SUBJECT SEC : E-COMMERCE

2ND SEMESTER (FYUGP)

UNIT – 3 IT ACT 2000 AND CYBER-CRIMES

IT Act, 2000: Definitions, Digital Signature, Electronic Governance, Attribution, Acknowledgement and Dispatch of electronic records, Regulation of Certifying Authorities, Digital Signatures Certificates, Duties of Subscribers, Penalties and Adjudication, Appellate Tribunal, Offences and Cyber-Crimes.

INTRODUCTION - The Information Technology Act was enacted in the year 2000 with major objectives to provide legal recognition for e-commerce and e-transactions, to facilitate e- governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide. The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures.

SCOPE OF THE IT ACT, 2000

IT ACT came into force from 17th October, 2000. It covers to whole of India. This act can also be operated to any offences or contravention committed outside India by any person irrespective of his nationality provided such offence of contravention involves a computer, computer system or network located in India (Section 1(2) read with Section 75).

The main issues covered under the IT ACT 2000, are given below:

(a) Legal recognition of digital signatures.

(b) Legal recognition of electronic documents.

(c) Offences and contraventions.

DIGITAL SIGNATURE

A digital signature authenticates electronic documents in a similar manner like a handwritten signature authenticates printed documents. This signature cannot be faked and a claims that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient of a digitally signed message can verify that the message originated from the person whose signature is attached to the document and that the message has not been altered either intentionally or accidentally since it was signed. Also the signer of a document cannot later disagree with it by claiming that the signature was forged. In other words digital signatures enable the authentication of digital messages assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

In short, it is used:

- To ensure message content integrity.
- To verify the authenticity of the message sender

ELECTRONIC GOVERNANCE

E-governance (or Electronic Governance) use information and communication technology (ICT) means (such as internet, Local Area Networks, mobiles etc.) to improve the quality of delivering government services, exchange of information, communication transactions to citizens, employees, businesses, other sectors of government. E-governance can be defined as the delivery of government services and information to the public by means of technology. The internet with its universal standards makes it easier for developing countries like India to offer e- government services. The main objective of e-governance is to provide government services to citizens in a convenient, efficient and transparent manner.

ATTRIBUTION, ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

The IT Act 2000 provides a legal recognition of attribution, acknowledgement and dispatch of electronic records.

Attribution of electronic records states that 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.

Acknowledgment of receipt states that If the originator has not specified any specific mode of acknowledgement (an act by the addressee that he/she has received the electronic record), the acknowledgement can 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.

If the originator has specified a format and time period for sending the acknowledgement, then the addressee must send the acknowledgement in that format and within the given time period otherwise the originator can send a notice to the addressee stating that no acknowledgement was received.

Time and place of despatch and receipt of electronic record states that

1. The dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

2. 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,

- receipt occurs at the time when the electronic, record enters the designated computer resource; or
- 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. An electronic record is deemed to be dispatched 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.

REGULATION OF CERTIFYING AUTHORITIES

As per Section 17 of IT Act, 2000, the Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

- The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

- The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
- The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
- There shall be a seal of the Office of the Controller.

DIGITAL SIGNATURE CERTFICATION

Section 3 states that any person can make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government. Every such application should be accompanied by such fee not exceeding twenty-five thousand rupees. The Certifying Authority will issue the Digital Signature Certificate to subscriber after satisfying that:

- the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate.
- the applicant holds a private key, which is capable of creating a digital signature.

Section 36: Representations upon issuance of Digital Signature Certificate - A Certifying Authority while issuing a Digital Signature Certificate shall certify that:

- It has complied with the provisions of this Act and the rules and regulations made there under.
- It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it.
- The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate.

- The subscriber's public key and private key constitute a functioning key pair
- The information contained in the Digital Signature Certificate is accurate.

Section 37: Suspension of Digital Signature Certificate - This section states that Certifying Authority may suspend Digital Signature Certificate on receipt of request from subscriber or any person behalf of that subscriber. The CA may also suspend Digital Signature Certificate in public interest in public interest.

DUTIES OF SUBSCRIBERS

- **Section 40: Generating key pair-** This section states that as the subscriber holds the private key corresponding to the public key which is listed in the Digital Signature Certificate, the subscriber will generate the key pair by applying the security procedure.
- **Section 41: Acceptance of Digital Signature Certificate -** This section states that a subscriber will be considered to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate to one or more persons. By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate.
- **Section 42: Control of private key -** This section states that a subscriber should take all the 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 authorized to affix the digital signature of the subscriber.

PENALTIES AND ADJUDICATION

The Central Government may, by an order published in the Official Gazette. appoint as many officers of the Central Government, not below the rank of Registrar under the provisions of IT Act 2000. The adjudicating officer may, by an order impose the penalty on the company and the officer who is in default stating any non-compliance or default under the relevant provision of the Act. The Adjudicating Officer has power for holding an inquiry for purpose of adjudicating offences punishable under various

The penalties can be imposed by the adjudicating officer for:

- Unauthorized accesses to computer, computer system or computer network;
- Downloads, copies or extracts any data, database or information from computer, computer system or computer network.
- Introduction of any computer virus into any computer, computer system or computer network;
- Damage to any data, database, information or any other programs from computer, computer system or computer network.
- Disruption of any computer, computer system or computer network;
- Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network
- Providing any assistance to any person to facilitate access to a computer, computer system or computer network
- Charging 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.

CYBER APPELLATE TRIBUNAL

The Cyber Appellate Tribunal shall be the Appellate body where appeals against orders passed by the adjudicating officers shall be preferred. The first Cyber Appellate Tribunal in India was formed by the Central Government in accordance with the provisions described under Section 48(1) of the Information Technology Act, 2000. The Cyber Appellate Tribunal is not guided or governed by the Code of Civil Laws but is guided by the principle of Natural Justice. It has the same power as a Civil Court. The Cyber Appellate Tribunal has powers to regulate its own procedure including the place at which it has its sittings. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973

PROCEDURE AND POWERS OF THE CYBER APPELLATE TRIBUNAL

(a) Calling and binding the attendance of any person and examining him on oath,
(b) Demanding the discovery and production of documents or other electronic records,
(c) Receiving evidence on affidavits;
(d) Issuing commissions for the examination of witnesses or documents;
(e) Reviewing its decisions,
(f) Dismissing an application for default or deciding it ex parte;
(g) Any other matter which may be prescribed.

OFFENCES & CYBER-CRIMES

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. The offences included in the IT Act 2000 are as follows:

1. Tampering with computer source documents (Section 65) - If a person 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.

Penalty: Imprisonment up to three years, or/and with fine up to Rs2,00,000

2. Hacking with computer system (Section 66) - If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes of alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

Penalty: Imprisonment up to three years, or/and with fine up to Rs 25,00,000

3. Receiving stolen computer or communication device (Section 66B) - A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.

Penalty: Imprisonment up to three years, or/and with fine up to Rs1,00,000

4. Using password of another person (Section 66C) - A person fraudulently uses the password, digital signature or other unique identification of another person.

Penalty: Imprisonment up to three years, or/and with fine up to Rs 1,00,000

5. Cheating using computer resource (Section 66D) - If a person cheats someone using a computer resource or communication.

Penalty: Imprisonment up to three years, or/and with fine up to Rs 1,00,000.

6. Publishing private images of others (Section 66E) - If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.

Penalty: Imprisonment up to three years, or/and with fine up to Rs 2,00,000.

7. Acts of cyber-terrorism (Section 66F) - If a person denies access to authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber-terrorism.

Penalty: Imprisonment up to life.

8. Publishing information which is obscene in electronic form (Section 67) - If a person publishes or transmits or causes to be published 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.

Penalty: Imprisonment up to five years, or/and with fine up to Rs Rs 1,000,000

9. Publishing images containing sexual acts (Section 67A) - If a person publishes or transmits images containing a sexual explicit act or conduct.

Penalty: Imprisonment up to seven years, or/and with fine up to Rs 1,000,000.

10. Publishing child porn or predating children online (Section 67B) - If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.

Penalty: Imprisonment up to five years, or/and with fine up to Rs 1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs 1,000,000 on second conviction.

11. Failure to maintain records (Section 67C) - Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.

Penalty: Imprisonment up to three years, or/and with fine.

12. Failure/refusal to comply with orders (Section 68) - The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.

Penalty: Imprisonment up to three years, or/and with fine up to Rs 2,00,000

13. Failure/refusal to decrypt data (Section 69) - If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the Information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.

Penalty: Imprisonment up to seven years and possible fine.

14. Attempt to secure access to a protected system (Section 70) - The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.

Penalty Imprisonment up to ten years, or/and with fine.

15. Misrepresentation (Section 71) - If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.

Penalty: Imprisonment up to three years, or/and with fine up to Rs 1,00,000.