UNIT 3 INFORMATION TECHNOLOGY ACT – PART II

Structure

3.1 INTRODUCTION

In the previous unit you have seen that various new concepts such as digital signature, e-governance, functional equivalent approach etc. have been introduced by the IT Act, 2000. The first unit of this block gave you some idea as to what types of challenges are faced by the legal system due to the advancement of information technology.

You may have understood the fact that these challenges require different types of adjudicatory mechanism and different types of offences and penalties to be incorporated in law because the existing law cannot deal adequately with these issues.

In this unit we shall discuss the adjudicatory mechanism provided in the IT Act. We shall also discuss the offences and penalties provided in the Act and how the offences under the Act be investigated. The investigation of IT related offences is a very complicated affair. In these types of investigations special kind of investigation techniques are applied.

The Act also amends certain provisions of Indian Penal Code, Indian Evidence Act etc. The objective of these amendments is to enlarge the definitions of certain offences so as to include within them the commission of these offences electronically and give legal recognition to evidence of electronic records.

While studying this unit it is recommended that apart from the copy of the IT Act, 2000, you should also keep the copies of the IPC, 1860 and Indian Evidence Act, 1872 with you for having a glance at the bare provisions of these Acts to understand the true scope of this unit.

3.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss the powers, functions and qualifications and what procedure is to be followed by the adjudicating officer and C.R.A.T., and discuss the penalties and offences in case of the contravention of the Act;
- define the term and discuss network service provider and his/her liabilities for offences committed using his/her network. What are the circumstances under which he/she may be exempted from such liabilities?
- describe amendments made by this Act in different statutes to give legal recognition to the electronically kept document, enlarge the definitions of certain offences to include within them the commitment of offences electronically and transfer of fund electronically.

3.3 ADJUDICATION (CHAPTER IX)

The Act provides for its own adjudicating mechanism and procedure. It appoints adjudicating officers conferring on them powers to adjudicate upon any allegations of contravention of the provisions of the Act or rules or regulations made thereunder. It also constitutes a Cyber Regulations Appellate Tribunal (CRAT) for the purpose of hearing appeals arising out of decisions of the adjudicating officer as also the Controller under various provisions of the Act.

3.3.1 Adjudicating Officer

Section 46 of the Act provides for appointment, powers and functions of the adjudicating officer. Under sub-section (1), the Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer. Such adjudicating officers should possess such experience in the field of Information Technology and legal or judicial experience as prescribed by the Central Government. The adjudicating officer is required to hold an inquiry and thereafter, adjudge whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under. If, after providing such opportunity and on the basis of inquiry made under sub-section (1), the adjudicating officer is satisfied that the person has committed the contravention, then, he/she may impose such penalty or award such compensation as he/she thinks fit in accordance with the provisions of that section.

3.3.2 Cyber Regulations Appellate Tribunal

Chapter X of the Act contains provisions relating to Cyber Regulations Appellate Tribunal (CRAT). The Central Government by notification will establish one or more appellate tribunals to be known as Cyber Regulations Appellate Tribunal (CRAT). The Central Government will also in such notification specify the matters and places in relation to which the CRAT may exercise jurisdiction. CRAT will consist of one person only ('the Presiding Officer') to be appointed by the Central Government, by notification.

Presiding Officer of CRAT

For appointment as a Presiding Officer of CRAT, a person will not be qualified unless he/she (a) is, or has been, or is qualified to be, a Judge of a High Court; or, (b) 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.

Appeal to and Procedure and Powers of the CRAT

The Central Government in exercise of its rule-making power under section 87 of the Act framed the Cyber Regulations Appellate Tribunal (Procedure) Rules, 200[1] regulating the procedure to be followed in applications made to the CRAT.

Section 57 of the Act provides for appeal to the CRAT. Sub-section (1) gives the right to appeal to any person who is aggrieved by the order of the Controller or an adjudicating officer under this Act to CRAT having jurisdiction in the matter. However, this right is subject to the provisions of sub-section (2) which prohibits any appeal against any order of an adjudicating officer made with the consent of the parties.

The appeal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.[2] As regards the procedure to be followed during an appeal, Section 58 of the Act provides that CRAT is not bound by the procedure laid down by the Code of Civil Procedure, 1908. However, it shall be guided by the principles of natural justice. Sub-section (2) of section 58 provides that the CRAT has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908.

Section 61 of the Act bars the jurisdiction of all other courts to entertain any suit or proceeding in respect of any matter which an adjudicating officer or the CRAT is empowered under this Act to determine. The section further provides that no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred under this Act.

Section 62 of the Act provides for an appeal to the High Court against the order of the CRAT. Such appeal can be made on any question of fact or law arising out of the order appealed against. The scope, therefore, of interference in the order of the CRAT by the High Court is quite wide.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Give a brief account of the powers and functions of the adjudicating officer and the CRAT.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.4 PENALTIES AND OFFENCES (CHAPTER IX & XI)

Penalties and offences are dealt with in different Chapters in the Act. Chapter IX, which also harbours provisions relating to adjudication, enumerates the various penalties and the entailing civil consequences. Chapter XI deals exclusively with offences.

3.4.1 Penalties

Three kinds of conduct have been listed out in the Act which would give rise to civil consequences. Firstly, any person involved in any action relating to damage to computer, computer system, etc., under section 43 of the Act, would be liable to damages. Second group pertains to failure to furnish information, returns, etc. under section 44. And finally section 45 contains the residuary clause.

Section 43 of the Act provides a list of activities which, if carried out by any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network, would cause such person who is carrying out the act to be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Such activities include:

A) Accessing or securing access to a computer, computer system or computer network. This in effect refers to unauthorized access.

B) Downloading, copying or extracting any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. This means data theft and would also include acts of copyright infringement like downloading of music.

C) Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

D) Damaging or causing to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network.

E) Disrupting or causing disruption of any computer, computer system or computer network.

F) Denying or causing the denial of access to any person authorized to access any computer, computer system or computer network by any means.

G) Providing 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 there under. This is a facet of hacking.

H) Charging the services availed of by a person to the account of another person by tampering with or manipulation any computer, computer system or computer network. This refers to theft of Internet hours.

Confiscation of computer, computer system, floppies, compact disks, tape drives or any other accessories in respect of which of any provision of this Act, rules, orders or regulations has been or is being contravened, can be resorted to under section 76.

3.4.2 Offences

Chapter XI of the Act enumerates the various acts which constitute an offence under the Act along with the punishment be it either imprisonment or fine or both. Such offences:

In case of offences committed by companies, such persons who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, will be, under sub-section (1) of section 85 of the Act, guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, if such person proves that the contravention took place without his/her knowledge or that he/she exercised all due diligence to prevent such contravention, he/she shall not be liable to punishment. Sub-section (2) of section 85 also deems a director, manager, secretary or any other officer of the company to be guilty of contravention and liable for punishment if it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of such person. ‘Company’, for the purpose of this section, has been explained to mean any body corporate and includes a firm or other association of individuals. ‘Director’, in relation to a firm, would mean a partner in the firm.

3.4.3 Investigation

Section 78 of the Act places the powers of investigation with a police officer not below the rank of Deputy Superintendent of Police. This provision overrides anything contrary in the Code of Criminal Procedure. Section 80 confers the powers on police officers to enter and search premises.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Discuss the provisions of the IT Act 2000 relating to the penalty and punishment.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.5 NETWORK SERVICE PROVIDER LIABILITY (CHAPTER XII)

The issue of Network Service Provider has gained importance with the increase of offences being committed via the Internet especially in the area of copyright infringement. They are being held up for abetting the offence by providing infrastructural facilities which help the offender to commit the offence. However, to provide immunity to them, section 79 of the Act provides for certain cases where they will not be liable. In case of any allegation of liability under the Act, rules or regulations against a Network Service Provider for any third party information or data made available by him/her, he/she shall not be liable if he/she proves that the offence or contravention was committed without his/her knowledge or that he/she had exercised all due diligence to prevent the commission of such offence or contravention. ‘Network service provider’, for the purpose of this section, has been explained to mean an intermediary. ‘Third party information’ is given to mean any information dealt with by a network service provider in his/her capacity as an intermediary.

To take an example, if A is hacking B's computer and using the network services provided by Z, a network service provider, then, to the extent that Z is able to prove that the offence was committed without his/her knowledge or that he/she had exercised all due diligence to prevent the commission of such offence, he/she will be saved from any liability by virtue of section 79 of the Act. However, what is worth taking note of is that the burden of proof has been shifted to the network service provider. It would not be very difficult for someone to just pull any network service provider into litigation and then burdening him with the task of proving due diligence and commission without knowledge. Keeping in mind the number of litigations that might ensue due to contraventions based on the Internet, the task for network service providers has really been reduced and immunity provided can still be burdensome. Alternatively, the initial burden of proving that enough communication was given to the network service provider should lie on the complainant. Thereafter, the onus could shift to the network service provider that there was no knowledge or that due diligence was exercised.

3.6 AMENDMENTS TO CERTAIN STATUTES

The Act, to further the acceptance and use of documents, evidence, and transfer of funds through electronic means, has amended the Indian Penal Code, Indian Evidence Act, Bankers' Books Evidence Act and Reserve Bank of India Act vide the First, Second, Third and Fourth Schedule respectively. As the Act proposes such heavy induction of use of electronic means for documents and signatures, as also governance, it became necessary to also amend certain penal statutes to bring it on par with the offences relating to or committed with the help of such electronic means. Many of such offences have already been enumerated in the Act itself. However, such offences relate to a new category which has emerged with the use of computer technology like hacking, damage to computer systems, etc. There is another set of offences which were already on the statute books but with the use of electronic means have taken a new dimension and their scope needs to be further widened by appropriate amendments in such statutes. This is what the amendments made by the Act purport to achieve.

3.6.1 Amendments to the Indian Penal Code, 1860

Certain provisions of the Indian Penal Code (IPC) have been amended by Section 91. These provisions primarily are offences relating to document. The aim is to also include 'electronic record' thereby including such offences which till now were only paper-based but can now also be paperless. For example, for the purpose of forgery, it is no more necessary that the document forged has to be signed (which traditionally would require a signature of a person on a paper-based document) but has now been extended to forgery by affixing a digital signature as well.

Largely, the amendments to the IPC can be categorised under five headings:

a) *Definition*: By insertion of section 29A, the definition of 'electronic record' as understood by section 2(1) (t) of the Act has been introduced in the IPC.

b) *Offences by or relating to public servants*: Section 167 deals with the offence committed by a public servant of framing an incorrect document with intent to cause injury. The amendment makes the public servant liable to punishment for the offence even in case of framing, preparation or translation of an electronic record.

c) *Offences of contempt of the lawful authority of public servants*: Chapter 10 of IPC deals with contempt of the lawful authority of public servants and is meant to enforce obedience and respect to their lawful authority. All the amendments made in this Chapter pertain to introduction of 'electronic record' by the side of 'document' and bringing on par both paper-based and paperless offences. Sections 172,[3] 173[4] and 175[5] have been amended to ensure that any action which was done by way of a paper-based document would still be an offence if done by way of electronic means.

d) *Offences relating to evidence*: Sections 192[6] and 204[7] have been amended under the Chapter relating to offences of false evidence and offences against public justice. After the amendments, the offence of fabricating false evidence would also include fabricating of a false electronic record. Likewise, any destruction of an electronic record would attract punishment under section 204.

e) *Offences in relation to document*: The major portion of the amendments made in the IPC is dedicated to the Chapter 18 that is offences relating to documents. All such offences pertaining to and based on the document have been given a wider scope and are applicable to electronic records as well. Such amendments primarily relate to use of electronic record and affixation of digital signatures for the purpose of forgery. Section 463 which makes forgery a punishable offence has been amended to include forgery by electronic record. Making of a false document under section 464 now includes dishonestly or fraudulently affixing any digital signature on any electronic record. 'Affixing digital signature' has been given the same meaning as assigned to it in section 2(1) (d) of the Act. Sections 466, [8] 468, [9] 470, [10] 471[11] and 474[12] have been amended to the same effect that is committing forgery by electronic record and affixing digital signature.

3.6.2 Amendments to the Indian Evidence Act, 1872

Section 92 of the Act amends certain provisions of the Evidence Act. These amendments can be summarized under four headings:

a) *Amendments permitting evidence in electronic form*: The definition of 'documentary evidence' under section 3 of the Evidence Act has been amended to include 'electronic records' as well. The definitions of 'certifying authority', 'digital signature', 'digital signature certificate', 'electronic form', 'electronic records', 'information', 'secure electronic record', secure digital signature and 'subscriber' have been inserted and are to have the same meaning as assigned to them in the IT Act. Section 17 of the Evidence Act dealing with the definition of admission now

includes a statement contained in electronic form as well. Sections 34[13] and 35[14] have been amended to include documents maintained in electronic form and electronic record respectively. Section 39 dealing with the evidence to be given when statement forms part of a conversation, document, book or series of letters or papers has been appropriately amended to include within its gamut 'electronic records'. Section 59 states that 'all facts except the contents of documents may be proved by oral evidence'. The amendment now permits proving of all facts by oral evidence except contents of document or electronic records. Therefore, one cannot by oral evidence prove the contents of an electronic record. Section131[15] has been amended to include any person in possession of an electronic record. The purpose of these amendments seems to basically inculcate the concept of evidence through electronic records. It creates a base for the amendments mentioned herein below. This set of amendments does not pertain to the questions of genuineness of the electronic records being produced as evidence or issues relating to their evidentiary value. The only object is to be able to produce evidence in electronic form in a court.

b) *Expert opinion on digital signatures*: Section 47A has been inserted whereby the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact[16] when the court has to form an opinion as to the digital signature of any person.

c) *Amendments relating to evidentiary value and evidence*: Certain amendments by way of insertions have been made by the IT Act in the Evidence Act to introduce electronic evidence in the Indian legal system. Such electronic evidence has been permitted by use of electronic records before a court of law. Section 3 as noted above was amended to include electronic records within the definition of evidence. In continuation to this amendment, certain further amendments have been made permitting electronic records to be evidence. As to what should be the rules to test the acceptability and genuineness of such electronic records as evidence has been introduced by these amendments. Section 22A relates to the relevance of oral admissions as to the contents of an electronic record unless the genuineness of the electronic record produced is in question. Section 65A and 65B collectively form the base for proving the contents of an electronic record. Sections 67A and 73A relate to proving and verification of digital signature respectively.

d) *Presumptions*: Introduction of evidence through electronic records has also led to certain additional presumptions under the Evidence Act. Section 81A provides for presumption of genuineness of Gazettes in electronic form. Certain presumptions have been provided for under sections 85A, 85B and 85C relating to electronic agreements, electronic records and digital signatures, and digital signature certificates. Section 85C relates to presumption with respect to electronic messages and section 90A with regard to presumption as to electronic records which are purported or proved to be five years old.

Please answer the following Self Assessment Question.

Self Assessment Question 3 & 4 *Spend 6 Min.*

Discuss in brief the amendment made by the IT Act, 2000 in the IPC. What is the objective behind these amendments?

Discuss the amendments made by the IT Act, 2000 in the Evidence Act, 1872. What is the purpose of this amendment?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.7 SUMMARY

In this unit we have discussed the adjudicatory mechanisms provided in the IT Act, 2000. We have also discussed the offences and penalties provided for in the Act including the liability of the service providers. Finally we have also examined the amendments made by the IT Act, 2000 in the Indian Penal Code, 1860 and Indian Evidence Act, 1872. The purpose of these amendments is to redefine various offences so as to include the commission of these offences electronically and to give the electronic records the same evidentiary value as the paper based documents.

3.8 TERMINAL QUESTIONS

1) Discuss the powers, functions and procedure for the adjudication of disputes under the IT Act, 2000.

2) What amendments has been made in the Indian Penal Code, 1860 and Indian Evidence Act, 1872 by the I.T. Act? What is the purpose of these amendments?

3.9 ANSWERS AND HINTS

1) The Act provides for the appointments of the adjudicating officers and cyber regulation appellate tribunals to settle the disputes relating to the offences and penalties provided in the act.

2) Three kinds of conduct have been listed out in the Act which would give rise to civil consequences. Firstly, any person involved in any action relating to damage to computer, computer system, etc., under section 43 of the Act, would be liable to damages. Second group pertains for failure to furnishing of information, returns, etc. under section 44. And finally section 45 contains the residuary clause.

Section 43 of the Act provides a list of activities which, if carried out by any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network, would cause such person who is carrying out the act to be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Such activities include:

A) Accessing or securing access to a computer, computer system or computer network. This in effect refers to unauthorized access.

B) Downloading, copying or extracting any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. This means data theft and would also include acts of copyright infringement like downloading of music.

C) Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

D) Damaging or causing to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network.

E) Disrupting or causing disruption of any computer, computer system or computer network.

F) Denying or causing the denial of access to any person authorized to access any computer, computer system or computer network by any means.

G) Providing 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 there under. This is a facet of hacking.

H) Charging the services availed of by a person to the account of another person by tampering with or manipulation any computer, computer system or computer network. This refers to theft of Internet hours.

Confiscation of computer, computer system, floppies, compact disks, tape drives or any other accessories in respect of which any provision of this Act, rules, orders or regulations has been or is being contravened, can be resorted to under section 76.

Offences

Chapter XI of the Act enumerates the various acts which constitute an offence under the Act along with the punishment be it either imprisonment or fine or both. Such offences:

In case of offences committed by companies, such persons who, at the time the contravention was committed, was in charge of, and was responsible, to, the company for the conduct of business of the company as well as the company, will be, under sub-section (1) of section 85 of the Act, guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, if such person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, he shall not be liable to punishment. Sub-section (2) of section 85 also deems a director, manager, secretary or any other office of the company to be guilty of contravention and liable for punishment if it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of such person. 'Company', for the purpose of this section, has been explained to mean any body corporate and includes a firm or other association of individuals. 'Director', in relation to a firm, would mean a partner in the firm.

3 & 4) The objective of the amendments in the various statutes by this act is to give same status to the electronic records and signature as the paper based documents and signature underhand.

3.10 REFERENCES AND SUGGESTED READINGS

1. *Vide* G.S.R. 791 (E). 17 Oct. 2000.
2. S. 57(6) of the IT Act, 2000.
3. S. 172 of the Indian Penal Code. - Absconding to avoid service to summons or other proceedings.
4. S. 173 of the Indian Penal Code. - Preventing service of summons or other proceeding, or preventing publication thereof.
5. S. 175 of the Indian Penal Code. - Omission to produce document to public servant by person legally bound to product it.
6. S. 192 of the Indian Penal Code. - Fabricating false evidence.
7. S. 204 of the Indian Penal Code. - Destruction of document to prevent its production as evidence.
8. S. 466 of the Indian Penal Code. - Forgery of record of Court or of public register, etc.
9. S. 468 of the Indian Penal Code. - Forgery for purpose of cheating.
10. S. 470 of the Indian Penal Code. - Forged document.
11. S. 471 of the Indian Penal Code. - Using as genuine a forged document.

12. S. 474 of the Indian Penal Code. - Having possession of document described in S. 466 or 467, knowing it to be forged and intending to use it as genuine.

13. S. 34 of the Evidence Act. - Entries in books of account when relevant.

14. S. 34 of the Evidence Act. - Relevance of entry in public record, made in performance of duty.

15. S. 131 S. 34 of the Evidence Act. - Production of documents or electronic records which another person, having possession, could refuse to produce.

16. This has an important bearing keeping in mind S. 5 of the Evidence Act which states that, 'Evidence may be given in any suit or proceeding of the existence or non-existence of every fact in issue and of such other facts as are hereinafter declared to be relevant, and of no others.'