CYBER LAW FOR TRADE AND COMMERCE IN INDIA

Ashutosh Verma*

Abstract *Cyberspace is a time-dependent set of interconnected information systems with no physical boundaries making it extremely complex system to be regulated. Parliament of India enacted the Information Technology Act in the year 2000 with extensive amendments in subsequent years. This paper deals with the legal framework and executive regulatory mechanism under this Act which is relevant for the trade and business operations in India. It analyses the implications of commercial agreements in cyberspace and the requirements to be fulfilled for affixing digital signatures on business agreements and documents. The recent rules framed under the Act aim to tighten the data protection regime in India and ensure the secrecy of the data provided by the customers. It puts the responsibility on the business entities for implementing adequate safety measures against unauthorized access and transmission of personal data. There are provisions for payment of compensation in case of damage to the computer systems and networks. However, in areas like intellectual property rights, the law needs to be strengthened to protect such rights in cyberspace.*

Keyword: *Cyber Law, Digital Signatures, E-Documents, E-Governance, Data Protection*

In today's technologically advanced world, most commercial and non-commercial activities including personal communications are done in cyber space which includes computers, local area networks and various storage devices like hard disks, USB ports, internet, cell phones, ATM machines and the websites. Gibson (1984) originally coined the term cyberspace in a fictional setting in a novel, however there is no unanimity on the definition of cyberspace and Strate (1999) illustrated that there is a rich taxonomy for describing cyberspace. Ottis and Lorents (2012) define cyberspace as a time-dependent set of interconnected information systems and the human users that interact with these systems. Thus, the definition includes not only the dynamically changing technical system but also the various users like business, individuals, state and associations. The advancement in cyberspace gave a great stimulus to trade and commerce on a global level. It also led to significant increase in productivity, efficiency and accuracy in all spheres of business activities. The use of cyberspace changed the personal preferences, tastes, behavior, interactions and societal dynamics thereby bringing in a paradigm shift in the strategic approach of the business to the customers. All commercial operations done in cyberspace through electronic and internet medium are classified as e-commerce (Kalakota & Whinston, 2000). The types of e-commerce transactions include business to customers (B2C), business to business (B2B), government to business (G2B) and government to citizens (G2C) (Gandhi, 2006) However, commercial operations in cyberspace have certain peculiar features as compared to the physical space. It is characterized by a very crowded market where millions of people are engaged in various activities like shopping, banking, sending mails and sharing data. It totally overrides the boundaries of nations imposed by physical locations. Thus, a person sitting in India has access to all the websites on the world and can place a buy order on any of these sites. It is difficult to find out the identity of the person and offers full opportunity of maintaining anonymity. The option of instant downloading of electronic versions of books, audio and video cds enables one to totally bypass the laws which may be imposed in a physical market in the country and also for import of the items from abroad. The cyber space has significantly increased the risk of violation of intellectual property rights like the source code of highly priced software can be downloaded within minutes. It is highly mobile and data transfer from one country to another can be done in minutes unlike the transfer of goods and services. Computer or cyber crimes in business transactions have increased significantly and are considered as illegal, unethical or unauthorised behaviour of people relating to the automatic processing and transmission of data, use of computer systems and networks. As it is a global network with dynamic time-dependent changes having participants which include states, businesses, other organizations, individuals, groups of individuals and associations, it becomes extremely complex as a system to be regulated. As the cyber activities have largely evolved around the 90s, there is absence of any international treaty or agreement of regulating the cyber space. The framing of cyber laws is complicated process as it covers the use of technology which keeps on changing and therefore requires frequent review and revision of the enactments to ensure that they are able to cope with the new issues which may be arising on account of newer technology. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. Subsequently, the General

*Associate Professor, Indian Institute of Forest Management (IIFM), Bhopal

Assembly of United Nations recommended the same model to be adopted by all the member countries wherein the electronic records will have the same status as the paper documents. India being one of the supporters of the Model Law subsequently enacted the Information Technology Act (ITA) 2000 to regulate the entire aspects dealing with technology, computers, e-commerce, e-communication, e-banking, e-documents and internet. Being the first Act of its kind in India with broader effect, it had inherent flaws and was subject to heavy debate and criticism. Based on the inputs from various stakeholders, the Parliament passed the Information Technology (Amendment) Act (ITAA) 2008 which took care of the omissions, rectifications to the original Act and inserted new provisions on emerging issues. The ITA and subsequent ITAA Act is applicable to the whole of India and except as otherwise provided, it applies also to any offence or contravention committed outside India by any person. It has 94 sections of which the last four deal with the amendments to Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934. The Act defines a number of terms which include computer system, computer resource, computer network and data. Thus, it provides definitions which are broader so as to include all activities and aspects of cyber space. This paper develops a perspective on the major provisions, including rules and circulars which have relevance to trade and commerce in general (not confined to e-commerce) in India.

ELECTRONIC DOCUMENTS

The Act gives legal recognition to electronic documents for the first time in India and it is a major step towards moving to electronic document based record system. In fact one of the main objectives enumerated in the Act is "to grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication" (ICAI, 2012). Thus, now all e-documents will have the same validity as paper documents. However, the Act has specifically mentioned that the provision of e-documents is specifically not applicable to the negotiable instrument, power of attorney, trust, will, contract for sale or conveyance of immoveable property as defined under the relevant Acts. The Act originally also exempted cheques but subsequently deleted it due to insertion of two new categories of instruments, namely, cheque in electronic form and truncated cheque in the Negotiable Instrument Act. The Act has amended the Banker's Book Evidence Act to confer equal status on electronic records as compared to paper based documents (Nagpal, 2012). If by any law, a document is required to be in writing either typed or printed shall be deemed to be complied with if it is in electronic form and is accessible so as to be used for future reference. Similarly any document bearing the digital signature shall be deemed to have fulfilled the condition to be signed by the concerned person. The Act has provision for the maintenance of records or information as may be prescribed under the different laws. The records shall be deemed to have been properly maintained if they are retained and maintained in the electronic form in such a manner that they can be referenced subsequently and the details facilitate the determination of the date and place of origin of the document and its subsequent receipt and dispatch in the electronic format. The record needs to be maintained in the electronic format in such a manner that it will continue to represent the information which was originally generated, sent or received. The provision for audit of documents in electronic form will be as in the same manner as it is applicable to the printed documents. The electronic records shall be considered as secured from the point when the security procedure has been applied. The security procedure may be such as may be specified by the central government having regard to the nature of transactions, feasibility of implementation of procedures, level of technical capacity of the parties, sophistication of the technology used and the procedures adopted.

Electronic Contracts

In case of use of electronic means either for the formation of the contract, acceptance and communication of proposal and acceptance, the contract will have the same validity as it is in case of a written contract. Once the electronic contracts are recognised, it is necessary to have legal provisions regarding dispatching issues and acknowledgement of documents so as to avoid legal disputes relating to contracts. A person shall be considered as originator of an electronic document if it was sent by himself or with his authority by information which was operated by or on behalf of the originator. The Act deals with procedures of receipt and sending of electronic documents which are legally required to be in writing and signed by the concerned person. The document sent by electronic means may be acknowledged by the receiver by any communication or conduct so as to indicate the acknowledgement of the document unless the originator of the document has prescribed certain mode for acknowledgement of the e-document. In case the originator indicates that the acknowledgement is necessary to bind the agreement and no such acknowledgement is received, then it shall be treated as if the document has never been sent by the originator. Wherever the acknowledgement is not specified as a pre-condition for being bound by the contract then the originator may sent a communication to the receiver and specify the time limit within which the communication be sent, failing which it shall be treated that the document has never been sent by the originator. The ITAA also has provisions relating to the time and place of

dispatch and receipt of electronic records. Unless agreed otherwise between the parties, the dispatch of a document is complete when it enters a computer resource as to be out of the reach of the originator. The document is dispatched and received by the respective originator and receiver at their place of business, irrespective of the fact that the computer resource through which the document is sent and dispatched is at a different location. In case the originator has more than one place of business, then it shall be the principal place of business and if there is no principal place of business then the usual place of residence shall be treated as the place of business. As regards the time of receipt of documents, if there is a computer resource for receipt, then the time of receipt is the time when the document reached the prescribed computer centre. In other cases where resource is not specified, the time of retrieval by the receiver shall be the time of receipt of the electronic record.

ELECTRONIC FILING

One of the objectives of the Act is to facilitate the electronic filing of documents with government departments. This provision has a significant effect on the interaction between the commercial organisations and the government agencies and has improved the administrative machinery of the state. Departments like Income tax now require e-filing of returns for persons who have income above Rs.10 lakhs. The filing of the documents electronically has been the latest trend in the modern times and this is how the system has changed over a period of time (Ryder, 2007). Section 6 of the original Act sets the background for use of electronic documents in the governance of the state matters. The appropriate government may prescribe the electronic format for filling of any prescribed form, application or any document, issue or grant of any license, permit or the receipt or payment of money to any agency or office of the government. The form and the names of filling of such documents shall be prescribed by the government/agency/body and will be effective not withstanding any other manner or method prescribed under any other law for the time being in force. The government may in order to improve the delivery of services through electronic means may authorise any individual, private agency or any other entity to setup, maintain and upgrade the computerised services. Such service providers may also be authorised to charge or levy such service charges as may be specified by the government notwithstanding that the relevant law under which that service is provided does not have any express or implicit provision for levy of such fee or charges. The provision for publication of any act, rules, regulations, circulars shall be deemed to have been satisfied if it is published in the electronic format. However, it may be noted that while the electronic forms can be used in official matters related to submission of required information to the government, no person can insist that the documents must be accepted by the government in electronic form.

ELECTRONIC SIGNATURES

The Act aimed to give legal recognition to digital signatures for authentication of any information or matter which requires signature under any law. It deals with legal recognition to digital signatures in various spheres of business, statutory, governmental activities and the issues arising there from. Chapter 3 of the Act deals with authentication of electronic documents by affixing digital signatures. Any person in whose name the digital signature record is issued may authenticate an electronic record by affixing his digital signature as per the procedure prescribed. The authentication of any electronic record will require two steps, first is the development and transfer of the electronic record into a message digest by the use of asymmetric cryptosystem and hash function. The hash function means an algorithm mapping whereby whenever it is executed for the same electronic record it produces the same hash result which is translation of sequence of bits into smaller one, popularly known as 'hash result'. This will make it computationally infeasible to reconstruct the original record from the same hash result and also the two electronic records can produce the same hash result using the algorithm. This use of hash functions seals the record ensuring that if any alteration or tampering is done with the record, the digital signature will become invalid. The subscriber who authenticates the document has a private key which is attached to the record and can be verified by any person who has the public key of the subscriber. This public and private key constitute a functioning key pair and are unique to the subscriber. Electronic signature will be secured provided its creation was stored and affixed in such manner as may be prescribed. There is an exception which deals with techniques other than asymmetric cryptosystem and the hash function. Accordingly a subscriber may authenticate a document by any other technique which may be considered reliable by the government and which is specified in the second schedule to the Act. The technique will be considered reliable if the signature creation data or the authentication data are within the context in which they are used are linked to the signatory or the authenticator, or such data were under the control of the signatory or authenticator at the time of signing the document. It will be reliable if any alteration to the electronic signature or to the information made after affixing of such signature or authentication is detectable. The Central government may add, omit or delete the procedure to be adopted as well as the techniques to be used for electronic signature or authentication. The specific mention of the cryptosystem were criticised as being technology dependent and therefore the term electronic signature was included along with the digital signature by ITAA 2008 thereby bringing in technological neutrality.

There is entire administrative machinery set up by the government to regulate the issue and use of digital signatures. The Controller appointed by the central government and the associated administrative machinery can issue license to the persons authorising them to issue electronic signature certificates. These persons will be called as certifying authorities and have to ensure that the person applying for digital signatures must hold the private key which can create a digital signature and does correspond to the public key. The certifying authority can revoke or suspend the digital signature certificate on certain conditions and in certain situations. It is the responsibility of the subscriber to ensure that proper care is exercised to retain control of the private key corresponding to the public key listed in his/her signature. The license to issue certificates may be suspended by the Controller, if it found that such certificate had been obtained through false information or violated any conditions imposed while granting the license.

Damages to Computer System

Business organisation which are maintaining electronic records on computer systems and networks are also exposed to the risk of damages to such system resulting in business losses of different types. There were cases where an outgoing employee disturbed the records, took away the database of clients, manipulated the records without any knowledge of the superiors. The Act originally envisaged that it will facilitate and encourage electronic storage of data, however, on account of the damages to computer hardware, software, database, records and unauthorised access of data, there was a strong demand from the chambers of trade and commerce to insert appropriate provisions in the Act to check such mishaps. Therefore, the ITAA of 2008 inserted a provision for compensation in case of damages arising on account of following acts in relation to a computer, computer system or network, computer resource, external storage devices:

- Unauthorised access
- Unauthorised copying, downloading, extracting database or other information
- Introducing any computer contaminant or computer virus
- Damaging programmes
- Disruption of the functioning
- Denying access to any authorized person
- Facilitating access in contravention of the provisions of this Act
- Charging services availed by one person to another person's account
- Tampering or manipulating records
- Destroying, altering any information which diminishes its value or utility
- Stealing, concealing, destroying, and altering any computer source code.

Any person who engages in any of the above mentioned acts in relation to computer, computer system or network, computer resource, he/she shall be liable to pay damages by way of compensation to the person so affected by the acts. Thus, while this provision provided protection to the business, the incidence of unauthorised access of personal information and sharing of such information resulted in government framing the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (herein called, the rules) which impose obligations as regards the manner of collecting information and its protection.

Protection of Customers'/Clients' Personal Information

These rules have enumerated certain information to be sensitive personal information and include password, debit/credit card details, medical records, biometric details or other information obtained under a legal contract. However, sensitive personal information specifically excludes any information available in the public domain or information which has to be provided under the Right to Information Act. The body corporate or any other business entity has to frame a policy regarding private/personal information covering aspects like its collection practices and policies, type of information collected, purpose of collection and the same must be displayed on its website. The policy should also be brought to the notice of the person with whom the body corporate is going to enter into the contract and from whom the information is going to be collected. The body corporate or any person including its agent who is collecting information should obtain the consent of the person in writing from whom the information is to be collected. It should also indicate the usage or the purpose of collection of the information. While collecting the information adequate steps have to be taken by the body corporate to ensure that the person from whom the information is collected is having knowledge of the fact that information is being collected from him/her. The personal sensitive information once collected cannot be retained by the business entity once the purpose for which the information is collected has been achieved or the time period for which the information was to be held has expired. Any person whose information has been collected will have the right to review the information provided by him/her and it will be obligatory on the part of the body corporate to rectify and correct any incorrect or deficient information. But the body corporate will not be held responsible for the authenticity of the information provided by the concerned person. Further, the person from whom the information is collected will be given the

option not to provide the information. Subsequently also the provider of information may withdraw his consent by furnishing it in writing. However, on withdrawal of consent, the body corporate will have the option not to supply the goods and services with reference to which information was being provided.

Implementation of Reasonable Security Practices and Procedures

Information security remains one of the key priorities for the Indian IT Enabled Services–Business Process Outsourcing (ITES-BPO) industry, a challenge that has to be overcome in order to firmly establish the sector's credentials as a trusted sourcing destination (Lawande,2012) . The rules aim to improve the status of security practices and procedures covering the various managerial, operational, technical and physical aspects so that adequate protection is available to the information assets existing in the organisation. The body corporate must also have policy document or manual which provides in sufficient detail the security procedures and practices for information assets of the organisation. It will be obligatory on the part of the business entity to take the appropriate steps as enumerated in the security protocol manual in case of any breach of the procedures and practices causing threats to the information assets. The agency appointed under law may also call upon the body corporate to demonstrate that they have implemented the security procedures as per their manual. The rule has specified that the International Standard IS/ISO/IEC 27001 on "Information Technology-Security Techniques-Information Security Management System – Requirements" is one such standard which may be considered suitable to be adopted for security practices and procedures. However, it is not mandatory to implement this system and any industry association may develop a code of its best practices and get them approved by the government.

Grievance Settlement

The central government has constituted Cyber Appellate Tribunal and any person who is aggrieved by any order made by the Controller or an adjudicating officer may appeal to the Cyber Appellate Tribunal. Civil courts are barred from entertaining any suit or proceeding in respect of any matter which an adjudicating officer has the power to determine under this Act.

Offences

The various acts which are considered as offences under the Act and have relevance to business include:

- Tampering with the source code for a computer programme, network.
- Hacking, i.e. destroying the information stored in computer or on a website.
- Obtaining the electronic signature fraudulently.
- Sending offensive electronic messages.
- Receiving or retaining any stolen computer resource or device.
- Identity theft like using/logging into others bank accounts.
- Personating with the objective of cheating the other person.

Different punishments have been prescribed for all these acts and there are other offences related to cyber terrorism and publication of obscene material (Seth, 2010).

CONCLUSION

The Act has given legal recognition to electronic documents, signatures, contracts and electronic filing of documents to be submitted to the government and has thus facilitated the functioning of trade and business in a significant way. However, one area where the law needs to strengthen is the protection of the intellectual property rights in the cyber space. The law along with its various amendments is silent on this aspect affecting the trade and industry. It has to specifically deal with the issues in the software industry, the greatest threat of risk to software industry, engineering process and education is due to lack of future imagination and inability to understand strongest bond established between software engineering discipline and legal issues of the cyber space (Kumar, 2012). According to Jenkins (2010), though law cannot possibly be expected to keep pace with changes in technology, but the provisions have to be reviewed frequently to keep some pace with the changes in technology and ensuring that the impediments to free flow of trade and business are minimised if not completely removed.

REFERENCES

Gandhi, S. K. (2006). E-Commerce and Information Technology Act 2000. Vidyasagar University Journal of Commerce, 11(3), pp. 82 - 91.

Gibson, W. (1984). Neuromancer. New York: Ace Books.

Institute of Chartered Accountants of India. (2012). Information Technology (Amended) Act. Retrieved September 10, 2012 from http://xa.yimg.com/kq/groups/22830576/356371266/name/17796IT_ACT_2008.pdf

Jenkins, G. P. (2010). Information Technology and Innovation in Tax Administration. London: Kluwer Law

International.

Kalakota, R. & Whinston, A. B. (2000). Frontiers of Electronic Commerce. Delhi: Addison-Wesley.

Kumar, A. (2012). Issues of Cyber Laws and IPR in Software Industry and Software Process Model. International Journal of Computer Applications, 44(7), pp. 210 - 219.

Lawande, P. P. (2012). Initiative for Prevention of Cyber Crime in India. Indian Streams Research Journal, July, 2(6), pp. 20 - 28.

Nagpal, R. (2012). 7 Years of Indian Cyber Law. Retrieved September 10, 2012 from http://www.asclonline.com/index.php? title=Ebooks

Ottis, R. & Lorents, P. (2012). Cyberspace; Definitions and Implications. Retrieved September 6, 2012 from www.ccd-coe.org/articles/.../Ottis_Lorents_CyberspaceDefinition.pdf

Ryder, R. D. (2007). Guide to Cyberlaws: Information Technology Act, 2000. E-Commerce, Data Protection and Internet. Nagpur: Wadhwa Publications.

Seth, K. (2010). Cyber Laws in Information Technology Age. Nagpur: Lexis Nexis Butterworth and Wadhwa Publications.

Strate, L. (1999). The Varieties of Cyberspace: Problems in Definition and Delimitation. Western Journal of Communication, 63(4), pp. 382 - 412.