Information Technology Act, 2000

- The Information Technology Act, 2000 or ITA, 2000 or IT Act, was notified on October 17, 2000. It is the law that deals with cybercrime and electronic commerce in India.

Objectives of the Act

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

The objectives of the Act are as follows:

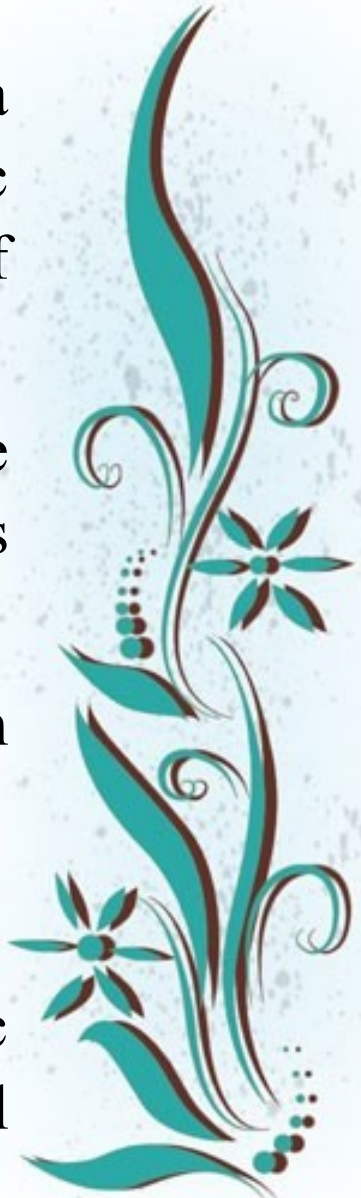
i. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication

iii. Facilitate the electronic filing of documents with Government agencies and also departments

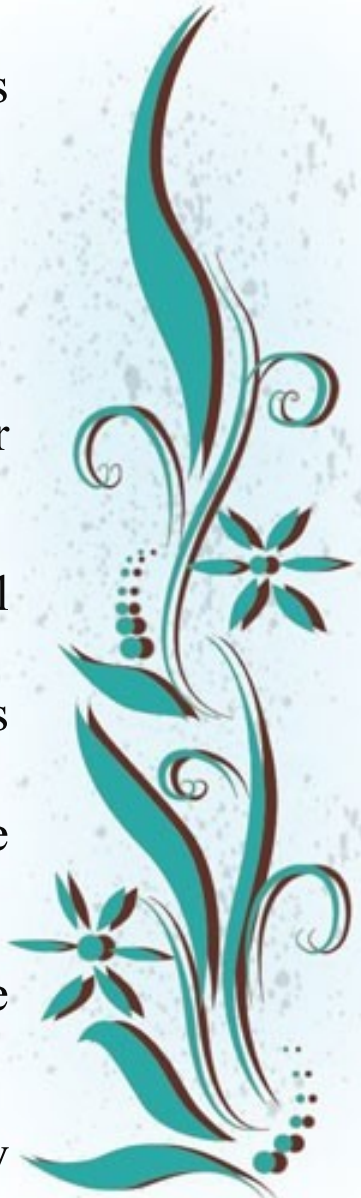
iv. Facilitate the electronic storage of data

v. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions



Features of the Information Technology Act, 2000

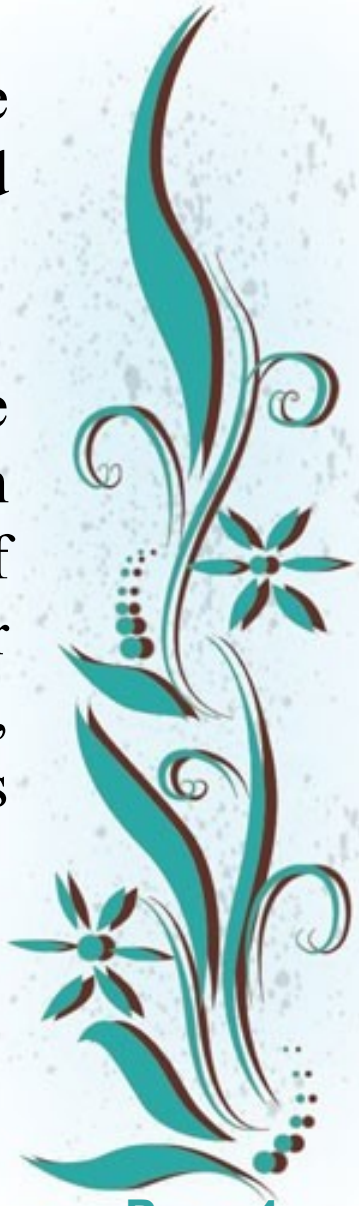
- All electronic contracts made through secure electronic channels are legally valid.
- Legal recognition for digital signatures.
- Security measures for electronic records.
- A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized.
- Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act.
- An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court.
- The Act applies to offences or contraventions committed outside India
- Senior police officers and other officers can enter any public place and search and arrest without warrant
- Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government.



Applicability of the Act:

According to Section 1 (2), the Act extends to the entire country, which also includes Jammu and Kashmir.

Section 1 (2) along with Section 75, specifies that the Act is applicable to any offence or contravention committed outside India as well. If the conduct of person constituting the offence involves a computer or a computerized system or network located in India, then irrespective of his/her nationality, the person is punishable under the Act.



Electronic Record and E-Governance

According to the World Bank, E-Governance is when government agencies use information and communication technologies to transform relations with citizens, businesses, and other government agencies. One of the prime objectives of the IT Act, 2000 is the promotion of electronic governance.

Provisions for e-governance under the IT Act, 2000:

1. Legal Recognition of Electronic Records (Section 4)

2. Legal recognition of digital signatures (Section 5)

3. Use of electronic records and digital signatures in Government and its agencies (Section 6)

4. Retention of electronic records (Section 7)

5. Publication of rules, regulations, etc., in Electronic Gazette (Section 8)

6. Power to make rules by Central Government in respect of digital signature (Section 10)

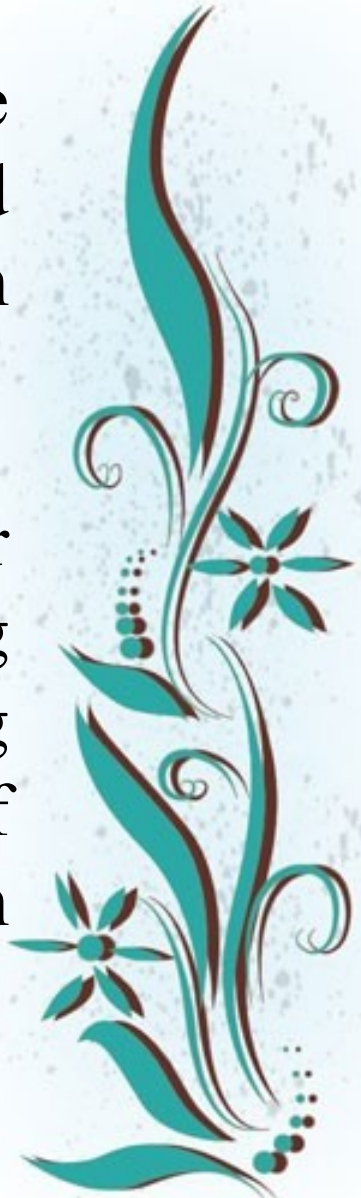
What are digital signatures?

Digital signatures mean the authentication of any electronic record using an electronic method or procedure in accordance with the provisions of the Information Technology Act, 2000. Also, a handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature.

Digital Signature

According to Section 2(1)(p), digital signature means ‘authentication of any electronic record using an electronic method or procedure in accordance with the provisions of Section 3‘.

Further, authentication is a process for confirming the identity of a person or proving the integrity of information. Authenticating messages involves determining the source of the message and verifying that is has not been altered or modified in transit.



Digital Signature

Digital signature is a mathematical scheme to verify the authenticity of digital documents or messages. Also, a valid digital signature allows the recipient to trust the fact that a known sender sent the message and it was not altered in transit.

The three important features of digital features are:

Authentication – They authenticate the source of messages. Since the ownership of a digital certificate is bound to a specific user, the signature shows that the user sent it.

Integrity – Sometimes, the sender and receiver of a message need an assurance that the message was not altered during transmission. A digital certificate provides this feature.

Non-Repudiation – A sender cannot deny sending a message which has a digital signature.

Provisions for e-governance under the IT Act, 2000

1. Legal Recognition of Electronic Records (Section 4)

Let's say that a certain law requires a matter written, typewritten, or printed. Even in the case of such a law, the requirement is satisfied if the information is rendered or made available in an electronic form and also accessible for subsequent reference.

2. Legal recognition of digital signatures (Section 5)

Let's say that the law requires a person's signature to authenticate some information or a document. Notwithstanding anything contained in such law, if the person authenticates it with a digital signature in a manner that the Central Government prescribes, then he satisfies the requirement of the law.

3. Use of electronic records and digital signatures in Government and its agencies (Section 6)

(1) If any law provides for –

1. the filing of a form, application, or any document with any Government-owned or controlled office, agency, body, or authority
2. the grant or issue of any license, sanction, permit or approval in a particular manner
3. also, the receipt or payment of money in a certain way

Provisions for e-governance under the IT Act, 2000

4. Retention of electronic records (Section 7)

(1) Let's say that the law requires the retention of certain records, documents or information for a specific period. In such cases, the requirement is also satisfied if the retention is in an electronic form, provided:

1. the information contained therein is accessible and also usable for a subsequent reference.
2. the format of the electronic record is the same as the one originally created, received or sent. Even if the format is changed, then it must accurately represent the original information.
3. the electronic record contains details to facilitate the identification of the origin, destination, and also the date and time of the dispatch or receipt of the record.

5. Publication of rules, regulations, etc., in Electronic Gazette (Section 8)

Let's say that law requires the publishing of official regulation, rule, by-law, notification or any other matter in the Official Gazette. In such cases, the requirement is also satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette.

Provisions for e-governance under the IT Act, 2000

6. Section 6,7 and 8 do not confer a right to insist document should be accepted in Electronic form (Section 9)

It is important to note that, nothing contained in Sections 6, 7, and 8 confer a right upon any person to insist either the acceptance, issuance, creation or also retention of any document or a monetary transaction in the electronic form from:

- Ministry or Department of the Central/State Government
- Also, any authority or body established under any law by the State/Central Government

7. Power to make rules by Central Government in respect of digital signature (Section 10)

The IT Act, 2000 empowers the Central Government to prescribe:

- Type of digital signature
- Also, the manner and format of affixing the digital signature
- Procedures which facilitate the identification of the person affixing the digital signature
- Control processes and procedures to ensure the integrity, security, and confidentiality of electronic payments or records
- Further, any other matter which is legally important for digital signatures

Data Protection

Section 43A of the Information Technology Act, 2000:

Let's say that a body corporate which possesses, deals or handles any sensitive personal data or information in a computer resource which it owns, controls or operates, is certainly negligent in implementing and maintaining reasonable security practices and procedures leading to a wrongful loss or gain to a person.

In such cases, the body corporate is liable to pay damages by way of compensation. Further, these damages cannot exceed five crore rupees.

Further, the Government of India notified the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, under section 43A of the IT Act, 2000. These rules specifically pertain to sensitive personal information or data and are applicable to all body corporates within India.

Introduction to Cyberspace

Two decades ago, the term cyberspace seemed right out of a science fiction movie. In the second decade of the twenty-first century, cyberspace is probably the place where most of us spend a major part of our lives. It has become an inseparable element of our existence.

Cyber Appellate Tribunal

The Information Technology Act, 2000 also provides for the establishment of the Cyber Appellate Tribunal.

Establishment of Cyber Appellate Tribunal (Section 48)

- The Central Government notifies and establishes appellate tribunals called Cyber Regulations Appellate Tribunal.
- The Central Government also specifies in the notification all the matters and places which fall under the jurisdiction of the Tribunal.

The composition of Cyber Appellant Tribunal (Section 49)

The Central Government appoints only one person in a Tribunal – the Presiding Officer of the Cyber Appellate Tribunal.

Cyber Appellate Tribunal

The qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal (Section 50)

A person is considered qualified for the appointment as the Presiding Officer of a Tribunal if –

a. He has the qualification of the Judge of a High Court

b. He is or was the member of the Indian Legal Service and holds or has held a post in Grade I of that service for at least three years.

The Term of Office (Section 51)

The Term of Office of the Presiding Officer of a Cyber Appellate Tribunal is five years from the date of entering the office or until he attains the age of 65 years, whichever is earlier.

Classification of Cyber Crimes

Cyber crimes are classified based on the subject of the crime, the person or organization against whom the crime is committed, and the temporal nature of the crimes committed online.

- **Crimes against individuals** – These are committed against individuals or their properties. Some examples are:Email harassment
- Cyber-stalking
- Spreading obscene material
- Unauthorized access or control over the computer system
- Indecent exposure
- Spoofing via email
- Fraud and also cheating
- Further, crimes against individual property like computer vandalism and transmitting a virus. Also, trespassing online and intellectual property-related crimes. Further, internet time thefts are also included.

- **Crimes against organizations** – Some examples of cyber crimes against organizations are:Possessing unauthorized information
- Cyber terrorism against a government organization
- Distributing pirated software
- **Crimes against society** – Some examples of crimes against society are:Polluting the youth through indecent exposure
- Trafficking
- Financial crimes
- Selling illegal articles
- Online Gambling
- Forgery

Provisions of Cyber Crimes in the IT Act, 2000

Section 43 – Penalty for damage to a computer, computer system, etc.

This section applies if any person, without the permission of the owner or the person in charge of a computer, system, or network –

Penalty – Compensation, not exceeding one crore rupees to the affected person.

Section 65 – Tampering with the computer's source code documents

Penalty – Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.

Section 66 – Hacking of a Computer System

Penalty – Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.

Section 67 – Publishing obscene information in an electronic form

Penalty – In case of the first conviction, imprisonment of up to five years and a fine of up to one lakh rupees. For subsequent convictions, imprisonment of up to 10 years and a fine of up to two lakh rupees.

Provisions of Cyber Crimes in the IT Act, 2000

Section 74 – Publication with the intention of fraud

This section applies to a person who knowingly creates, publishes or makes available a digital certificate with the intention of fraud.

Penalty – Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 44 – Failure to furnish information, returns, etc.

Penalty

- A monetary fine of up to one lakh and fifty thousand rupees for each such failure
- A fine of up to five thousand rupees for every day if the failure continues
- A fine of up to ten thousand rupees for every day if the failure continues

Section 71 – Misrepresentation

Penalty – Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 72 – Breach of confidentiality and privacy

Penalty – Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases

Provisions of Cyber Crimes in the IT Act, 2000

Section 73 – Publishing a Digital Certificate with incorrect details

Penalty – Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 74 – Publication with a fraudulent purpose

Penalty – Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 85 – Company Offences

(1) This section applies to a company who commits a contravention to the provisions of the Act. In such cases, all the people who were in charge and responsible for the company's conduct of business as well as the company are guilty of the contravention. Further, those responsible are liable for punishment. However, if a person is not aware of any such contravention, then he is not liable.

(2) Notwithstanding anything contained in the sub-section (1), if it is proved that the contravention was with the consent of, or due to the negligence of any director, manager or any other officer, then such people are also held liable.

Non-Applicability/ Limitations of the Act

According to Section 1 (4) of the Information Technology Act, 2000, the Act is not applicable to the following documents:

1. Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.
2. Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
3. Creation of Trust under the Indian Trust Act, 1882.
4. Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition
   by whatever name called.
5. Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central Government in the Gazette.