

Overview of e-business regulation in India

Prathiba M. Singh LL.M. (Cantab)

Singh & Singh Advocates, tel: 011-4314741, e-mail: mansingh@ndf.vsnl.net.in

India has witnessed a stupendous growth in the revenues of IT companies and software-related activities, which have provided the necessary impetus to the Indian government to enact the Information Technology Act 2000 (ITA). The ITA grants statutory recognition to e-commerce transactions, thereby bringing about revolutionary changes in statutes that have been unamended for more than 120 years.

IN 1

The Information Technology Act 2000 (ITA)

The ITA recognises digital signatures for agreements/transactions that have been entered into through electronic means. It provides legal recognition for electronic records, allows for electronic filing with governmental agencies and also provides for the creation of an electronic gazette that will facilitate notification of government rules, regulations, bye-laws, circulars and orders.

IN 1.1

Recognition of digital signatures

Section 5 of the ITA gives legal recognition to digital signatures and provides for a system by which digital signatures can be created and recognised.

In fact, s.5 provides that whenever a signature of a person is required for authentication of any document under any law, this purpose will be fulfilled with a digital signature. Any document bearing the digital signature, subject to verification, shall be presumed to be of the originator.

IN 1.2

Authentication

For authenticating digital signatures, India has adopted the use of the 'asymmetric crypto system' and 'hash function', which envelop and transform the initial electronic record into another electronic record.

There will be two keys to enable authentication of any digital signatures. The first is the private key and the second is the public key, defined in s.2 of the Act as:

- "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"

This system of having two keys for the authentication of electronic records is commonly known as Public Key Infrastructure.

IN 1.3

Certifying Authorities

In order to issue these public and private keys (which are nothing but a pair of numbers) and to maintain a directory of the public keys, the ITA provides for certifying authorities, whose role shall be:

- to identify and verify the credibility, worthiness, designation and employment of a person who applies to obtain the digital signature certificate
- to confirm the existence of a person applying for the certificate and maintenance proof of signatures
- to take all steps, as may be required, to ensure that the private key is kept confidential

IN 1.4

Controller of Certifying Authorities

The ITA contemplates the establishment of a Controller of Certifying Authorities (s.17) whose functions shall be:

- exercising supervision over the activities of certifying authorities
- certifying public keys of the certifying authorities
- laying down the standards to be maintained by certifying authorities
- specifying the qualifications and experience which employees of the certifying authority should possess
- specifying the conditions subject to which the certifying authorities shall conduct their business
- specifying the content of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key
- specifying the form and content of a Digital Signature Certificate and the key
- specifying the form and manner in which accounts shall be maintained by the certifying authorities
- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them
- facilitating the establishment of any electronic system by a certifying authority either solely or jointly with other certifying authorities and regulation of such systems

- specifying the manner in which certifying authorities shall conduct their dealings with the subscribers
- resolving any conflict of interests between the certifying authorities and the subscribers
- laying down the duties of the certifying authorities
- maintaining a database containing the disclosure record of every certifying authority containing such particulars as may be specified by regulations, which shall be accessible to public

The central government has also provided for recognition of certifying authorities from other countries: only those certifying authorities who are approved by the central government, and notified in the Official Gazette, can act as certifying authorities in India.

The ITA itself does not stipulate the conditions that a foreign certifying authority needs to fulfil in order to obtain recognition. (However, it is possible that these conditions may be stipulated in the rules that are being framed under this Act.)

IN 1.5

Certifying licences

The pre-qualifications for becoming a certifying authority are contained in s.21 of the Act. This prescribes that a person applying to become a certifying authority has to fulfil all the criteria relating to qualification, expertise, manpower, financial resources and other infrastructure facilities necessary to the issue of digital signature certificate, as may be prescribed by the government.

It also has to fulfil all the criteria relating to maintenance of internal security, established/proved experience and proficiency in encryption and decryption technologies, and secrecy of digital signatures and adequate reliability (s.18).

No time period has been fixed for the validity of the licence of a certifying authority. Such a licence is not transferable under the Act (s.21(3)(b)). The ITA, however, provides for the suspension and revocation of a licence by the Controller of Certifying Authorities: if there are any false or incorrect particulars in the application made by any person; if the requisite standards/terms and conditions have not been complied with; if the person has contravened any provisions of the Act, rules, circulars or any other regulations made under the ITA.

The ITA, however, ensures that there are reasonable safeguards in favour of the certifying authority and provides that any suspension cannot subsist for more than 10 days unless the Authority has been given a reasonable opportunity to show cause against the suspension. However, during such suspension, the certifying authority cannot issue any digital signature certificate.

IN 1.6

Digital signatures (ss.35-38)

The various particulars which are to be contained in the digital signature certificate are:

- identity of the applicant including the name, address and other data for identification
- the name of the certifying authority and identification number on the certificate
- qualification of the person
- financial limits of the person
- digital signatures

Where a digital signature certificate is granted, the person holding the certificate shall be presumed to have the private key of the public key mentioned in the certificate. The Certifying authority is the guarantor to the facts:

- that the digital signature certificate has been granted in accordance with the provisions, rules and regulations of the ITA
- that the public key and the private key constitute a functioning pair that can be used by any person wishing to transact with the holder of the certificate
- that the information is accurate and reliable

The use of the certificate can be suspended on the request of a holder/subscriber of a certificate or anyone authorised to act on behalf of the said holder/subscriber. It can also be suspended if it is in the public interest. The certificate is also liable to be revoked on three counts (s.38):

- if the subscriber ceases to exist on reasons of death, insolvency, winding up
- if there was any fraud committed
- if the private key was not kept in a confidential/secured manner

IN 1.7

Subscribers' responsibilities (ss.40-42)

The acceptance by a subscriber of a digital signature certificate means that the subscriber holds the private key to the public key listed in the certificate, and that the information contained in the certificate is accurate. The subscriber therefore must ensure that the private key is controlled with adequate care and is kept confidential.

The subscriber has a duty to inform the certifying authority if he, for some reason, feels that the private key is no longer confidential. Until and unless such notification is made to the certifying authority by the subscriber, the risk and responsibility of all persons who may be using the public key lies on the subscriber.

IN 1.8

Provisions relating to computer crimes (s.43)

The ITA has made specific provisions relating to crimes committed on computers. These have been categorised in s.43. These categories include:

- accessing or securing access to a computer, computer system or computer network without the permission of the owner or person in charge of the said system or network
- downloading, copying or extracting any data, database or information from such a computer, system or network
- introducing or causing to introduce any computer contaminant or computer virus into any computer, system or network
- damaging or causing to be damaged any such computer, system or network including the data, database or any other programme residing any such computer, system or network
- disrupting or causing any disruption on any computer, system or network
- denial of access to the person who is authorised to access such computer, system or network
- assisting any person in obtaining access to a computer, system or network in contravention of the provisions of the ITA or the rules and regulations thereunder
- Tampering with any computer system or network resulting in charging the services availed of by one person into the account of another.

IN 1.9

Tampering and hacking (ss.65 and 66)

The ITA also has made tampering with computer source documents and hacking offences (ss.65 and 66)

‘Tampering’ has been defined as intentional concealment, destruction or alteration, or causing any of these in any computer source code used for a computer, computer programme, computer system or computer network when the source code is required to be kept or maintained by law.

‘Hacking’ has been defined as destruction, deletion or alteration of any information residing in a computer resource, or diminishing its value or utility, or affecting it injuriously by any means.

Tampering and hacking are punishable by up to five years’ imprisonment, or a fine, or both.

The ITA also makes the publication or transmission in electronic form of any material that is lascivious, or appeals to the prurient interest, or any other obscene material, an

offence punishable with imprisonment of up to five years on the first occasion and up to 10 years on the second occasion.

IN 1.10

Adjudication

An adjudicating officer determines whether a person has contravened the above provisions. The officer is appointed by the central government or the state government and is not to be below the rank of director to the government of India or the state government.

The adjudicating officer is given the powers of a civil court. He or she has to be a person experienced in the field of information technology and have legal/judicial experience.

An appeal from the decision of the adjudicating officer is referred to that of Cyber Appellate Tribunal, which shall be presided by a person equivalent to the status of a judge of High Court or a member of the Indian Legal Service for at least three years or has been a member of the Indian Legal Service in Grade I for at least three years. An appeal from the Cyber Appellate Tribunal lies in the High Court.

IN 1.11

Liability of network service providers

One important provision which has been included in this Act is in relation to the liability of a network service provider. India has now statutorily provided that no person providing any service as a network service provider shall be liable under the ITA rules and regulations for any third-party information or data made available by it, provided it can be proved that:

- the offence was committed without his or her knowledge or
- that he or she had exercised all due diligence to prevent the commission of the said offence (s.79)

This provision is likely to be put to test in a number of cases and may be the subject of enormous debate. The difficulties in establishing the lack of knowledge and exercise of due diligence could pose a threat to service providers. It is therefore important that service providers build in sufficient safeguards in order to guard themselves against any liability arising out of offences or violations committed by the users of their services.

IN 2

Consequential amendments to other statutes

The ITA has brought about several changes in the Indian Penal Code, the Indian Evidence Act, the Bankers Book Evidence Act, and the Reserve Bank of India Act. The amendments, by and large, relate to the creation of electronic documents and their legal recognition.

IN 2.1

Penal code

The definition of electronic records contained in s.2(1)(t) in the ITA has also been added as a definition under the Indian Penal Code. All the provisions of the Indian Penal Code, relating to "documents" have been substituted with the term "document or electronic record".

For example, s.466 of the Indian Penal Code relates to forgery and contains the words "whosoever forges a document". From now on, this shall be substituted with "whosoever forges a document or an electronic record".

IN 2.2

India Evidence Act 1872

In the same manner the Indian Evidence Act 1872 has also been amended to include definitions of various terms including digital signature, electronic record, subscriber etc, as has been defined in the ITA.

Changes have been brought about in the definitions of what constitutes an "admission", maintenance of government records in electronic form, admissibility of electronic records as evidence in court proceedings, proof of digital signatures, presumption of validity of government notifications in gazettes issued in electronic form, presumption of validity of electronic agreements, namely, agreements concluded by affixing digital signatures, presumption as to digital signature certificates.

IN 2.3

Reserve Bank of India Act

Another statute which has been amended is the Bankers Book Evidence Act 1891 wherein bankers books included only ledgers, day books, cash books and accounts books. This definition has now been expanded to include all such books whether kept in written form or as print-outs of data stored in floppy disks, tapes or any other form of data storage devices. A print-out of such data maintained by the bankers duly certified by the bank will be accepted as certified copies of entries appearing therein.

In the Reserve Bank of India Act 1934, the Reserve Bank of India has been vested with the power of regulation of transfer of funds through electronic means either between

banks or financial institutions. Hitherto wire transfers were not statutorily recognised. With the passing of the ITA, electronic transfer has been given statutory recognition.

IN 3

Critique of the Information Technology Act 2000

The enactment of the ITA is a step in a positive direction for India, which has become a hub of activities in the field of Information Technology.

Even so, much remains to be done under this Act. An entire infrastructure relating to certifying authorities needs to be set up. Some of the provisions of the ITA are vesting enormous powers with the governmental authorities. (For example, under s.28, the Controller of Certifying Authorities has been given powers that are otherwise conferred on income tax authorities.) These powers are useful, if effectively used. However, if misused, major impediments and obstacles in a growing industry can be created. Such far-reaching powers with one or two individuals should be exercised in an extremely careful manner and it is, therefore, important that the appointments to these posts are made on the basic premise of honesty and integrity.