signature validation, cyber crimes and jurisdiction issues. But it has not explicitly dealt with ODR. Yet the provisions could be optimized for ODR in various sectors. In addition to such optimization of IT Act and changes in Arbitration and Conciliation Act 1996, other inputs like training, infrastructure and most importantly the willingness of the disputants to be part of the process are essential.

The lack of awareness of and expertise in management of ODR apart from inadequate infrastructure facilities are responsible for the slow emergence of ODR in India. There is hardly few ODR providers in this country. The Government and other LAW Institutions like Law Commission, Academic institutions should address these aspects and recommend ways to popularize the ODR in India.

Conclusion

India is one of the top players in Information Technology in the world. It also has become a hub for International commercial arbitration. The e-commerce has also grown tremendously. By creating awareness of ODR, establishing training programmes, improving the infrastructural facilities and modifying the laws suitably, India can become the hub of ODR in the world. Panel of experts may be constituted to study the various issues connected with ODR application in off line dispute resolution. We would even recommend for the research scholars to take up research work on this subject in both legal and sociological fields for pursuing PhD.

REFERENCES

1. *Esher van den Heuvel*, 'online Dispute Resolution as a solution to cross border E-disputes, an introduction to ODR', WWW.esher@schasfoort.com, June 01, 2012.

2. *Katsh Ether* and *Janet Refkin*, 'Online Dispute Resolution-Resolving Conflicts in Cyberspace', San Francisco, USA, Jessey-Bass, 2001.

3. *Rajan R.D*, 'A Primer on Alternative Dispute Resolution for Business', (New Edition) Thirunelveli, Tamil Nadu, India, Bharathi Law Publishers, 2005

4. *Rule Colin*, 'Online Dispute Resolution for Business' San Francisco, USA, John Wiley and Sons, 2002

5. *Sharma Vakul*, 'Information Technology - Law and Practice' (Third Edition), New Delhi, India, Universal Law Publishers, 2011.

RECOGNITION AND ENFORCEMENT OF ELECTRONIC CONTRACTS IN INDIA

By

—S.B. MD. IRFAN ALI ABBAS, Advocate
L.L.M., (Corp. Laws), PGDCL, PGDPL, PGDADR, GNIIT
Malakpet, Hyderabad, A.P.
e-mail: sbmiadv@gmail.com

Introduction :

The cyber world has no physical boundaries; no singe authority governs it. Internet is the medium for freely sharing information and opinions; it provides everyone with round the clock access to information, credit and financial services, and

shopping. Even network information systems are being adopted by Governments worldwide, that is why Governments across the world are recognizing the need to securing and regulating the cyber world.

A Cyber/Electronic contract is a contract modeled, executed and enacted by a software system or entered into by using computer as a mode of concluding the contract. Cyber/Electronic Contracts facilitate transactions and agreements electronically without the parties meeting each other personally, even between persons in different countries. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirement as to (a) writing and (b) signature of legal recognition, in all the countries internationally and apart from these the establishment of jurisdiction in cyberspace is a critical issue, which steers the entire enforcement mechanism.

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce, which was followed by the Model Law on Electronic Signatures in 2001 and the Convention on the Use of Electronic Communications in International Contract in 2005 (collectively the "UN Initiatives"). The goal of the UN Initiatives has been to provide national legislatures with a set of internationally recognized rules to remove legal obstacles and create a more certain legal environment for electronic commerce. The UN Initiatives adopt a "functional equivalence" approach by setting out principles so that electronic communications are given technological neutrality. For example, when there is a legal requirement to present information in writing, this will be satisfied by an electronic document if the information contained in the document is "accessible so as to be usable for subsequent reference"[1]. The UN Initiatives also provide electronic standards to meet signature requirements, originality requirements, time and place of communications, and the use of automated systems for formation of contract[2].

Position in India:

In accordance to the said UNCITRAL Model Law on Electronic Commerce, the Information Technology Act, 2000[3] has been enacted on the guidelines of the Model Law and is the primary law in India which governs cyberspace and the Information Technology Amendment Act, 2008[4] has also been passed amending the I.T. Act. The Information Technology (Other Standards) Rules, 2003, The Information Technology (use of electronic records and digital signatures), 2004, The Information Technology (Security Procedure) Rules, 2004, The Information Technology (Certifying Authorities) Rules, 2000, The Information Technology (Certifying Authority) Regulations, 2001, The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000, The Cyber Regulations Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Presiding Officer) Rules, 2003 and other related guidelines are the rules which govern the cyber related transactions. Suitable amendments have also been made in the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 for related matters to give recognition and enforcement to the Cyber transactions.

All the contracts in India, including the Cyber Contract are governed and regulated by the Indian Contract Act. The cardinal

1. Article 6 of the UNICTRAL Model Law on Electronic Commerce (1996).

2. Chapter 8 of UNCTAD Information Economy Report 2006 : The development perspective "Laws and Contracts in an E-Commerce Environment" (2006).

3. Came into force on 17.10.2000, *vide* G.S.R. 788(E), dated 17.10.2000.

4. Came into force of 9.2.2009.

rules of the contract of the Indian Contract Act apply to the Cyber Contract, only the technical issues and the mode of the formation, execution, completion of the contract and its validity are governed by the Information Technology Act, 2000 and the legal rules regarding admissibility in evidence have been incorporated in the Indian Evidence Act. The I.T. Act lays down guidelines to validate electronic records and rules as to communication through e-mail, security of messages and their authenticity.

Information Technology Act, 2000

The relevant provisions of the Information Technology Act, which confer validity to and empower the enforcement of electronic contracts in India, are:

- Section 4 gives legal recognition to Electronic Records *i.e.* files, folders, e-mails, sms *etc.*, in the eyes of law, if the conditions of making it available in electronic form and accessible, usable for subsequent reference are satisfied, and has provided that such electronic records shall be treated same as in writing or typewritten. As such, it forms edifice for the validity of the Cyber Contracts and their enforcement.

- Section 3 has recognized the digital signatures and specified the nature and character of a valid digital signature. By the I.T. Amendment Act, 2008 Section 3A has been inserted and it recognizes Electronic Signature also. The Section 5 has treated digital signature and also electronic signature as an equivalent to a handwritten signature. The authenticity of any information or any matter can be ascertained with the help of the electronic or digital signature affixed on the said electronic record.

- The I.T. Amendment Act, has made a major contribution to the Cyber Contracts by inserting the Section 10A which gives validity and recognition to the contracts which have been concluded by communications made in electronic form or by means of electronic record.

- The communication of offer and acceptance form an integral part of a contract, and attribution of the Electronic record to the person who sent the record is very necessary to validate offer and acceptance, which is provided under Section 11 of the I.T. Act. The person who sends the electronic record is called as "Originator" and the record is said to be sent by the originator if he sent it by himself, or it was sent by his agent or it was set automatically by the information system of originator. Further the Section 12 deals with acknowledgement of the receipt of electronic record.

- The Section 13 deals with the time and place of dispatch and receipt of electronic record, which plays a very crucial role in the Cyber Contracts, in the aspects of territory, jurisdiction, applicable laws, evidentiary issues, period of limitation on litigations and other issues. It can be observed that, the Sections 12 and 13 of the I.T. Act lay down the regulations on the transaction aspects of the offer and acceptance.

- As, the transactions through the internet and electronic media are on rise in the present world, the security, integrity of electronic records is an issue of vital importance. As per Section 14 the security procedure shall be followed by the parties handling with the electronic record to make the record a secure electronic record and to secure their transaction from the impending offenders.

- The I.T. Amendment Act, 2008 has substituted the old Sections 15 & 16 with new sections, including the Electronic Signature in the place of Digital Signature and Security Procedure for the same. It is provided that, the Central Government may prescribe the security procedures and practices having regard to the commercial circumstances, nature of transactions and such other appropriate related factors.

- Apart from these issues, the Act enables for a certifying authority and officers and functions in Section-17 and they are from Sections 18 to 34 on the various aspects of security and privacy issues.

- Contracts drawn in cyber world need to take care of mutual interest of the establishments and the clients. This needs an adequate framework and the I.T. Act Sections 35-39 dwells on the digital signature and its various aspects. However the act also specifies the duties of subscribers in Sections 40 to 42, which are of importance in cyber contract.

- The Sections 43 to 47 of the I.T. Act deal with the Penalties, Compensation and Adjudication, and the Cyber Appellate Tribunal is vested with the power of adjudication in respect of the same. The Cyber Appellate Tribunal, its composition, jurisdiction is discussed under Sections 48 to 64 of the Act, and the Central Government by notification is empowered to determine its jurisdiction. It is the Tribunal which adjudicates and provides relief in respect of the matters dealing with the I.T. Act.

Indian Evidence Act

It is pertinent to contextualize at this juncture that evidence recorded or stored by availing the electronic gadgets is to be given the evidentiary status for effective enforcement. The emergence of Information Communication Technology (ICT) witnessed sea change by elevating the status of the evidence recorded, generated or stored electronically from the secondary to primary evidential status. As such, the following sections have been inserted in the Indian Evidence Act to provide evidentiary value to the matters recognized in the I.T. Act:

- As regards presumption to electronic agreements, the Section 85A has been incorporated, which says that every electronic record of the nature of an agreement is concluded as soon as a digital signature is affixed to the record. The presumption is only valid to electronic records, electronic records that are five years old and electronic messages that fall within the ambit of Sections 85B, 88A and 90A of Indian Evidence Act.

- Section-85B provides that, Court shall presume the fact that record in question has not been put to any kind of alteration, in case contrary has not been proved. The secure status of the record may be demanded till a specific time. The digital signature should also be presumed to have been affixed with an intention of signing and approving electronic record. Further it has been provided that it should not be misread as to create any presumption relating to the integrity or authenticity of the electronic record or digital signature in question.

- Section-88A states that, the Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission, but the

Court shall not make any presumption as to the person by whom such message was sent. The words "may presume" authorize the Court to use its discretionary power as regards presumption. Sections 85A and 85B contained the words "shall presume" which expressly excluded this discretionary power of the Court.

- As per Section 90A, in case of an electronic record being five years old, if proved to be in proper custody, the Court may presume that the digital signature was affixed so as to authenticate the validity of that agreement. An exception can be effected in case circumstances of a particular case render its origin probable.

- As far as a digital signature certificate is concerned, as per Section 85C the Court shall presume that information listed in the certificate is true and correct. The words "shall presume" relate to expressed exclusion of the discretionary power of Court.

- Section 65B talks about admissibility of electronic records. It says that any information contained in an electronic record which is printed on a paper or stored/recorded/copied on optical/ magnetic media produced by a computer shall be deemed to be a document and is admissible as evidence in any proceeding without further proof of the original.

- However, to protect consumers from potential abuses, electronic versions of the following documents are invalid and unenforceable by the Information Technology Act: 1) wills, codicils, and testamentary trusts; 2) documents relating to adoption, divorce *etc.*; 3) Court orders, notices, and other Court documents such as pleadings or motions; 4) notices of default, repossession, foreclosure, or eviction, *etc.*

Conclusion:

The major issues in the Cyber Contract are the technical issues relating the authenticity of the electronic record, the receipt and acknowledgement of the record, the time and place of the concluding of the contract. Based on these issues only, the jurisdiction, applicable laws are decided. The Information Technology Act, 2000 has been incorporated to resolve these technical issues, and the Information Technology Amendment Act, 2008 has brought vital changes to the act and increased its application and scope. But in practical scenario, in comparison to the laws of United States and European Nations, there is still a lacuna and more development and improvement shall be made in the administrative mechanism for the implementation of the laws. There is urgent necessity to educate the Judges, police and enforcement mechanism about the vital importance of the cyber transactions and increase the efficiency of the same. However, it is also past time to develop common standards for E-Commerce throughout the globe. Not only should jurisdictional outcomes be as predictable as possible, but also they should be as uniform as possible.

———————