THE INFORMATION TECHNOLOGY ACT, 2000

Introduction

Connectivity via the Internet has greatly abridged geographical distances and made communication even more rapid. While activities in this limitless new universe are increasing incessantly, laws must be formulated to monitor these activities. Some countries have been rather vigilant and formed some laws governing the net. In order to keep pace with the changing generation, the Indian Parliament passed the much-awaited Information Technology (IT) Act, 2000 (hereinafter referred to as 'the Act')

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft.

After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber crime and to facilitate speedy locating of a cyber criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. As Mr. Dewang Mehta, Executive Director of the National Association of Software and Service (NASSCOM) said, "it would only result in closing down of all cyber cafés and ultimately deprive people of these facilities." Finally, this suggestion was dropped by the IT Ministry in its final draft.

The Union Cabinet approved the bill on May 13, 2000 and both the houses of Parliament finally passed it by May 17, 2000. The Presidential Assent was finally received in the third week of June 2000.

The Preamble to the Act states that it aims at providing 'legal recognition for transactions carried out by means of electronic data interchange and other

means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and aims at facilitating electronic filing of documents with the Government agencies.

The General Assembly of the United Nations had adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its General Assembly Resolution A/RES/51/162 dated January 30, 1997. The Indian Act is in keeping with this resolution that recommended that member nations of the UN enact and modify their laws according to the Model Law.

Thus with the enactment of this Act, Internet transactions will now be recognised, on-line contracts will be enforceable and e-mails will be legally acknowledged. It will tremendously augment domestic as well as international trade and commerce.

Q1. Explain the important provisions relating to the Digital Signature in the IT Act 2000

The Act has adopted the Public Key Infrastructure (PKI) for securing electronic transactions. As per Section 2(1)(p) of the Act, a digital signature means an authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the other provisions of the Act. Thus a subscriber can authenticate an electronic record by affixing his digital signature. A private key is used to create a digital signature whereas a public key is used to verify the digital signature and electronic record. They both are unique for each subscriber and together form a functioning key pair.

Section 5 provides that when any information or other matter needs to be authenticated by the signature of a person, the same can be authenticated by means of the digital signature affixed in a manner prescribed by the Central Government. Under Section 10, the Central Government has powers to make rules prescribing the type of digital signature, the manner in which it shall be affixed, the procedure to identify the person affixing the signature, the maintenance of integrity, security and confidentiality of electronic records or payments and rules regarding any other appropriate matters.

Furthermore, these digital signatures are to be authenticated by Certifying Authorities (CAs) appointed under the Act. These authorities would inter alia, have the license to issue Digital Signature Certificates (DSCs). The applicant must have a private key that can create a digital signature. This

private key and the public key listed on the DSC must form the functioning key pair.

Once the subscriber has accepted the DSC, he shall generate the key pair by applying the security procedure. Every subscriber is under an obligation to exercise reasonable care and caution to retain control of the private key corresponding to the public key listed in his DSC. The subscriber must take all precautions not to disclose the private key to any third party. If however, the private key is compromised, he must communicate the same to the Certifying Authority (CA) without any delay.

How Contracts are made possible in the electronic form?

Section 4 of the Act states that when under any particular law, if any information is to be provided in writing or typewritten or printed form, then notwithstanding that law, the same information can be provided in electronic form which can also be accessed for any future reference. This non-obstante provision will make it possible to enter into legally binding contracts on-line.

Explain the provision relating to Attribution, Acknowledgement and Dispatch of Electronic Records.

Chapter IV of the Act explicates the manner in which electronic records are to be attributed, acknowledged and dispatched. These provisions play a vital role while entering into agreements electronically.

Section 11 states that an electronic record shall be attributed to the originator as if it was sent by him or by a person authorised on his behalf or by an information system programmed to operated on behalf of the originator.

As per Section 12, the addressee may acknowledge the receipt of the electronic record either in a particular manner or form as desired by the originator and in the absence of such requirement, by communication of the acknowledgement to the addresses or by any conduct that would sufficiently constitute acknowledgement. Normally if the originator has stated that the electronic record will be binding only on receipt of the acknowledgement, then unless such acknowledgement is received, the record is not binding. However, if the acknowledgement is not received within the stipulated time period or in the absence of the time period, within a reasonable time, the originator may notify the addressee to send the acknowledgement, failing which the electronic record will be treated as never been sent.

Section 13 specifies that an electronic record is said to have been dispatched the moment it leaves the computer resource of the originator and said to be received the moment it enters the computer resource of the addressee.

What is the use of electronic records and digital signatures in e-governace?

According to the provisions of the Act, any forms or applications that have to be filed with the appropriated Government office or authorities can be filed or any licence, permit or sanction can be issued by the Government in an electronic form. Similarly, the receipt or payment of money can also take place electronically.

Moreover, any documents or records that need to be retained for a specific period may be retained in an electronic form provided the document or record is easily accessible in the same format as it was generated, sent or received or in another format that accurately represents the same information that was originally generated, sent or received. The details of the origin, destination, date and time of the dispatch or receipt of the record must also be available in the electronic record.

Furthermore, when any law, rule, regulation or byelaw has to be published in the Official Gazette of the Government, the same can be published in electronic form. If the same are published in printed and electronic form, the date of such publication will be the date on which it is first published.

However, the above mentioned provisions do not give a right to anybody to compel any Ministry or Department of the Government to use electronic means to accept, issue, create, retain and preserve any document or execute any monetary transaction. Nevertheless, if these electronic methods are utilised, the Government will definitely save a lot of money on paper!

Explain Issuance, Suspension and Revocation of Digital Signature Certificates (DSCs):

As per Section 35, any interested person shall make an application to the CA for a DSC. The application shall be accompanied by filing fees not exceeding Rs. 25,000 and a certification practice statement or in the absence of such statement, any other statement containing such particulars as may be prescribed by the regulations. After scrutinising the application, the CA may either grant the DSC or reject the application furnishing reasons in writing for the same.

While issuing the DSC, the CA must *inter alia*, ensure that the applicant holds a private key which is capable of creating a digital signature and corresponds to the public key to be listed on the DSC. Both of them together should form a functioning key pair.

The CA also has the power to suspend the DSC in public interest on the request of the subscriber listed in the DSC or any person authorised on behalf of the subscriber. However, the subscriber must be given an opportunity to be heard if the DSC is to be suspended for a period exceeding fifteen days. The CA shall communicate the suspension to the subscriber.

There are two cases in which the DSC can be revoked. Firstly, as per Section 38 (1), it may be revoked either on the request or death of the subscriber or when the subscriber is a firm or company, on the dissolution of the firm or winding up of the company. Secondly, according to Section 38(2), the CA may *suo moto* revoke it if some material fact in the DSC is false or has been concealed by the subscriber or the requirements for issue of the DSC are not fulfilled or the subscriber has been declared insolvent or dead et al.

A notice of suspension or revocation of the DSC must be published by the CA in a repository specified in the DSC.

What penalties for Computer Crimes are prescribed under IT Act 2000?

As per the Act, civil liability and stringent criminal penalties may be imposed on any person who causes damage to a computer or computer system. The offender would be liable to pay compensation not exceeding Rs. 1 Crore (10 million) for gaining unauthorised access to a computer or computer system, damaging it, introducing a virus in the system, denying access to an authorised person or assisting any person in any of the above activities.

Furthermore, the Act also defines specific penalties for violation of its provisions or of any rules or regulations made thereunder. However, if any person contravenes any rules or regulations framed under the Act for which no specific penalty is prescribed, he will be liable to pay compensation not exceeding Rs. 25,000.

Moreover, any person who intentionally or knowingly tampers with computer source documents would be penalised with imprisonment upto three years or a fine of upto Rs. 2 lakhs or both. In simpler terminology, hacking is made punishable.

The Act also disallows the publishing and dissemination of obscene information and material. The introduction of this provision should curtail pornography over the net. Any person who disobeys this provision will be punishable with imprisonment of two years and a fine of Rs. 25,000 for the first conviction. In the event of a subsequent conviction, the imprisonment is five years and the fine doubles to Rs. 50,000.

The Controller has the power to issue directions for complying with the provisions of the Act. Failure to comply with his directions is punishable. Moreover, the interference with 'protected systems' or the reluctance to assist a Government Agency to intercept information in order to protect state sovereignty and security is also made punishable.

The adjudicating court also has the powers to confiscate any computer, computer system, floppies, compact disks, tape drives or any accessories in relation to which any provisions of the Act are being violated. No penalty or confiscation made under this Act will affect the imposition of any other punishment under any other law in force.

If penalties that are imposed under the Act are not paid, they will be recovered as arrears of land revenue and the licence or DSC shall be suspended till the penalty is paid.

Short Notes on:

Adjudicating Officers:

The Central Government shall appoint an officer not below the rank of Director to the Government of India or equivalent officer of the State Government as an adjudicating officer to adjudicate upon any inquiry in connection with the contravention of the Act. Such officer must have the legal and judicial experience as may be prescribed by the Central Government in that behalf.

The Adjudicating Officer must give the accused person an opportunity to be heard and after being satisfied that he has violated the law, penalise him according to the provisions of the Act. While adjudicating, he shall have certain powers of a Civil Court.

Cyber Regulations Appellate Tribunal (CRAT):

A Cyber Regulations Appellate Tribunal (CRAT) is to be set up for appeals from the order of any adjudicating officer. Every appeal must be filed within

a period of forty-five days from the date on which the person aggrieved receives a copy of the order made by the adjudicating officer. The appeal must be the appropriate form and accompanied by the prescribed fee. An appeal may be allowed after the expiry of forty-five days if 'sufficient cause' is shown.

The appeal filed before the Cyber Appellate Tribunal 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. The CRAT shall also have certain powers of a civil court.

As per Section 61, no court shall have the jurisdiction to entertain any matter that can be decided by the adjudicating officer or the CRAT. However, a provision has been made to appeal from the decision of the CRAT to the High Court within sixty days of the date of communication of the order or decision of the CRAT. The stipulated period may be extended if sufficient cause is shown. The appeal may be made on either any question of law or question of fact arising from the order.

Powers of Police Officer in IT Act 2000:

A police officer not below the rank of deputy superintendent of police has the power to enter any public place and arrest any person without a warrant if he believes that a cyber crime has been or is about to be committed. This provision may not turn to be very effective for the simple reason that most of the cyber crimes are committed from private places such as one's own home or office. Cyber-cafés and public places are rarely used for cyber crimes. However, if the Act did give the police department powers to enter people's houses without search warrants, it would amount to an invasion of the right to privacy and create pandemonium. Keeping this in mind, the Legislature has tried to balance this provision so as to serve the ends of justice and at the same time, avoid any chaos.

On being arrested, the accused person must, without any unnecessary delay, be taken or sent to the magistrate having jurisdiction or to the officer-in-charge of a police station. The provisions of the Code of Criminal Procedure, 1973 shall apply in relation to any entry, search or arrest made by the police officer.

Inapplicability of IT Act 2000:

The provisions of the Act do not apply to the following:

a. a negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881;
b. power of attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;
c. a trust as defined in Section 3 of the Indian Trusts Act, 1882;
d. a will as defined in Section (h) of Section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called;
e. any contract for the sale or conveyance of immovable property or any interest in such property.

It is envisaged that the efficacy of the Act may not be considerable owing to its restrictive applicability.

Certifying Authorities (CA):

A CA is a person who has been granted a license to issue digital signature certificates. These CAs are to be supervised by the Controller of CAs appointed by the Central Government. Deputy or Assistant Controllers may also assist the Controller. The Controller will normally regulate and monitor the activities of the CAs and lay down the procedure of their conduct.

The Controller has the power to grant and renew licenses to applicants to issue DSCs and at the same time has the power to even suspend such a license if the terms of the license or the provisions of the Act are breached. The CAs have to follow certain prescribed rules and procedures and must comply with the provisions of the Act.

Definitions

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

"Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

"Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

"Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorise d access, use, disclosure, disruption, modification or destruction.

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

"Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;

"Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

"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";

"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;

"Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

"Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

"Private Key" means the key of a key pair used to create a digital signature;

"Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

"Secure System" means computer hardware, software, and procedure that -

(a) Are reasonably secure from unauthorised access and misuse;
(b) Provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions;
(d) adhere to generally accepted security procedures;

"Subscriber" means a person in whose name the Electronic Signature Certificate is issued;

FOR INTERNAL CIRCULATION ONLY