UNIT 14: INFORMATION TECHNOLOGY (IT) ACT

Structure

14.0 INTRODUCTION

In this Unit, we shall examine the provisions of the Information Technology Act, 14000, and its amendments 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 new concepts such as “digital signature”, “e-governance”, etc. The Act gives legal recognition to electronic records and treats them at par with the paper-based system if all the safeguards are

followed. We shall also 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 kinds of investigation techniques are applied.

The Act also amends certain provisions of the 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.

14.1 LEARNING OUTCOMES

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 electronic signature;
- discuss the provisions relating to e-governance and legal recognition of electronic records;
- discuss the process of adjudication;
- discuss the penalties and offences in case of the contravention of the Act;
- define the term and discuss network service provider; and
- describe the amendments of this Act and its criticism.

14.2 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 utilised 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 United Nations Commission adopted the Model Law on Electronic Commerce on International Trade Law. It recommended the States to give 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 the electronic system whereby the communication and storage of data would be through the electronic medium rather than on paper.

The solution is by giving a statutory mechanism to create and use digital signatures in the country. For this purpose, the required institution is created, which would be responsible for the 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 for e-governance by providing for e-records. It provides statutory support to electronic records so that they can be used for the promotion of efficient delivery of government services. Cybercrimes have also been dealt with by providing punishment for certain computer-related wrongs. Finally, the Act provides for the electronic transfer of funds.

14.3 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. It also applies to any offence or contravention there under 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 also applies 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 (14), 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.

Due to the borderless connectivity of the computers through the Internet and the ease with which one can commit a cybercrime 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.

14.4 ELECTRONIC SIGNATURES

The concept of electronic signature was introduced under section 3A of the Information Technology (Amendment) Act 14008. Sec 14 (ta) of Information Technology Act 14000 had defined electronic signature as "Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature".

The adoption of 'electronic signature' has made the Act technological neutral as it recognises both the digital signature method based on cryptography technique and electronic signature using other technologies.

Section 3A of the Information Technology Act 14000 is based on Article 6, "Compliance with a requirement for a signature" of UNCITRAL Model Law on Electronic Signatures 14001. According to the United Nations Commission on International Trade Law (UNCITRAL), electronic authentication and signature methods may be classified into the following categories:

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those are based on the user's physical features, i.e., biometrics.
- Those are based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Without falling under any of the above categories, types of authentication and signature methods might also be used to indicate the originator of electronic communication (Such as a facsimile of a handwritten signature or a name typed at the bottom of an electronic message).

Check Your Progress: 1

Note: 1) Use the space below for your answers.

2) Compare your answers with those given at the end of this Unit.

1. Discuss the extra-territorial effect of the IT Act in your own words.

   ……..

   ……..

2. What are the electronic authentication and signatures methods categories, as per the UNCITRAL?

   ……..

   ……..

14.5 E-GOVERNANCE

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 the 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 objectives of the Act of introducing e-governance by 'facilitating electronic filing of documents with the government agencies.

14.5.1 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 to determine how those purposes or functions could be fulfilled through electronic-commerce techniques. When adopting this approach in the UNCITRAL Model Law, attention was given to the existing hierarchy of form requirements, which provides a distinct level of reliability, traceability, and inalterability regarding paper-based documents. This approach singles out the basic functions of paper-based form requirements, with a view to providing criteria which, once electronic documents meet them, enable such e-documents to enjoy the same level

of legal recognition as corresponding paper documents performing the same function. 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 a legal sanction.

14.5.2 Legal Recognition of Electronic Records

Section 4 of the Act deems the fulfilment of the requirement of any information to be in writing in typewritten or printed form if such information fulfils 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 purpose is to basically provide legal sanctity to the production of any information in electronic form. With reference to information, it means any information generated, sent, received, or stored in media, magnetic, optical, computer memory, microfilm, computer-generated micro fiche or similar device.

14.5.3 Legal Recognition of Digital Signatures

Section 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:

(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. 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 signatures 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.

14.5.4 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 in paper-based mode. However, with the increase in computers for processing and storing information, it became imperative to provide legal sanctions to the storage of information electronically. 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 the retention of information in electronic form and gives legal recognition to electronic records retention.

14.6 ADJUDICATION

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.

14.6.1 Adjudicating Officer

Section 46 of the Act provides for the adjudicating officer's appointment, powers, and functions. 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 thereunder. 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.

14.6.2 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.

In the exercise of its rule-making power under section 87 of the Act, the Central Government framed the Cyber Regulations Appellate Tribunal (Procedure) Rules, 14000 regulating the procedure to be followed in applications made to the CRAT.

Section 57 of the Act provides for an appeal to the CRAT. Sub-section (1) gives the right to appeal to any person who is aggrieved by 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 (14), 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.

14.7 PENALTIES AND OFFENCES

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.

14.7.1 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 the computer, computer system, etc., under section 43 of the Act, would be liable to damages by way of compensation not exceeding one crore rupees to the person so affected. The 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, including:

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

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

H) Charging the services availed of by a person to another person's account by tampering with or manipulating any computer, computer system or computer network. This refers to the 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.

14.7.2 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.

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 the 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, suppose such a person proves that the contravention took place without his/her knowledge or that he/she exercised all due diligence to prevent such contravention. In that case, he/she shall not be liable to punishment. Sub-section (14) 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 anybody corporate and includes a firm or other association of individuals. 'Director', in relation to a firm, would mean a partner in the firm.

Check Your Progress: 2

Note: 1) Use the space below for your answers.

2) Compare your answers with those given at the end of this Unit.

1. What is the equivalent functional approach? Discuss how it is adopted in the Act with respect to digital signature and electronic records.

   ……..

   ……..

2. Give a brief account of the powers and functions of the adjudicating officer and the CRAT in your own words.

   ……..

   ……..

3. Discuss the provisions of the IT Act 14000 relating to penalty.

   ……..

   ……..

14.8 NETWORK SERVICE PROVIDER LIABILITY

The issue of Network Service Providers 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 that help the offender commit the offence. However, section 79 of the Act provides for certain cases where they will not be liable to provide immunity to them. 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.

14.9 AMENDMENTS TO INFORMATION TECHNOLOGY ACT, 14000

14.9.1 Information Technology (Amendment) Act, 14008

A major amendment of the IT Act 14000 was made in 14008. The amendment was passed on 1414 December 14008 without any debate in Lok Sabha and by the Rajya Sabha on the next day. President Pratibha Patil signed the proposed amendment into law on 5 February 14009. The IT (Amendment) Act 14008 aimed at tightening procedures and safeguards for monitoring and interception of data to prevent cybercrimes. Besides monitoring and interception, the amended Act also deals with the Indian Computer Emergency Response Team (ICERT) appointment, which deals with computer security and situations arising from cyber-attacks. Additionally, provisions have been made addressing pornography, child porn, cyber terrorism and voyeurism. The following amendments (Sections and Provisions) were made:

a) *Section 66A:* Section 66A of the IT (Amendment) Act, 14008 prohibits sending offensive messages through a communication device (i.e. through an online medium). The types of information these covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of "causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will". One can face imprisonment up to 3 years along with a fine under this section.

b) *Section 67 and 67A*: Section 67 and 67(A) of the IT (Amendment) Act, 14008 prohibits sending of obscene and sexually explicit content through a communication device, respectively.

c) Section 69: Section 69 has been redrafted, enabling Government agencies to intercept, monitor or decrypt any electronic information with the help of subscribers, intermediary or person in charge of computer resources.

d) *Section 69A:* Section 69A of the IT (Amendment) Act, 14008, allows the Central Government to block content where it believes that this

content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. The Government has to adhere to a set of procedures and safeguards when doing so have been laid down in what has become known as the Blocking Rules.

e) *Section 79:* Section 79 of the Information Technology (Amendment) Act, 14008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute a move towards the privatisation of censorship in India.

Criticism of the Information Technology (Amendment) Act, 14008

IT (Amendment) Act, 14008 faced criticism in the form of restriction of free speech, constitutionality of the amendment, surveillance and data privacy. In lieu of Section 66(A), which was challenged multiple times, on 144 March 14015, the Supreme Court of India verdict that Section 66A is entirely unconstitutional. The Court said that Section 66A of IT Act 14000 "arbitrarily, excessively and disproportionately invades the right of free speech" provided under Article 19(1) of the Constitution of India. Similarly, the ban on Chinese apps based on Section 69A has been criticised for possibly being in conflict with Article 19(1)(a) of the Constitution of India, ensuring freedom of speech and expression to all, as well as possibly in conflict with WTO agreements. But the Court turned down a plea to strike down sections 69A and 79 of the Act, which deals with the procedure and safeguards for blocking certain websites.

14.9.2 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 140141

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 140141 is secondary or subordinate legislation that suppresses India's Intermediary Guidelines Rules 14011. The IT Rules, 140141, have stemmed from Section 87 of the IT Act, 14000 and are a combination of the draft Intermediaries Rules, 14018 and the OTT Regulation and Code of Ethics for Digital Media.

The IT Rules, 140141 aim to serve a dual purpose: (1) increasing the accountability of the social media platforms (such as Facebook, Instagram, Twitter etc.); and (14) empowering the users of social media by establishing a three-tier redressal mechanism for efficient grievance resolution. The IT Rules 140141 are to be governed as:

1. Guidelines Related to Social Media to Be Administered by Ministry of Electronics and IT
2. Digital Media Ethics Code Relating to Digital Media and OTT Platforms to Be Administered by Ministry of Information and Broadcasting

The salient features of the rules are:

- The IT Rules 140141 aim to empower ordinary users of social media platforms and OTT platforms with a mechanism for redressal and

timely resolution of their grievances with the help of a Grievance Redressal Officer (GRO) who should be a resident in India.

- Special emphasis has been given to the protection of women and children from sexual offences, fake news and another misuse of social media.
- The rules stress the point that online content publishers and social media intermediaries should follow the Constitution of the country and subject themselves to domestic laws.
- Identification of the "first originator of the information" would be required in case of an offence related to the sovereignty and integrity of India. A Chief Compliance Officer, a resident of India, also needs to be appointed, and that person shall be responsible for ensuring compliance with the Act and Rules. A monthly compliance report mentioning the details of complaints received and action taken on the complaints would be necessary.
- The OTT platforms, online news and digital media entities, on the other hand, would need to follow a Code of Ethics. Under the new rules, OTT platforms would be called 'publishers of online curated content'. They would have to self-classify the content into five categories based on age and use parental locks for age above 13 or higher. They also need to include age verification mechanisms for content classified as 'Adult'.

Criticism of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 140141

IT Rules, 140141 have faced criticism on various counts:

- Social media companies like WhatsApp have expressed apprehensions about the provisions in the new rules, which require them to identify traceability when required to do so by authorities. They contend that this could possibly lead to the breaking of end-to-end encryption, which in turn can compromise users' privacy.
- Rule 4(14), which makes it mandatory for every social media intermediary to enable tracing of originators of information on its platform, purportedly in furtherance of Section 69 of the IT Act, violates Article 19(1)(a) (Freedom of Speech and Expression).
- The creation of a grievance redressal mechanism through a governmental oversight body (an inter-departmental committee constituted under Rule 14) amounted to excessive regulation.

14.10 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 that has emerged with the use of computer technology like hacking, damage to computer systems, etc. There is another set of offences that 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.

Check Your Progress: 3

Note: 1) Use the space below for your answers.

2) Compare your answers with those given at the end of this Unit.

1. Discuss the IT (Amendment) Act, 14008, in your own words. Explain the criticism faced by the amendment from a legal perspective.

   ……..

   ……..

2. Discuss the IT Rule, 140141, in your own words. Explain the criticism faced by the amendment from a legal perspective.

   ……..

   ……..

14.11 LET US SUM UP

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 Act aims to give legal recognition to the information collected, stored, and utilised electronically to facilitate electronic commerce and e-governance. The Act also gives legal recognition to electronic signatures and provides for its issuance. It also provides a controlling mechanism to check the abuse of digital signatures. The Act adopts the equivalent functional 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.

We have also discussed the adjudicatory mechanisms provided in the IT Act, 14000. Furthermore, this Unit also emphasises the offences and penalties provided for in the Act, including the liability of the service providers. Finally, we have also examined the amendments made in the IT Act 14000 in the form of the IT (Amendment) Act, 14008 and IT Rules, 140141. We have also briefly looked at the amendments made by the IT Act, 14000 and the purpose of these amendments.

14.12 FURTHER READINGS

1. Information Technology Act, 14000
2. Information Technology (Amendment) Act, 14018

3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 140141

4. Manohar Parrikar Institute for Defence Studies and Analyses. https://www.idsa.in/idsacomments/it-rules-140141-dbhattacharya-0406141

5. Press Information Bureau. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749

6. PRS Legislative Research. https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-140141

14.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress: 1

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 also applies to any offence or contravention there under committed outside India by any person. Due to the borderless connectivity of the computers through the Internet and the ease with which one can commit a cybercrime 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.

2. According to the United Nations Commission on International Trade Law (UNCITRAL), electronic authentication and signature methods may be classified into the following categories:

   - Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
   - Those are based on the user's physical features, i.e., biometrics.
   - Those are based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
   - Without falling under any of the above categories, types of authentication and signature methods might also be used to indicate the originator of electronic communication (Such as a facsimile of a handwritten signature or a name typed at the bottom of an electronic message).

Check Your Progress: 2

1. 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. This approach singles out the basic functions of paper-based form requirements, with a view to providing criteria which, once electronic documents meet them, enable such e-documents to enjoy the same level of legal recognition as corresponding paper documents performing the same function.

2. 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. 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 the computer, computer system, etc., under section 43 of the Act, would be liable to damages. The 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.

Check Your Progress: 3

1. The IT (Amendment) Act 14008 aimed at tightening procedures and safeguards for monitoring and interception of data to prevent cybercrimes. Besides monitoring and interception, the amended Act also deals with the Indian Computer Emergency Response Team (ICERT) appointment, which deals with computer security and situations arising from cyber-attacks. Additionally, provisions have been made addressing pornography, child porn, cyber terrorism and voyeurism.

   Criticism: Restriction of free speech, the constitutionality of the amendment, surveillance and data privacy.

2. The IT Rules, 140141 aim to serve a dual purpose: (1) increasing the accountability of the social media platforms (such as Facebook, Instagram, Twitter etc.); and (14) empowering the users of social media by establishing a three-tier redressal mechanism for efficient grievance resolution. Rules to be administered by the Ministry of Electronics and IT include the due diligence required of intermediaries and the grievance redressal mechanism. Rules to be administered by the Ministry of Information and Broadcasting include a code of ethics, a self-classification system and an oversight mechanism.

   Criticism: Violation of Freedom of Speech and Expression, Right to Privacy and Excessive Regulation

NOTES

NOTES