International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 6, June 2017

ISSN: 2394-4404

The Legal Issues Of Electronic Commerce And The Legal Mechanism Under Virtual World: An Indian Perspective

Dr. Azmat Ali

Department of Law, Jamia Millia Islamia, New Delhi

***Abstract:** The growth of E-Commerce is required the vibrant and effective regulatory mechanism to further strengthen the legal infrastructure to the success of E-Commerce in India. However, all these regulatory mechanisms as well as legal infrastructure come within domain of cyber law. Nowadays awareness about cyber law has begun to grow. Initially, several technical experts considered that legal regulation of the internet was not necessary, but fast growth of technologies and the internet compelled to think that no activity on the internet could have remained free from the influence of the cyber law because feature of the internet, which caused much controversy in the legal community.*

***Keywords:** Electronic Commerce, Legal Mechanism, Digital signature, Asymmetric Cryptostem, Electronic Evidence.*

I. INTRODUCTION

With the advent of internet and its commercialization since 1994, E-Commerce rapidly emerged in the new world economy. E-commerce may be defined as the use of the internet and other networking technologies for conducting business transactions. Nowadays most people think, E-Commerce means online shopping. However, web shopping is only a small part of the picture. In addition, E-Commerce includes business-to-business connections that make purchasing easier for big corporations. Furthermore, E-Commerce will significantly have impact the global economy as well as play a vital part in future economic development. Several developing countries have started to pursue policies to provide a consistent legal and regulatory framework to support electronic transactions across state, national and international borders.

Thus, E-Commerce includes several issues relating to organizational management, commercial negotiations and contract, legal and regulatory frameworks, financial settlement arrangements and taxation, among many others. Internet facilitates online execution of commercial transaction. It may be either business to business or business to consumer or inter-organizational. The growth and development in the field of E-Commerce has equally needed an effective regulatory mechanism. Cyber law is still a constantly evolving process. With the growth of internet, some issues are also growing relating to jurisdiction, cyber crime, admissibility of e-transaction. Electronic Commerce (EC)/Electronic Data Interchange (EDI) is revolutionizing the way people look at commercial as well as administrative exchanges of information because it does not require paper. In the world of paper documents, the established norms of contract and commercial law have been sufficient to resolve legal disputes concerning these documents. However, an EDI imposes new risks and behavior related to legality electronic data interchange transaction, digital signature, and the risk of erroneous transmission, lost record, sabotage and fraud.

These are few complex issues of security, privacy, authentication and anonymity, which have been thrust into the forefront as confidential information increasingly traverses modern networks. For the functioning of E-Commerce, confidence, reliability and protection of information against security threats are very crucial prerequisite. A security threat may be defined as a crucial condition or event with the potential to cause economic hardship or loss to data or network resources by disclosure, modification of data, denial of service, fraud, waste and abuse. In sum, the fast developing technology innovation in the world of the Wired and Wireless internet require for increasing governance capacity among social, educational and political organization to create an equitable and safe knowledge Society.

II. MEANING AND CONCEPT OF E-COMMERCE

The Commerce is a communicative transaction between two parties playing a very familiar role that is buyer and seller. For commerce to occur, somebody must do the selling, somebody must do the buying, and these two bodies must share a basic understanding of how the transaction is generally supposed to flow. Electronic commerce, commonly known as E-Commerce, consists of the buying and selling of products or services over electronic systems such as the internet and other computer networks. E-Commerce describes the buying, selling, and exchanging of products, services, and information through computer networks, primarily the internet. E-Commerce is changing all business functional areas and their important tasks, ranging from advertising to paying bills. In simple terms, E-Commerce is a form of computerized buying and selling both by consumer and from by company, which facilitates choosing the goods, ordering, delivery, after sales support and payment.

E-Commerce is an umbrella concept to integrate a wide range of existing and new applications. The World Trade Organization (WTO) Ministerial Declaration on E-Commerce defines E-Commerce as the production, distribution, marketing, sales or delivery of goods and services by electronic means. The six main vehicle of E-Commerce that have been recognized by WTO are telephone, fax, TV, electronic payment and money transfer system, electronic data interchange (EDI) and the internet. According to European Commission, E-Commerce encompasses more than the purchase of goods online. It includes a disparate set of loosely define behaviour, such as shopping, browsing the internet for goods and services, gathering information about items to purchase and completing the transaction. It also involves the fulfillment and delivery of those goods and services and inquiries about the status of orders. Like any other sustained business activity is also means conducting consumer satisfaction surveys, capturing information about consumers and maintaining consumer databases for marketing promotions and other related activities.

Electronic transactions are conceptually very similar to traditional (paper-based) commercial transactions. Vendors present their products, prices and terms to prospective buyers. Buyers consider their options, negotiate prices and terms (where possible), place orders and make payment. Then, vendors deliver the purchased products. While the precise order of these events and the mechanisms through which they are transacted vary, these activities are in principle, fundamental to both traditional and electronic commerce.

III. THE LEGAL MECHANISM AS THE LIFEBLOOD OF E-COMMERCE IN INDIA

The E-Commerce refers buying and selling goods and services through electronic means especially on the internet but E-Commerce cannot be flourished without vibrant and effective legal mechanism. The vital role is played in the E-Commerce mechanism as following.

A. REGULATION OF DIGITAL SIGNATURE AND TRANSACTION UNDER INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) was passed to fulfill the following three objects:

- ✓ To respond and give the effect to the United Nations Call to all states to consider Model Law.
- ✓ To provide legal recognition for transactions carried out by means of electronic data interchange.
- ✓ To facilitate electronic filing of documents with the government agencies so as to promote efficient delivery of government services.

Apart from the above stated objectives, the principal propellant on which the whole structure of the Act is based that is trust reposed between business partners. The breach of trust must be subject to law. The users of information technology must have trust in the security of information and communication infrastructure. The IT Act, 2000 was passed to facilitate electronic commerce and hence, it provides legal recognition to electronic records, to digital signature etc. Main electronic transactions under the Act are:

a. ASYMMETRIC CRYPTOSTEM

The word Cryptology Stems from Greek root meaning ‘hidden word’ and is used to describe the ancient science of secret communications. It means a system capable of generating a secure key pair consisting of a private key and public key. This definition pertains to the dual key encryption techniques. Encryption is a technique to convert data into an unintelligible form that cannot be recovered into the original format without a secret decryption key. The object of applying cryptography to documents to transfer over the open networks, such as the internet, is to prevent vital information getting into the hands of unauthorized persons.

There are basically two types of encryptions

- ✓ Symmetric (secret/private)key
- ✓ Asymmetric (public) key

Private or Symmetric key creates digital signature and public key verifies the digital signature which is called dual key encryption techniques. This cryptographic technique involves the use of two cryptographic keys -a public key and a private key. The public key is freely distributed and made available to anyone who wishes to send a message to a given person.

The encryption used for these keys is of such a high degree of complexity that it is theoretically impossible to crack within a reasonable timeframe.

Transaction security is a significant barrier to the development of E-Commerce. Parties must be able to use techniques to ensure that the business conducted over the networks will be secure. The most reliable means is through cryptography (i.e. encryption and decryption techniques). Cryptography uses sophisticated mathematical algorithms, particularly a technology known as ‘Asymmetric Cryptography’. Cryptography can be differentiated between the following:

- ✓ Use of cryptography for confidentiality of a message; and

- ✓ Use of cryptography in digital signature.

The most popular and useful method of encryption for general messaging is public key cryptography that is encryption and decryption techniques involve the use of two kinds of keys, public keys and private keys, both of which are mathematically linked. One key is used for encryption and the other corresponding key is used for decryption. Each user has a pair of keys, of which the private key is kept secret and the public key is open to all.

b. ADOPTION OF DIGITAL SIGNATURE

The term digital signature is defined in section 2(p) of Information Technology Act, 2000 as "Digital Signature" means authentication of an electronic record by a subscriber by means of an electronic method or procedure in accordance with a provision of section 3 of Information Technology Act, 2000. This definition has been taken from the Singapore Electronic Transactions Act, 1998 and indicates the method commonly used in the West to verify electronic documents. "Digital Signature" means a Signature is affixed in electronic from consisting of a transformation of an electronic record using asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the transformation was made. The term hash function is defined by way of Explanation to section 3(2) of the Information Technology Act, 2000.

A digital signature involves two components-the public key and the private key. The sender signs a document using his private key that ensures the document's safety in transit as the text is encrypted and only the sender has access to his private key.

The reasons for placing a digital signature on an electronic document are exactly the same as the reasons for placing a handwritten signature on a paper document.

They are:

- ✓ *IDENTIFICATION:* By placing a signature on a document, the signer identifies himself by the unique style of writing his name. Similarly, a digital signature uniquely identifies the sender of an electronic message.
- ✓ *AUTHENTICATION:* By performing the act of signing, the signer acknowledges that he authorizes and adopts the contents of the document. Similar, intent can be attributed to the sender of the digitally signed e-mail message.
- ✓ *SECURITY:* A signature on a document should be difficult to forge. Moreover, some aspect of the signature, such as the individuality of the style of the person signing, offers security to the other party that as to the identity of the signer. Digital signatures offer the same form of security.
- ✓ *TAMPER RESISTANCE:* The nature of a written signature is such that changes to the signed text or the signature itself are clearly apparent except in the case of the cleverest forgeries. A digital signature, if anything, is even more tampering proof as they are almost incapable of being forged without actually altering the message irretrievably.

c. DIGITAL SIGNATURE AND PUBLIC KEY INFRASTRUCTURE PROCESS

The basic problem related to digital signature regime is that it operates in online and software driven space without human intervention. Sender sends a digitally signed message then recipient receives and verifies it. The only requirement is that both sender and the recipient to have digital signature software at their respective ends. A digital signature certificate security binds the identity of the subscriber. It contains name of the subscriber, his public key information, name of the certifying authority who issued the digital signature certificate, its public key information and the certificate's validity period. These certificates are stored in an online repository that is publicly accessible repository maintained by the Controller of Certifying Authorities or in the repository maintained by the Certifying Authority. Every Certifying Authority (CA) has to maintain operation as per its certification practice statement (CPS). The Certification Practice Statement (hereinafter referred to as CPS) specifics the practices that each Certifying Authority employs in issuing digital signature certificates.

The mass implementation of digital signature certificates in the internet environment is done via Public Key Infrastructure. It establishes a framework or system to use digital signature certificates, encryption and digital signatures as an authentication mechanism and devises management methods for such usage. The basic idea behind Public Key Infrastructure (hereinafter referred to as PKI) is to integrate the use of digital certificates, CAs and other security mechanisms to provide an infrastructure that can be used to validate each party involved in E-Commerce, thereby making E-Commerce more secure.

d. DIGITAL SIGNATURE OR ELECTRONIC SIGNATURE CERTIFICATE

In simple terms, a digital certificate is a reliable electronic method of signing electronic documents that provides the recipient with a way to verify the sender and also determine whether the content of the document has been tampered with digital certificates use a method of cryptography called asymmetric encryption. Unlike symmetric encryption, which uses the same secret password to view messages, asymmetric encryption, also called public key encryption, uses a pair of keys, namely a public and a private key. The public key is published in a public directory and the corresponding private key is kept secret.

Depending upon the level of inquiry, which a certifying authority may undertake to confirm the identity of public key holders, different types of certificates may be issued by the Certificate Authority (hereinafter referred to as CA). Class I certificates are designed for casual web browsing and secure e-mail and are issued to the individuals only. Class II are more expensive and confirm that the information provided by the subscriber in his/her application is in accord with the information available in a well recognized consumer data base. Class III certificates will require personal presence of the subject or he may submit registered credentials and pass an automated identification check**. Class IV** certificates involve through investigation of both an individual as well as organization whether private or public.

IV. REGULATION OF CERTIFYING AUTHORITY

The problem of identification of public key holder can be solved by appointing a third party, trusted by sender as well as recipient to perform the tasks necessary to associate a person or entity with a specific public key. This third party is generally called as Certifying Authority (hereinafter referred to as CA). It is a trusted body either public or private that ascertain the identity of the applicant of digital signature certificate and certifies that the public key of a public-private key pair used to create digital signature belongs to that person. The process of issuing a certificate differs from CA to CA. Generally, it requires:

- ✓ Public-private key pair to be generated by the applicant.
- ✓ Proof of identity such as identity card, driver's license or passport.
- ✓ The applicant demonstrates that he/she holds the private key corresponding to the public key without disclosing the private key. Once the CA has verified the association between an identified person and a public key, the CA then issues a certificate. The person to whom the certificate is issued is called subscriber.

The regulation of CAs is primarily done by the Controller of Certification Authorities (Controller), who is vested with the functions of licensing, certifying, monitoring and overseeing the activities of CAs. The central government notified the Certifying Authority Rules (CA Rules) on 17 October 2000, which prescribe the conditions under which CAs can apply for a license in India, and carry on their operations. The IT Act, 2000 has adopted an extremely complex mechanism for the registration and operation of the CAs.

V. DUTIES OF SUBSCRIBERS

The Chapter-VIII, the IT Act, 2000 contains sections 40 to 42. Every certifying authority has certain responsibilities. The subscribers too have certain responsibilities. Chapter-VIII specifies the duties of subscriber. The term "subscriber" is defined in section 2(2) (1) of the IT Act, 2000 as a person in whose name the digital signature certificate is issued. The IT Act, 2000 envisages a pair of keys - one private and the other public. It is the responsibility of the subscriber to retain control of his private key corresponding to the public key listed in its digital signature certificate. The subscriber should keep the identity of his digital signature secret. He should use the digital signature himself. He should not reveal it to others. He owes a duty to inform the certifying authorities without any delay in case his private key has been compromised in any manner. The Information Technology Draft Bill, 1998, Section 63(l) (g) included such fraudulent acts and makes it a crime. Such a clear definition is conspicuously absent in the IT Bill, 1999. The IT Act, 2000, has made amendments to section 464 of the Indian Penal Code, 1860 that comprehensively cover all kinds of fraudulent acts committed on or through the internet.

VI. ADMISSIBILITY OF ELECTRONIC EVIDENCE

The United Nation Commission on International Trade Law (hereinafter referred to as UNCITRAL) Model Law of Electronic Commerce 1996 (Model Law) includes a provision dealing with admissibility and evidential weight of data messages. The expression data messages is defined to include information generated, sent, received or stored by electronic, optical or similar means, including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy. Article 9 of Electronic Commerce 1996 (Model Law), provides that the rules of evidence must not deny the admissibility of a data message in evidence on the sole ground that it is a data message, nor where the data message is the best evidence reasonably available, on the grounds that it is not in its original form. The UNCITRAL Model law on Electronic Commerce (1996) deals with the admissibility and evidentiary weight of data messages in Article 9(1). The article mandates that in any legal proceeding, the rules of evidence should not apply to exclude a data message because it is a data message (electronic format) or, if it is the best evidence that the person adducing it could reasonably be expected to obtain on the ground that it is not in its original form. The Enactment Guide of the UNCITRAL Model Law on Electronic Commerce, as regards Art (9) states, the purpose of.... Art 9(1) is to establish that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form; puts emphasis on the general principles stated in Article 4 and is needed to make it expressly applicable to admissibility of evidence. Particularly complex issue might arrive in certain jurisdiction in an area.

A. EVIDENCE AND COMPUTER GENERATED EVIDENCE

The law should be indicative of positive acceptance of the use of information technology and dynamism to facilitate its growth. The proliferation of Computers/Internet has created a number of problems for the law. Many legal rules assume the existence of paper records, of signed records, of original records. The Law of Evidence traditionally relies on paper records as well though of course oral testimony and other kinds of physical objects have always been part of court-rooms, too. As more and more activities are carried out by electronic means, it becomes more and more important that evidence of these activities by available to demonstrate the legal rights that flow from them. The term reliability has caused confusion between the principles of authentication, best evidence, hearsay and weight. There has been a growing demand from industry and users for new types of signatures to effectively substitute the hand written signature in the electronic environment, granting integrity, confidentiality and authenticity of information and documents. The advent of the internet is similar to that of the telephone, telegraph, and fax machine communication is facilitated. The internet must be facilitated the focus must be on facilitating the speed and use of technology with specific reference to evidence, the admissibility of electronic evidence in order to ensure a proper examination of electronic evidence adduced before the court. The system so devised to encompass technologies. Technologies have revolutionized our lives.

With the enactment of the Information Technology Act, 2000, the law recognizes electronic counter parts of paper documents and signatures. They are admissible in courts. They may be proved with few barriers such as requirements of originals. Thus, electronic records are vulnerable to tampering and there is no full proof way of authentication. However, the acceptance and reliance on such forms of evidence to be tailored to the needs of each case Hon'ble Judges may exercise careful method of deciding this as there is no objective standard for integrity depending on the peculiarity of the system.

B. INDIAN POSITION

The Indian Evidence Act, 1872 when compared with the General Clauses Act, 1897, excludes the world ‘written’ from the definition of ‘document’. The focus of this statute is the purpose the document is to be used for i.e; recording the matter. The Evidence Act further goes on that, some limited exception, when the contents of a document are to be proved, the document itself has to be adduced and copies of it shall not be admissible. The way to examine an electronic document is by displaying it on a secondary device, either a screen or a printout. It is a tenable argument that such display is not original, but amounts to a copy and is therefore, inadmissible as evidence. Indian law does not resolve this issue. An alternative route could be using the evidence for corroborative purposes. Oral evidence can be introduced if it relates to the relevant fact.

Further, under the second proviso to section 60 of the Indian Evidence Act, if the oral evidence refers to the existence or condition of any material thing other than a document, the court may require the production of such material thing for inspection. Thus, if oral evidence as to the existence of a contract is adduced, then computer evidence may become admissible as it can be termed as material thing. Therefore, computer evidence may be allowed to corroborate the oral evidence.

In *MP Verma* v. *Surinder Kaur*, Indian courts have allowed tape recordings to be admissible in this manner. With the passing of Information Technology Act, 2000 discussion on this point becomes purely academic. The Act through its amending section brings in a new section 65B into the Indian Evidence Act, which starts with the heading Admissibility of Electronic records. It says that any information contained in an electronic record with is pointed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be also document, if the condition mentioned in this section are satisfied. Thus, with the amendment to the Evidence Law, an electronic document can for all practical purposes have the same legal effect as a paper based original document so long as the conditions mentioned in sub clauses of the amended section are satisfied.

VII. CONCLUSION

The Indian government tried to fill up gap to cyber law by passing the Information Technology Act, 2000. However, some issues are still not covered by the Act, which have wide ranging ramification for the growth of E-Commerce in India. The information technology has imposed new legal problems that do not have a precedent in the common law world. The principle of common law has become inapplicable to the legal issue that has evolved in cyberspace, which knows no boundaries and physical environment. These issues do not have any solution in the existing legal regime. However, the Information Technology Act, 2000 tried to fill the gap but in many situation, it becomes not applicable. Thus, the legal positions pertaining to the electronic transactions as well as civil liability for the acts executed in cyberspace is still blur.The Digital Signature can provide a high degree of assurance that a message is originated from a particular person and that its contents could not been altered in transmission. However, no system can provide an absolute guarantee but there seems little doubt that in term of authenticating the terms of a message and the identity of the sender. A well managed system of encryption may be less susceptible to forgery and fraud in comparison to traditional method of contracting.

The Information Technology Act, 2000, has also not touched payment issue and so there seems no any legal status or validity of an electronic instruction for payment in India. Negotiable Instruments do not include in the applicability of the Act but all transaction concerning with or relating to E-Commerce involving the Negotiable Instruments Act would go to civil courts. The Information Technology Act, 2000 also does not expressly exclude cash and by necessary implication, it may be argued that the Information Technology Act, 2000 would apply in case of cash transaction for E-Commerce. However, actual implication is yet to be seen. In addition, the Information Technology Act, 2000 could not touch the issue of e-transfer of funds. The Information Technology Act, 2000 mentioned about the authentication of the digital signature. Still it is not functional and practical. Hence, govt. should take some effective measures to make the digital signature practical to boost E-Commerce.

REFERENCES

[1] Farooq Ahmad Mir, “Emerging Legal Issues of E-Commerce in India” 2(2) International Journal of Electronic Commerce Studies (2011).

[2] Farooq Ahmad, Cyber Law in India (New Era Law Publication, 4th edn., 2013).

[3] Fatima, Talat, Cybercrimes (Eastern Book Company, Lucknow, 1st edn., 2011).

[4] Gaur, K. D., A Textbook on The Indian Penal Code (Universal Law Publishing Co. Pvt. Ltd New Delhi, 4th edn., 2013).

[5] Hossein Bidgoli, Electronic Commerce: Principles and Practice (Academics, California, 2002).

[6] Kamath, Nandan, The Law Relating to Computers, Internet and E-Commerce (Universal Law Publication Co.2nd edn., 2000).

[7] Kapil Raina, "Evidentiary Value of E-Contracts," available at: http://www. legalserviceindia.com/article/l127-E-Contracts.html (last visited on February 5, 2013).

[8] Kaushik, Anjali, Sailing Safe in Cyberspace (SAGE Publication Ltd, London, 1st edn, 2013).

[9] Kesari, U.P.D., The Administrative Law (Central Law Publications, 2003).

[10] Madan Lal Bhasin, "E-Commerce Payment Systems" 4(1) chartered secretary (2007).

[11] Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publication Co.2nd edn., 2000).

[12] Pradeep Kaur, Mukesh M Joshi, "E-Commerce in India: A Review" 3(1) International Journal of Computer Science and Technology (January-March, 2012).

[13] R. K. Chaubey, An Introduction to Cyber Crime and Cyber Law (Kamal Law House, Kolkata, 1st edn., 2008).

[14] Rahul Malthan, Law Relating to Computers and Internet (Butterworths India, New Delhi, 1st edn., 2000).

[15] See, Article 9(1)(a) of UNCITRAL Model Law on E-Commerce (1996).

[16] See, available at: http://europa.eu.int. (last visited on September 18, 2011).

[17] See, available at: http://www.wto.org. (last visited on September 18, 2011).

[18] Sridhar Vaithianathan, "A Review of E-Commerce Literature on India," available at: http://download. Springer.Comstaticpdf186art%253a10.1007%252fs10660 -010-9046-0.Pdfauth66 =1393853765_Ceb2a84f1fc05f57 feba8b3b56086344&Ext=.Pdf (last visited on February 1, 2013).

[19] Subhajit Basu, Richard Jones, "E-Commerce and The Law: A Review of India's Information Technology Act, 2000"12(1) Contemporary South Asia (2003).

[20] Tabrez Ahamad, Cyberlaw E-Commerce and M-Commerce (A.P.H. Publishing Corporation, 1st edn., 2003).

[21] V.D.Dudeja, Cyber Crimes and Law: Cyber Crimes and Law Enforcement (Commonwealth, 1st edn., 2002).

[22] Vakul Sharma, Information Technology Law and Practice (Universal Law Publication Co., 1st edn., 2004).

[23] Kumar, Sujeet, Encyclopaedia of Cyber Laws ABD Publishers, New Delhi, 1st edn., 2011).