

Lecture- 19



Features of Information Technology Act, 2000

Following are the features of the Act:

- The Act is based on the Model Law on e-commerce adopted by UNCITRAL.
- It has extra-territorial jurisdiction.
- It defines various terminologies used in the Act like cyber cafes, computer systems, digital signatures, electronic records, data, asymmetric cryptosystems, etc under Section 2(1).
- It protects all the transactions and contracts made through electronic means and says that all such contracts are valid. (Section 10A)
- It also gives recognition to digital signatures and provides methods of authentication.
- It contains provisions related to the appointment of the Controller and its powers.
- It recognises foreign certifying authorities (Section 19).
- It also provides various penalties in case a computer system is damaged by anyone other than the owner of the system.
- The Act also provides provisions for an Appellate Tribunal to be established under the Act. All the appeals from the decisions of the Controller or other Adjudicating officers lie to the Appellate tribunal.
- Further, an appeal from the tribunal lies with the High Court.
- The Act describes various offences related to data and defines their punishment.
- It provides circumstances where the intermediaries are not held liable even if the privacy of data is breached.
- A cyber regulation advisory committee is set up under the Act to advise the Central Government on all matters related to e-commerce or digital signatures.

Overview of Information Technology Act, 2000

The Act deals with e-commerce and all the transactions done through it. It gives provisions for the validity and recognition of electronic records along with a license that is necessary to issue any digital or electronic signatures. The article further gives an overview of the Act.

Electronic records and signatures

The Act defines electronic records under Section 2(1)(t), which includes any data, image, record, or file sent through an electronic mode. According to Section 2(1)(ta), any signature used to authenticate any electronic record that is in the form of a digital signature is called an electronic signature. However, such authentication will be affected by asymmetric cryptosystems and hash functions as given under Section 3 of the Act.

Section 3A further gives the conditions of a reliable electronic signature. These are:

- If the signatures are linked to the signatory or authenticator, they are considered reliable.
- If the signatures are under the control of the signatory at the time of signing.
- Any alteration to such a signature must be detectable after fixation or alteration.
- The alteration done to any information which is authenticated by the signature must be detectable.
- It must also fulfill any other conditions as specified by the Central Government.

The government can anytime make rules for electronic signatures according to Section 10 of the Act. The attribution of an electronic record is given under Section 11 of the Act. An electronic record is attributed if it is sent by the originator or any other person on his behalf. The person receiving the electronic record must acknowledge the receipt of receiving the record in any manner if the originator has not specified any particular manner. (Section 12). According to Section 13, an electronic record is said to be dispatched if it enters another

computer source that is outside the control of the originator. The time of receipt is determined in the following ways:

When the addressee has given any computer resource, Receipt occurs on the entry of an electronic record into the designated computer resource.

In case the record is sent to any other computer system, the receipt occurs when it is retrieved by the addressee.

When the addressee has not specified any computer resource, the receipt occurs when the record enters any computer source of the addressee.