IT Act 2000

Define IT Act 2000:

The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Thus, the IT Act 2000. the cyber law of India, gives the legal framework so that information is not denied legal effect. validity or enforceability, solely on the ground that it is in the form of electronic records.

Scheme of the IT Act. 2000:

1) Chapter-II of the Act specifically stipulate (promise) that subscriber may authenticate

2) Chapter-III of the Act details about Electronic Governanceand and provides inter alia amongst them that are any law provides the information or any other matter shall be in writing or is in printed form.

3) Chapter-IV of the said act gives scheme Regulation of Certifying Authorities.

4) Chapter-VII of the Act details about be seemed things relating to Digital Signature Certificate.

5) Chapter-IX of the said act talk about penalties and adjudication for various offences.

6) Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals agains theorders passed by the Adjudicating Officers, shall be preferred.

7) Chapter-XI of the Act talks about various offences and the said offences shall he investigated only by a Police Officer not below the rank of the Deputy Superintendent of PolPolic

Objectives of IT Act 2000 :

1. It is objective of I.T. Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration in employment exchange.
4. According to I.T. Act 2000, any company can store their data in electronic storage.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

Scope of IT Act 2000 :

1. Every electronic information is under the scope of I.T. Act 2000 but following electronic transaction is not under I.T. Act 2000
2. Information technology act 2000 is not applicable on the attestation for creating trust via electronic way. Physical attestation is must.
3. I.T. Act 2000 is not applicable on the attestation for making will of any body. Physical attestation by two witnesses is must.
4. A contract of sale of any immovable property.
5. Attestation for giving power of attorney of property is not possible via electronic record.

Digital & Electronic Signature :

Digital Signature (IT Act 2000) 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**. In this article, we will look at the sections of the Information Act, 2000 which deal with digital certificates.

Electronic Signature (Amended I.T. Act 2008)

E-signature, indicates either that a person who demands to have created a message is the one who created it. A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document

The Three important features of Digital features are:

1)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.

2)**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.

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

Digital Signature to Electronic Signature

- **Digital Signature** was the term defined in the old I.T. Act, 2000.
- **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008).
- The concept of Electronic Signature is broader than Digital Signature.
- Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

Duties Of Subscriber Under The It Act 2000

1. Generating key pair (section 40)

Where any Digital Signature Certificate, the **public key** of which corresponds to the **private key** of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

2. Acceptance of Digital Signature Certificate (section 41)

i) **A subscriber shall be deemed** to have accepted a Digital Signature Certificate if he publishes or authorise the publication of a Digital Signature Certificate-

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner,

ii) **By accepting a Digital Signature the subscriber certifie**s to all who reasonable rely on the information contained in the Digital Signature Certificate that-

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

3. Control of private key (section 42)

i) Every subscriber shall exercise shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

ii) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without and delay to the Certifying Authority in such manner as may be specified by the regulations.

E-governance

Electronic governance or **e-governance** is the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems between (G2C), (G2B), (G2G), (G2E) as well as back-office processes and interactions within the entire government framework.

Through e-governance, government services are made available to citizens in a convenient, efficient, and transparent manner. The three main target groups that can be distinguished in governance concepts are government, citizens, and businesses/interest groups. In e-governance, there are no distinct boundaries

Electronic Record

An **Electronic Record** is information recorded by a computer that is produced or received in the initiation, conduct or completion of an agency or individual activity.

Examples of electronic records include:

e-mail messages, word- processed documents, **electronic** spreadsheets, digital images and databases.

Certifying Authority (CAs)

A **Certifying Authority** is a trusted body whose central responsibility is to issue, revoke, renew and provide directories of Digital Certificates.

According to section 24 **under** Information Technology **Act 2000 "Certifying Authority"** means a person who has been granted a licence to issue Digital Signature Certificates.

Penalties, Compensation and Adjudication(fuokMk)

Section 43 of the IT Act 2000

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, or computer resource-

1. accesses or secures access to such computer, computer system or computer network;
2. 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;
3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. 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;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (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;
7. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
8. steel, conceals, 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

Offences included in the IT Act 2000

1. Tampering with the computer source documents (Section 65).
2. Hacking with computer system (Section 66).
3. Publishing of information which is obscene in electronic form. (Section 67)
4. Power of Controller to give directions (Section 68)
5. Directions of Controller to a subscriber to extend facilities to decrypt information (Section 69)
6. Protected system (Section 70)
7. Penalty for misrepresentation (Section 71)
8. Penalty for breach of confidentiality and privacy (Section 72)
9. Penalty for publishing Digital Signature Certificate false in certain particulars (Section 73)
10. Publication for fraudulent purpose (Section 74)
11. Act to apply for offence or contravention committed outside India (Section 75)
12. Confiscation (Section 76)
13. Penalties or confiscation not to interfere with other punishments (Section 77).
14. Power to investigate offences (Section 78).

Establishment of Cyber Appellate Tribunal (Section 48)

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

Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal (section 50)

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he-

1) is, or has been, or is qualified to be, a Judge of a High Court;

or

2) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

Terms of office (section 51)

The Presiding Officer of a Cyber Appellate shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixtyfive years, whichever is earlier.

Appeal to Cyber Appellate Tribunal

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the

Procedure and powers of the Cyber Appellate Tribunal Sec. 58

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sitting.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely : -

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses of documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte;

(g) any other matter which may be prescribed.

Thank You!