentication/ Validation/PKI)



Offer **tamper proof audit trail**
Keeping track of who signed what, how, and when.



Must have **Digital Signature Certificate** from an issuing Certifying Authority.

| Sections | Crime | Punishment |
|---|---|---|
| 499/500 IPC | Defamation | 2yrs/fine/both |
| 505 (1) IPC | Fake News | 3yrs/fine/both |
| 54 DM act | False alarm or warning regarding disaster | 1yr/fine/both |
| 153 (A) IPC | Spreading hatred | 6mnths/fine/both |
| 67 IT act | Pornography/ Cyber Bullying | 5yrs/fine/both |
| 67 B IT act | Child Porn | 7yrs/fine/both |
| 354 IPC | Outraging the modesty of women by action/force | 2yrs/fine/both |
| 507 IPC | Criminal Intimidation/Bullying | 2yrs/fine/both |
| 509 IPC | Outraging the modesty of women by words | 1 year/fine/both |
| 66 C IT act | Identity Theft | 3 yrs/fine/both |
| 66 D IT act | Cheating by Identity Theft | 3yrs/fine/both |
| 66 E IT act | Privacy violation | 3yrs/fine/both |
| 84 C IT act | Attempt of CyberCrime | Half years of crime punishment |
| 74 IT act | Forged electronic sign | 2yrs/fine/both |
| 66 F IT act | Cyber Terrorism | Life Imprisonment |
| 43-A IT act+ 66 IT act | Unauthorised Access | 3yrs/fine/both |

# Thankyou

# OFFENCES AND RELEVANT PENAL SECTIONS

## Cyber Crimes Mapping with Information Technology Act, 2000, Information Technology (Amendment) Act, 2008, IPC and Special and Local Laws.

| Sl. No | Nature of complaint | Applicable section(s) and punishments under ITA 2000 & ITAA 2008 | Applicable section(s) under other laws and punishment |
|---|---|---|---|
| 1 | Mobile phone lost/stolen | - | Section 379 IPC<br>3 years imprisonment or fine or both |
| 2 | Receiving stolen computer/ mobile phone/data (data or computer or mobile phone owned by you is found in the hands of someone else.) | Section 66 B of ITAA 2008<br>3 years imprisonment or Rupees one lakh fine or both | Section 411 IPC<br>3 years imprisonment or fine or both |
| 3 | Data owned by you or your company in any form is stolen | Section 66 of ITAA 2008<br>3 years imprisonment or fine up to rupees five lakh or both | Section 379 IPC<br>3 years imprisonment or fine or both |
| 4 | A password is stolen and used by someone else for fraudulent purpose. | Section 66C of ITAA 2008<br>3 years imprisonment and fine up to Rupees one lakh<br>Section 66D ITAA 2008<br>3 years imprisonment and fine up to Rupees one lakh | Section 419 IPC<br>3 years imprisonment or fine<br>Section 420 IPC<br>7 years imprisonment and fine |
| 6 | An e-mail is read by someone else by fraudulently making use of password | Section 66 of ITAA 2008<br>3 years imprisonment or fine up to Rupees five lakh or both<br>Section 66C of ITAA 2008<br>3 years imprisonment and fine up to Rupees one lakh | |
| 7 | A biometric thumb impression is misused | Section 66C of ITAA 2008<br>3 years imprisonment and fine up to Rupees one lakh | |
| 8 | An electronic signature or digital signature is misused | Section 66C of ITAA 2008<br>3 years imprisonment and fine up to Rupees one lakh | |
| 10 | A Phishing e-mail is sent out in your name, asking for login credentials | Section 66D of ITAA 2008<br>3 years imprisonment and fine up to Rupees one lakh | Section 419 IPC<br>3 years imprisonment or fine or both |
| 11 | Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge | Section 66E of ITAA 2008<br>3 years imprisonment or fine not exceeding Rupees two lakh or both | Section 292 IPC<br>2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction |
| 12 | Tampering with computer source Documents | Section 65 of ITAA 2008<br>3 years imprisonment or fine up to Rupees two lakh or both<br>Section 66 of ITAA 2008<br>3 years imprisonment or fine up to Rupees five lakh or both | |
| 13 | Data Modification | Section 66 of ITAA 2008<br>3 years imprisonment or fine up to Rupees five lakh or both | |

| | | | |
|---|---|---|---|
| 14 | Sending offensive messages through communication service, etc. | | Section 500 IPC 2 years or fine or both Section 504 IPC 2 years or fine or both Section 506 IPC 2 years or fine or both — if threat be to cause death or grievous hurt, etc. — 7 years or fine or both Section 507 IPC 2 years along with punishment under section 506 IPC Section 508 IPC 1 year or fine or both Section 509 IPC 1 years or fine or both of IPC as applicable |
| 15 | Publishing or transmitting obscene material in electronic form | Section 67 of ITAA 2008 first conviction — 3 years and 5 lakh Second or subsequent conviction— 5 years and up to 10 lakh | Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction |
| 16 | Publishing or transmitting of material containing sexually explicit act, etc., in electronic form | Section 67A of ITAA 2008 first conviction —5 years and up to 10 lakh Second or subsequent conviction— 7 years and up to 10 lakh | Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction |
| 17 | Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form | Section 67B of ITAA 2008 first conviction —5 years and up to 10 lakh Second or subsequent conviction— 7 years and up to 10 lakh | Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction |
| 18 | Misusing a Wi-Fi connection for acting against the state | Section 66 3 years imprisonment or fine up to Rupees five lakh or both Section 66F— life imprisonment of ITAA 2008 | |
| 19 | Planting a computer virus that acts against the state | Section 66 3 years imprisonment or fine up to Rupees five lakh or both 66F— life imprisonment | |
| 20 | Conducting a denial of service attack against a government computer | Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of ITAA 2008— life imprisonment of | |
| 21 | Stealing data from a government computer that has significance from national security perspective | Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both, 66F — life imprisonment | |
| 22 | Not allowing the authorities to decrypt all communication that passes through your computer or network. | Section 69 of ITAA 2008 imprisonment up to 7 years and fine | |
| 23 | Intermediaries not providing access to information stored on their computer to the relevant authorities | Section 69 of ITAA 2008 imprisonment up to 7 years and fine | |

| | | | |
|---|---|---|---|
| 24 | Failure to Block Web sites, when ordered | Section 69A of ITAA 2008 imprisonment up to 7 years and fine | |
| 25 | Sending threatening messages by e-mail | | Section 506 IPC 2 years or fine or both |
| 25 | Word, gesture or act intended to insult the modesty of a woman | | Section 509 IPC 1 years or fine or both – IPC as applicable |
| 26 | Sending defamatory messages by e-mail | | Section 500 IPC 2 years or fine or both |
| 27 | Bogus Web sites, cyber frauds | Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh | Section 419 IPC 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine |
| 28 | E-mail Spoofing | Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh | Section 465 IPC 2 years or fine or both Section 468 IPC 7 years imprisonment and fine |
| 29 | Making a false document | Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh | Section 465 IPC 2 years or fine or both |
| 30 | Forgery for purpose of cheating | Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh | Section 468 IPC 7 years imprisonment and fine |
| 31 | Forgery for purpose of harming reputation | Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh | Section. 469 IPC 3 years and fine |
| 32 | E-mail Abuse | | Sec. 500 IPC 2 years or fine or both |
| 33 | Punishment for criminal intimidation | | Sec. 506 IPC 2 years or fine or both – if threat be to cause death or grievous hurt, etc. – 7 years or fine or both |
| 34 | Criminal intimidation by an anonymous communication | | Sec. 507 IPC 2 years along with punishment under section 506 IPC |
| 35 | Copyright infringement | Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both | Sec. 63, 63B Copyrights Act 1957 |
| 36 | Theft of Computer Hardware | | Sec. 379 IPC 3 years imprisonment or fine or both |
| 37 | Online Sale of Drugs | | NDPS Act |
| 38 | Online Sale of Arms | | Arms Act |

**Disclaimer:** The above-mentioned explanations made herein are to the best of our knowledge and interpretations and are purely for academic and information purpose only. They may be used as a guiding force. They should not be construed as legal opinion by any stretch of imagination. We are thankful to all the stake holders for uploading information which we may have used for education purpose only.