Information Technology Act, 2000

Contents-

- **Objectives**
- **Scope**
- **Non applicability of IT Act**
- **Key Definitions – (Sec 2)**
- **Digital signature (Sec 3)**
- **Electronic Signature (Sec 3A)**
- **Electronic Governance- (Sec 4 -10)**
- **Attribution, Acknowledgement and dispatch of Electronic Records (Sec. 11-16)**
- **Regulation of certifying Authority**
- **Digital Signature Certificates (Sec.35-39)**
- **Duties of Subscriber (Sec.40-42)**
- **Penalties (Sec. 43-46)**
- **Offences (Sec. 65,66,67,77)**

Refer to Taxmann's Business laws (by-Sushma Arora) – Chapter 25, 26, 27, 28, 29, 30(only penalties and offences) - Page no. 441 to 483 and 492 to 496.

Refer to Business laws (by-Dr. Rajni Jagota) – Chapter 24, 25, 26,27,28,29 - Page no. 24.1 to 29.10

Information Technology Act, 2000

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce

(E-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

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.

Objectives of the Act

The objectives of the Act are as follows:

1. 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.
2. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication
3. Facilitate the electronic filing of documents with Government agencies and also departments
4. Facilitate the electronic storage of data
5. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions
6. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Non-Applicability

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.

Scope or Extent of the ACT

It extends to the whole of India

It also applies to any offence or contravention committed outside India by any person irrespective of his nationality, provided such offence or contravention involves a computer, computer system or network located in India.

Key Definitions (to be covered)

Sec. 2(1) (a)

Sec. 2(1) (b)

Sec. 2(1) (c)

Sec. 2(1) (d)

Sec. 2(1) (da)

Sec. 2(1) (g)

Sec. 2(1) (i)

Sec. 2(1) (j)

Sec. 2(1) (k)

Sec. 2(1) (l)

Sec. 2(1) (o)

Sec. 2(1) (p)

Sec. 2(1) (v)

Sec. 2(1) (w)

Sec. 2(1) (x)

Sec. 2(1) (zc)

Sec. 2(1) (zd)

Sec. 2(1) (ze)

Sec. 2(1) (h)

Sec. 2(1) (n)

Sec. 2(1) (r)

Sec. 2(1) (t)

Sec. 2(1) (za)

Sec. 2(1) (zg)

Sec. 2(1) (zh)

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, digital signatures authenticate the source of messages like an electronic mail or a contract in electronic form.

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.

Authentication of Electronic record

Section 3

Section 3 of the Information technology Act, 2000 provides certain provisions for the authentication of electronic records. The provisions are:

- Subject to the provisions of this section, any subscriber can affix his digital signature and hence authenticate an electronic record.

- An asymmetric crypto system and hash function envelop and transform the initial electronic record into another record which affects the authentication of the record.
- Also, any person in possession of the public key can verify the electronic record.
- Further, every subscriber has a private key and a public key which are unique to him and constitute a functioning key pair.

Read the Process and creation of Digital Signature (Rule 4 and Rule 5) – Chapter 26 (Sushma Arora) or Chapter 25 (Dr. Rajni Jagota)

Electronic Signature (Section 3A)

Electronic Signature has been defined under Section 2(1)(ta) of the Information Technology Act, 2000. Electronic Signature means the authentication of any electronic record by a subscriber by means of the electronic technique as specified under the Second Schedule and also includes a digital signature.

Read the Difference between Digital Signature and Electronic Signature – Chapter 26 (Sushma Arora) or Chapter 25 (Dr. Rajni Jagota)

Electronic Governance (Section 4 -10)

- **Meaning of E- Governance**
- **Provisions-**

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 the Government and also its agencies – Section 6
4. Delivery of services by service provider - Section 6 A
5. Retention of electronic records – Section 7
6. Audit of documents, records or information maintained in electronic form - Section 7A
7. Publication in Electronic Gazette – Section 8
8. Section 6,7 and 8 Not to confer right to insist on the acceptance of documents in the electronic form – Section 9
9. Central Government's power to make rules pertaining to digital signatures – Section 10
10. Validity of contracts formed through Electronic means – Section 10A

Attribution, Acknowledgement and dispatch of Electronic Records (Sec. 11-16)

Sec. 11 Attribution of electronic records.-An electronic record shall be attributed to the originator,-

(a) if it was sent by the originator himself;
(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
(c) by an information system programmed by or on behalf of the originator to operate automatically.

Sec. 12 Acknowledgement of receipt. –

(1) Where the originator has not agreed that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by-
(a) any communication by the addressee, automated or otherwise; or
(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement

must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Sec. 13. **Time and place of despatch and receipt of electronic record.-**

(1)Time of Dispatch- Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Time of Receipt- Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:-

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,-
(i) Receipt occurs at the time when the electronic record enters the designated computer resource; or
(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;
(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Place of Dispatch- Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) Place of Receipt- The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) Place of Business- For the purposes of this section,-

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;
(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

Sec. 14. **Secure electronic record**.-Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Sec. 15 Secure electronic signature. -An electronic signature shall be deemed to be a secure electronic signature if-
(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation. -In case of digital signature, the "signature creation data" means the private key of the subscriber.]

Sec. 16 Security procedures and practices. -The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices: Provided that in prescribing such security procedures and practices, the Central Government shall have regard

to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.] "16. Security procedure. -The Central Government shall, for the purposes of this Act, prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-
(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications."