P.G. Diploma Cyber Law

E-tutorials

Directorate of Distance Education
University of Kashmir, Srinagar
190006
(2011& 2016)

E-TUTORIAL NO.4-7

SUPPLIMENTARY

4 Amendment to the Information Technology Act

To overcome the existing inadequacies and practical difficulties in implementation of the Information technology Act, to address some of the emerging issues that has arisen from the use of cyberspace and the growing number of cybercrimes, the Government of India tabled the Information Technology amendment Bill, 2006 before both the houses of Parliament in December, 2006, which referred the said amendment bill to the Parliamentary Standing Committee on Information Technology. The Parliamentary Standing Committee, headed by Shri Nikhil Kumar, MP examined the proposed amendments in a comprehensive manner and thereafter gave its report and recommendations thereon. After examining the said recommendations, the Central Government brought the Information Technology Amendment Bill, 2008 in Parliament, which was passed by both the houses of Parliament on December 23and 24, 2008. It got the Presidential assent on February 5, 2009 and was notified for effectiveness on October 27, 2009. Information technology Act 2000 consisted of 94 sections segregated into 13 chapters. Four schedules form part of the Act. In the 2008 version of the Act, there are 124 sections (excluding sections that have been omitted from the earlier version) and 14 chapters. Schedule I and II have been replaced

With the introduction of Information Technology (Amendment) Act 2008 many changes have been made in the IT Act 2000 .Here the discussion is focused on the applicability of the Information Technology (Amendment) Act 2008 and on the main provisions relating to the **Legal Recognition, Authentication and Validity Of Electronic Records and Electronic Signatures, security procedure and practices**, how the Electronic Records and Digital Signatures can be used by Government and its agencies and delivery of e-Governance services by private service providers.

2.4 Important Definitions.

Communication Device :Section 2 (1)(ha) added in IT act 2008 to define " communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

In section 2(1)(j) "Computer Systems" and "Communication Devices", "Wire" "Wireless" added.

Cyber café: Section 2(1) (na) introduced to define the term cyber café to means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

Cyber security: Section 2 (1) (nb) has introduced the term "cyber security" which means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Indian Computer Emergency Response Team: Section 2 (1) (ua) defines "Indian Computer Emergency Response Team, which means an agency established under sub-section (1) of section 70B. Section 70B provides that Indian Computer Emergency Response Team to serve as national agency for incident response. As per Section 70(4), the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,

(a) Collection, analysis and dissemination of information on cyber incidents;

(b) Forecast and alerts of cyber security incidents;

(c) Emergency measures for handling cyber security incidents;

(d) Coordination of cyber incidents response activities;

(e) Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, presentation, and response and reporting of cyber incidents;

(f) Such other functions relating to cyber security as may be prescribed.

Parties that exist in connection with data text message

The Act recognizes that there are three parties that exist in connection with data text message viz., Originator, Addressee, intermediary.

Originator, means the person who sends ,generate, stores or transmits the electronic message or causes it to be sent, generated, stored or transmitted to any person.[sec 2(1)(za)]

'Addressee', means a person who is intended by the originator to receive the electronic record but does not include any intermediary [sec 2(1)(b)].

"intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes [Sec 2(1) (w)].

---

5. DIGITAL SIGNATURES AND ELECTRONIC SIGNATURE (Chapters II, V, VI, VII, VIII of IT Act)

Today with the advent of internet many contract have been entered online and however the validity of contract requires the identification of the persons signing the electronic document and also the authentication of the contents of the electronic document which is being signed. The most common method of signing electronically for giving the electronic authentication to the electronic document is the digital signature which often uses "public key cryptography", but it is only one of the types of electronic signature. Now the term "digital signature" has been replaced with "electronic signature" to make the Act more technology neutral. Section 2(1) (ta) and 2(1) (tb) has introduced the term of "Electronic Signature" and "Electronic Signature Certificate". "Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature. "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate.

5. 1 Authentication of Electronic Records

Chapters II, VI, VII and VIII are devoted to Electronic signatures. The Section 3 of the act provides 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 and this gives a legal sanctity to the usage of digital signatures in the country by a person to authenticate an electronic record. However by the IT act (amendment 2008) new Section 3 A has been introduced to define Electronic Signature which is an enabling provision permitting systems other than public key Infrastructure (PKI) based systems for authentication purpose. It provides that a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which (a) is considered reliable; and (b) may be specified in the Second Schedule. Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable (see proviso to sec 3A(4)). Electronic signature or electronic authentication technique shall be considered reliable if (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;(c) any alteration to the electronic signature made after affixing such signature is detectable;(d) any alteration to the information made after its authentication by electronic signature is detectable; and (e) it fulfils such other conditions which may be prescribed.

5.2 Secure Electronic records and security procedure and practices

The chapter V deals with the secure Electronic records, Electronic signatures has been deemed secured if at the time of affixing signature, the signature creation data was under the exclusive control of signatory and no other person and was also stored and affixed in such exclusive manner as may be prescribed (see section 15 of the IT act, as amended 2008). In case of digital signature, the "signature creation data" means the private key of the subscriber (explanation to sec 15).The security procedure and practices may be prescribed by central government with regard to commercial circumstances, nature of transactions and such other related factors as it may consider appropriate(sec16 of the IT act,2008).

5.3 Regulation of Certifying Authorities

Chapter VI deals with regulation of certifying authorities. Under Section 17(1) of the Act, the Central Government has been empowered to appoint a Controller and

also deputy and assistant controllers, the other officers and employees to assist the controller for discharge of his functions. this Controller of Certifying Authorities as notified by the central government, has the power to recognise foreign certificate authorities as Certifying Authorities (sec 19) and to lay down the duties and standards to be maintained by certifying authorities, specify form and content of electronic signature certificate and the Key; it can also specify the contents of written, printed, or visual materials and advertisements that may be distributed or used in respect of a electronic Signature Certificate and the public key; has power to resolve any conflict of interests that arise between the Certifying Authorities and the subscribers (see section 18 of the Act for functions of controller). However the responsibility of *Controller to act as Repository* under section 20 of the Act has been omitted. The whole mechanism for licence to issue electronic signature certificates, procedure for grant or rejection of licence, suspension and revocation of electronic signatures has been laid in sections 21 to 26 of the act. The Controller has been made the sole authority with regard to all above discussed activities but he can delegate any of his power in writing to the deputy and assistant controllers and any officer (sec-27). Section 28 empowers the Controller to take up investigation for any contravention of the provisions of this Act, rules or regulations made there under.

The controller has power to give directions to certifying authorities or any employee of such authorities to take such measures or cease carrying on such activities as specified in order if those are necessary to ensure compliance with the provisions of this act, rules or any regulation made there under sec 68 (1). According to Section 68 (2) any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both(see IT amendment act 2008)

5.4 Electronic Signature Certificates

Chapter VII further provides that certifying authorities can issue electronic certificate to the applicant or can also reject the application by recording reasons in writing and after giving reasonable opportunity to applicant for showing cause against the proposed rejection (sections 35, 36 of the act), certifying authorities like the controller also has the power to issue, suspend and revoke digital signature certificates (sections 35-39 of the act).

5.5 E-Governance

Chapter III has introduced the principle of functional equivalence giving recognition to the alternative method of communication and storage of information other than traditional paper based method. It provides foundation to one of the objects of the Act to introducing e-governance by facilitating electronic filing of documents with the Government agencies. this chapter covers the area of legal recognition to certain matters and information in electronic form, which should be in writing, typewritten or in printed form as per the requirement of law

Sections 4 to 8 provides for legal recognition of electronic records, electronic signatures, use of electronic records and electronic signatures in Government and its agencies, retention of electronic records, and publication of rule, regulation, etc. in Electronic Gazette.

---

6. LEGAL RECOGNITION OF ELECTRONIC RECORDS

Section 4 of the act provides for legal recognition of electronic records- the Act deems that the requirement of any information to be in writing in typewritten or printed form is fulfilled, if such information fulfils following two conditions.

(a) Such information should be rendered or made available in an electronic form

(b) Such information is accessible as to be usable for a subsequent reference.

The UNCITRAL Model law states that where the law requires information to be in writing, that requirement is met by data message if the information contained therein is accessible so as to be usable for subsequent reference (Art 6(1)). Here the word accessible means and requires that the information in the form of computer data should not only be readable and interpretable but the software that is be necessary to render such information readable should also be retained (as per the UNCITRAL Guide), the term ‘usable’ covers not only human use but also computer processing, the ‘Subsequent reference’ may imply merely the need for future reference. The main object of the section 4 of the IT act is to basically provide a legal sanctity to production of any information in electronic form however there is no requirement laid down that the electronic record should be reliable and the information provided is unaltered, correct and authentic.

Legal recognition of Electronic Signatures

Section 5 of the act provides for Legal recognition of digital signatures. It lays down that 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.

This section is based on the recognition of the functions of a signature in a paper-based environment. The above provisions stipulates that the digital signature must be affixed in the manner as may be prescribed by the Central Government and the under section 6(2), Central Government 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 per the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), the signature has the following functions of identifying a person:

- It provides certainty as to the personal involvement of that person in the act of signing;
- Associate such person with the content of the document.

The section 5 of the act has merely given the legal sanctity and acceptance to the use of electronic and digital signatures and the mode of signature is not significant, it may be paper-based or electronic. The Explanation to the Section further clarifies the ambit of the word ‘signature’ as to mean, ‘with its grammatical variations and cognate expressions, shall with reference to a person, means affixing of his hand written signature or any mark on any document the expression "signature" shall be construed accordingly.

The purpose of section 5 is not to ascertain whether the electronic 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 an electronic signatures in parity with hand-written signature in the cases where the law requires the affixation of such signature.

Use of Electronic Records and Electronic Signatures in Government and its agencies

Section 6 provides for use of electronic records and digital signatures in government functioning- it provides that where any law requires that the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner, or the issuance or grant of any license, permit, sanction or approval by whatever name called in a particular manner, or the receipt or payment of money in a particular manner, then, not withstanding anything contained in any other law for the time being in force , 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 which may be prescribed by the appropriate Government(Section 6(1)). 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. The expression 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(sec 2(e) of the act).

Retention of* Electronic *Records

There are various laws that provides for storage of document, information or record for various purpose may be tax, auditing etc. and conventionally this requirement is completed through pen and paper based record. However, with change in mode of technology and more use of computers for processing and storage of information, it has became imperative that legal sanction be accorded to storage of information in electronic form. Section **7** of the Act permits retention of information in electronic form and gives legal recognition to retention of electronic records. Sec 7(1) lays down that 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 fulfilment of the legal requirement of paper-based retention of information if the same is done in electronic form.

Further the government has been also given responsibility to get the documents, records or information in electronic form to be audited wherever such physical records were subject to audit (Section 7A).

Can person insist government for document, information or records in electronic form? :However the above provisions do not confer any rights on the any person to insist that government central/state and there departments ,ministries have to accept, issue, create, retain and preserve any document in form of electronic record or to effect any monetary transaction in the electronic form(sec 9 of the act).

Validity of electronic records :Sec 10A in the Act has been introduced for providing validity of contracts formed through electronic means - In a contract formation, when the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

---

7. DELIVERY OF SERVICES BY SERVICE PROVIDER

The IT act (amendment 2008) has introduced new section to provide for appointment of Service Providers to enable delivery of e-Governance services by private service providers.

Sec 6A.(1) provides that the appropriate Government may, for the purposes for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify by notification in the Official Gazette.

For the purposes of this section, authorised service provider includes:

- any individual,
- private agency,
- private company, partnership firm,
- sole proprietor firm

- or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector(see Explanation to sec)

- **e-service charges by the service providers** - sec 6A (2) of the Act provides that the appropriate Government may also authorise any service provider authorised under sub-section (1) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service. Further sec 6A (3) provides that subject to the provisions of sub-section (2), the appropriate Government may authorise the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.
- **Duty on the appropriate Government to specify the scale of service charges by the service providers-** sec 6 (4) cast duty on the appropriate Government to specify the scale of service charges which may be charged and collected by the service providers under this section by notification in the Official Gazette. Further the appropriate Government may specify different scale of service charges for different types of services.