UNIT 2 INFORMATION TECHNOLOGY ACT – PART I

Structure

2.1 INTRODUCTION

In the previous unit we have tried to present a broad picture of the IT Act. In the next two units, we shall examine the provisions of the Information Technology Act, 2000 in detail. In this unit we shall discuss the objectives for which this Act has been passed. This unit will also discuss the extra-territorial application of the Act. This has become important because computer related wrongs know no boundaries. A wrongful act committed in one country may affect the computers and computer networks of not only the country where the wrong has been committed but also of other countries.

The IT Act has introduced certain new concepts such as “digital signature” “e-governance” etc. The Act gives legal recognition to the electronic records and treat its at par with the paper based system if all the safeguards are followed.

2.2 OBJECTIVES

After studying this unit you should be able to:

- discuss the aims and objectives of the Act i.e. what does the Act try to achieve?

- analyse the concept of digital signature and discuss the powers and functions of the issuing authorities a authority to exercise control over the issuance of digital signatures; and
- discuss the provisions relating to e-governance and legal recognition of electronic records.

2.3 STATEMENT OF OBJECTS AND REASONS

The statement of objects and reasons of the IT Act reflects the purpose of the enactment and what it is trying to achieve. The concern of the framers of the IT Act was the need for information to be collected, stored and utilized in electronic form which in turn would serve the dual purpose of facilitating e-commerce and inducting e-governance in the system.

Another object was clearly aimed at giving effect to the United Nations General Assembly Resolution[1] whereby the Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law. It recommended the States to give a favourable consideration to the Model Law when they enact or revise their laws, '*in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information*'. Thus, the idea has been to make a shift from the paper-based system to electronic system whereby the communication and storage of data would be through the electronic medium rather than on paper.

The solution devised is by giving a statutory mechanism to the creation and use of digital signatures in the country. For this purpose, the required institution is created which would be responsible for issuance of Digital Signature Certificates and subsequent verification so that it can be used in e-commerce and e-governance. Certain 'deeming' provisions have been incorporated to supplement the existing laws and support them for the electronic era. The Act attempts to achieve the need of e-governance by providing for e-records. It provides a statutory support to electronic records so that they can be used for promotion of efficient delivery of government services.

Cyber crimes have been dealt with by providing for punishment for certain computer-related wrongs. Finally, the Act also provides for electronic transfer of funds. Various other Acts namely the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Reserve Bank of India Act, 1934 and the Bankers' Books Evidence Act, 1891 have been suitably amended to suit the electronic era.

2.4 APPLICATION OF THE ACT – THE EXTRA-TERRITORIAL EFFECT

The application of the Act and its extra-territorial effect can be well understood by a conjoint reading of **sections 1, 75 and 81**. The Act extends to the whole of India.[2] It applies also to any offence or contravention thereunder committed outside India by any person. However, an exception to this rule has been carved out in section 75 of the Act. Sub-section (1) of section 75 though in wider terms has made the Act applicable also to any offence or contravention committed outside India by any person irrespective of his nationality, this sub-

section has been made subject to the provisions of sub-section (2) which states that for the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention *involves* a computer, computer system or computer network in India. In effect, if an act (amounting to an offence under the Act) has been committed and where any computer, computer system or computers which are interconnected to each other in a computer network and which is in India is also involved (which might be either as a tool for committing the crime or as a target to the crime), then the provisions of the Act would apply to such an act. Section 81 provides effect to the provisions of the Act notwithstanding anything inconsistent contained in any other law for the time being in force. Therefore, effectively even if an offence (falling under the Act) is committed outside India by a foreigner, yet the courts in India would have the jurisdiction.

It is noticeable that with the IT Act, there has been a conceptual change with regard to the applicability of a statute. Due to the borderless connectivity of the computers through the Internet, and the ease with which one can commit a cyber crime in India while physically located beyond the boundaries of the country, the Parliament has made the provisions of the Act applicable irrespective of where the accused might be physically located. In contrast, if we see the extent of operation of the Indian Penal Code (IPC) under section 1,[3] it extends only 'to the whole of India except the State of Jammu and Kashmir'. No further applicability clause has been provided for. Section 2 of the IPC makes every person including a foreigner liable to punishment for every act or omission contrary to the provisions of IPC, of which he/she shall be guilty in India. Sections 3 and 4 of the IPC relate to the extra-territorial operation of the Code. But these sections too are restrictive in nature and not as broad as the combined effect of section 1(2) read with section 75 of the IT Act.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Discuss the extra-territorial effect of the IT Act. In what respect are its provisions are different from I.P.C.?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.5 DIGITAL SIGNATURES (CHAPTERS II, V, VI, VII, VIII)

Before we start discussing the topic of digital signature under the IT Act we must bear in mind that the expert committee to review the IT Act (discussed in the previous chapter) has proposed one major change that is the substitution of "digital signature" with "electronic signature" through an amendment to section 4. Digital signature is thus recognised as *one* of the types of electronic signature only. Therefore, very soon all references to digital signature in the IT Act may be substituted with electronic signature.

Any commercial transaction necessarily requires an agreement between two parties. For having a more secure transaction, people prefer having the agreement written and signed. With the advent of information technology and movement of the business on the Internet, it became necessary that there should be a secure form of entering into online contracts. In an online environment, the same is done through digital signatures.

Affixing a digital signature implies the electronic authentication of an electronic document. It has a two-fold purpose: (a) identification of the person who is signing the document; (b) authentication of the contents of the document which is being signed. In the Act, Chapters II, VI, VII and VIII are devoted to digital signatures. In these chapters have been laid down the mechanism for issuance, modification and revocation of digital signatures, the authorities who would be assigned the task related to digital signatures, their powers and functions, and the duties of the subscribers of the digital signatures.

The whole system creates a hierarchy in which at the top of is the Controller of Certifying Authorities who has the power to appoint Certifying Authorities and grant them the licence to issue Digital Signature Certificates. In turn, the Certifying Authorities can issue such Certificates to the subscribers. The process of application, renewal, suspension and revocation of licence of the Certifying Authorities has been provided. Likewise, the power to issue, suspend and revoke digital signature certificates is given in the hands of the Certifying Authorities. A hierarchy of digital signature certificates too has been provided for the purpose of verification of genuineness of digital signatures which ultimately can be verified by the Controller of Certifying Authorities who under the Act is the highest authority for digital signatures and related matters.

Section 2(p) of the Act defines 'digital signature' as 'authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3'. Chapter II of the Act has a single section that is section 3 providing for authentication of electronic records. Sub-section (1) of section 3 states that 'any subscriber may authenticate an electronic record by affixing his digital signature'. This forms the base of use of digital signature. Section 3(1) of the Act gives a legal sanctity to the usage of digital signatures in the country. A person can, if he/she wishes, use digital signatures to authenticate an electronic record and such authentication is now recognisable under the law.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is digital signature and what purpose is achieved by it?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.5.1 Controller of Certifying Authorities

At the top of the hierarchy of authorities under the Act for the purpose of issuance of digital signature certificates is the Controller of the Certifying Authorities. Under Section 17(1) of the Act, the Central Government has been empowered to appoint a Controller for the purposes of the Act.

The functions of the Controller have been enumerated under section 18 of the Act. These functions basically relate to Certifying Authorities or Digital Signature Certificate. It is the Controller's duty to regulate and control almost each and every activity of the Certifying Authorities. This is particularly important since the primary work of the Certifying Authorities is issuance of digital signatures and setting up infrastructure for its subsequent public verification. The Controller also has the function of specifying the form and content of a Digital Certificate and the key as also specifying the contents of written, printed, or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key. In case of conflict of interests between the Certifying Authorities and the subscribers, the Controller has been empowered to resolve the same.

Controller to act as Repository

Under section 20 of the Act, the Controller has been made the repository of all Digital Signature Certificates issued under the Act. The responsibility of the secrecy and security of the Certificates is on the Controller who shall make use of appropriate hardware, software and procedures that are secure from intrusion and misuse. The Controller is also under an obligation to

maintain a computerised database of all public keys in such a manner that such database and the public keys are available to any member of the public.

Recognition of Foreign Certifying Authorities

Section 19 of the Act gives the power to the Controller to recognise any Certifying Authority for the purposes of the Act subject to certain conditions.

Power to investigate contraventions

Section 28 empowers the Controller to take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

Directions to extend facilities to decrypt information

The Controller has, under sub-section (1) of section 69, the power to direct any agency of the Government to intercept any information transmitted through any computer resource. However, certain conditions have been laid down, which have to be fulfilled before such power can be exercised.

i) The Controller should be satisfied that such interception is necessary in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence.

ii) Such reasons must be recorded in writing.

iii) The direction to the agency must be by an order.

2.5.2 Licence to Issue Digital Signature Certificates

An elaborate discussion has been made in the Act with regard to the licence to issue Digital Signature Certificates. The provisions of the Act cover the application for licence, grant or rejection of licence, renewal of licence, suspension of licence, display of licence and surrender of licence. The Controller has been made the sole authority with regard to all these activities.

2.6 E-GOVERNANCE (CHAPTER III)

Chapter III covers the area of legal recognition of certain paper-based concepts and functions in electronic form. Sections 4 to 8 provide for legal recognition of electronic records, digital signatures, use of electronic records and digital signatures in Government and its agencies, retention of electronic records, and publication of rule, regulation, etc. in Electronic Gazette. This Chapter serves a dual purpose: (a) it introduces the principle of functional equivalence; and, (b) it provides the foundation to one of the averred objects of the Act of introducing e-governance by ‘facilitating electronic filing of documents with the government agencies’.

2.6.1 Functional-Equivalent Approach

Chapter III of the Act has adopted the ‘functional-equivalent’ approach. This approach is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or

functions could be fulfilled through electronic-commerce techniques. When adopting this approach in the UNCITARL Model Law, attention was given to the existing hierarchy of form requirements, which provides distinct level of reliability, traceability and inalterability with respect to paper-based documents. This approach singles out the basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by electronic documents, enable such e-documents to enjoy the same level of legal recognition as corresponding paper documents performing the same function enjoy. For example, if a contract is signed and sent as an electronic document, the chances of its reliability would be, in general situations, lesser than that of a paper-based document due to certain doubts as to its authenticity and chances of alteration of the contents. However, if the same electronic document is sent after being digitally signed by using a digital signature certificate issued by a trustworthy digital signature certificate provider, then, since it would be able to perform the same *functions* of reliability, traceability and inalterability as a paper-based document, it would receive legal sanction. What is noticeable is that a document in electronic form can, with suitable technical guards, perform the functions of writing much better than a paper-based document.

For the purpose of this Chapter, definition of 'electronic form', as provided under section 2(r) of the Act, is very material. It means, with reference to information, any information generated, sent, received, or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What is the functional equivalent approach? Discuss whether the electronically produced data with suitable technical safe-guard is as reliable, traceable and unalterable as the data written on paper.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.6.2 Legal Recognition of Electronic Records

Section 4[4] of the Act deems the fulfillment of the requirement of any information to be in writing in typewritten or printed form, if such information fulfills two conditions. Firstly, such information should be rendered or made available in an electronic form (for example, in a floppy disk). Secondly, such information is accessible as to be usable for a subsequent reference. The word 'accessible', as per the UNCITRAL guide, is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word 'usable' is not intended to cover only human use but also computer processing. 'Subsequent reference' seems to imply merely the need for future reference. The carefully worded section does not seem to lay down any stringent standards as to the reliability or durability of the electronic record. Rather, it merely requires that such information if made available at a certain point of time in electronic form should be available for usage at some future time as well. The purpose is to basically provide a legal sanctity to production of any information in electronic form. Whether such information provided is correct, or authentic, or unaltered, or reliable is not within the purview of this section. If the law provides something to be in writing, then, subject to certain conditions, the legal requirement of writing would be fulfilled if such information is in electronic form.

2.6.3 Legal Recognition of Digital Signatures

Section 5[5] proceeds on the functional-equivalent approach. It is based on the recognition of the functions of a signature in a paper-based environment. The following functions of a signature are considered in the UNCITRAL Guide[6]: (a) identifying a person; (b) providing certainty as to the personal involvement of that person in the act of signing; (c) associating such person with the content of the document.[7] Broadly, these being the functions of a signature, the purpose of section 5 is to merely introduce and give legal sanctity and acceptance to the use of digital signatures. It is not necessary as to what is the mode of signature; it may be paper-based or electronic. However, so long as the functions of the signature are being performed, such signature will receive legal recognition. Section 5 of the Act states that where any law provides that any information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. The Explanation to the Section further clarifies the ambit of the word 'signature' as to mean, 'with its grammatical variations and cognate expressions, with reference to a person, affixed of his hand written signature or any mark on any document'. Section 5, like section 4, has a limited field of operation. It is not the purpose of section 5 to ascertain whether the digital signature affixed is as per the rules prescribed, or whether the functions of a signature have been fulfilled. The purpose is merely to provide legal recognition to a digital signature on par with hand-written signature wherever the law requires the affixation of such signature.

2.6.4 Use of Electronic Records and Digital Signatures in Government and its Agencies

Section 6 provides for use of electronic records and digital signatures in government functioning. If any particular law requires filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government[8] in a particular manner, or the issuance or grant of any licence, permit, sanction or approval by whatever name called in a particular manner, or the receipt or payment of money in a particular manner, then, under sub-section (1) of the section 6, such requirement would be deemed to have been satisfied if such filing, issue, grant, receipt or payment, is effected by means of an electronic form. Such electronic form may be prescribed by the appropriate government. The appropriate government, under sub-section (2), has been given the power to make rules to prescribe the manner and format in which such electronic records shall be filed, created or issued, as also the manner or method of payment of any fee or charges for filing, creation or issuance of any electronic record.

Therefore, an application for a document say, a land record, if made in the prescribed electronic form to the revenue and land records department, it would be legally valid under section 6. Or, a grant of certificate of registration as a dealer by the government under a sales tax legislation in an electronic form is now legally recognisable.

2.6.5 Retention of Electronic Records

Various statutes provide for storage of information (for example, for tax purposes or auditing/accounting, etc.). Such information is generally stored on paper-based mode. However, with increase in computers for processing and storage of information, it became imperative to provide legal sanction to storage of information in electronic form. Modern trade works through information technology and requires it to retain all the information, though generated, sent or received in electronic form, in paper-based mode would be a step back. Section 7 of the Act permits retention of information in electronic form and gives legal recognition to retention of electronic records. Where any law provides that documents, records of information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in electronic form. The section deems the fulfillment of the legal requirement of paper-based retention of information if the same is done in electronic form.

2.7 SUMMARY

- In this unit we have examined in detail the objects and reasons for the IT Act, the applicability of the Act i.e. the extra territorial application of the Act, provisions relating to digital signatures, e-commerce and e-governance. This part of the IT Act deals with the recognition of the electronic record and its legalisation as an alternative to paper based records.

- The aim of the Act is to give legal recognition to the information collected, stored and utilized in electronic form so as to facilitate electronic commerce and e-governance.
- The Act gives legal recognition to digital signature and provides for the issuance, of it. It also provides for the controlling mechanism to check abuse of digital signature.
- The Act provides for the appointment of the controller of the certifying authority who shall issue licences to the authorities who can issue digital signatures. The Controller has also been granted powers to recognise foreign certifying authorities in this respect.
- The Act adopts the functional equivalent approach i.e. if the electronic records satisfy the same level of reliability as the paper document, it should be given the same recognition as the paper based record.

2.8 TERMINAL QUESTIONS

1) What is digital signature? How is it issued? Discuss the powers and functions of the controller of certifying authority and the certifying authorities.
2) What is the functional equivalent approach? Discuss how it is adopted in the Act with respect to the digital signature and electronic records. Do you think that the electronic records satisfy the test of reliability, traceability and inalterability in the same way as the paper based records?
3) What are the conditions of the recognition of electronic record? Do you think that the provisions contained in the Act adequately deal with the issue?

2.9 ANSWERS AND HINTS

1) The application of the Act and its extra-territorial effect can be well understood by a conjoint reading of **sections 1, 75 and 81**. The Act extends to the whole of India. It applies also to any offence or contravention thereunder committed outside India by any person. However, an exception to this rule has been carved out in section 75 of the Act. Sub-section (1) of section 75 though in wider terms has made the Act applicable also to any offence or contravention committed outside India by any person irrespective of his nationality, this sub-section has been made subject to the provisions of sub-section (2) which states that for the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention *involves* a computer, computer system or computer network in India. In effect, if an act (amounting to an offence under the Act) has been committed and where any computer, computer system or computers which are interconnected to each other in a computer network and which is in India is also involved (which might be either as a tool for committing the crime or as a target to the crime), then the provisions of the Act would apply to such an act. Section 81 provides effect to the provisions of the Act notwithstanding anything inconsistent

contained in any other law for the time being in force. Therefore, effectively even if an offence (falling under the Act) is committed outside India by a foreigner, yet the courts in India would have the jurisdiction.

It is noticeable that with the IT Act, there has been a conceptual change with regard to the applicability of a statute. Due to the borderless connectivity of the computers through the Internet, and the ease with which one can commit a cyber crime in India while physically located beyond the boundaries of the country, the Parliament has made the provisions of the Act applicable irrespective of where the accused might be physically located. In contrast, if we see the extent of operation of the Indian Penal Code (IPC) under section 1, it extends only 'to the whole of India except the State of Jammu and Kashmir'. No further applicability clause has been provided for. Section 2 of the IPC makes every person including a foreigner liable to punishment for every act or omission contrary to the provisions of IPC, of which he shall be guilty in India. Sections 3 and 4 of the IPC relate to the extra-territorial operation of the Code. But these sections too are restrictive in nature and not as broad as the combined effect of section 1(2) read with section 75 of the IT Act.

2) Affixing the digital signature implies the electronic authentication of an electronic document. It performs the same function as the signature by hand. The Act makes provision for the appointment of a Controller of Certifying Authorities that is empowered to grant licences to authorities who may issue digital signatures. The Act makes elaborate provisions in this regard.

3) Functional equivalent approach in the context of electronic signature and records mean that they perform similar functions as the signature by hand and paper based documents. If these are done with adequate safeguards, they are more reliable than their traditional counterparts.

2.10 REFERENCES AND SUGGESTED READINGS

1. Resolution no. A/RES/51/162. 30 Jan.1997.
2. S. 1(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.
3. S. 1. – This Act shall be called the Indian Penal Code, and shall extend to the whole of India except the State of Jammu and Kashmir.
4. S. 4. Legal recognition of electronic records. Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

   a) rendered or made available in an electronic form; and

   b) accessible so as to be usable for a subsequent reference.

5. S. 5. Legal recognition of digital signatures. Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.
6. Para. 53 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).
7. *Explanation.* — For the purposes of this section, "*signed*", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "*signature*" shall be construed accordingly.
8. S. 2(e). – 'appropriate Government' means as respects any matter, - (I) enumerated in List II of the Seventh Schedule to the Constitution; (ii) relating to any law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government.