HOCHSCHULE FURTWANGEN UNIVERSITY

Law in online business with special focus on India

Name: Radha krishan
Immatriculation Number: 230456
Course: BCM
Subject: E-Business Technologies
Professor: Dr. Eduard Heindl

Declaration

I here by declare that work done in this term paper is based on my own research and thoughts. The sources that are used as references are mentioned at the end of the paper.

Radha Krishan

Table of contents:

1. Introduction

The growth of electronic commerce has created the need for vibrant and effective regulatory mechanisms, which would strengthen the legal infrastructure that is crucial to the success of electronic commerce. All of these regulatory mechanisms and the legal infrastructure come within the domain of cyber law. Cyber law is important because it touches almost all aspects of transactions and activities concerning the Internet, the World Wide Web and cyberspace. As the nature and scope of the Internet is changing, it is perceived as the ultimate medium ever evolved in human history. Every activity in cyberspace can and will have a cyber legal perspective. From the moment a person registers a domain name, sets up and promotes his or her web site, and then conducts electronic commerce and has transactions on the site, various cyber law issues are involved. As the Internet grows, numerous legal issues arise relating to domain names, intellectual Property rights, electronic commerce, privacy, encryption, electronic contracts, Cyber crime, online banking, spamming and so on. The arrival of the Internet and related technologies has made irreversible changes to the world today. In a world, which is moving steadily towards the information society and knowledge economy, it is essential that law must contribute its inputs to promote e-commerce. As cyber law develops around the world, there is a growing realization among different nations that their laws must be harmonized and international best practices and principles must guide implementation. Many countries are trying to establish legal regimes in order to promote online commerce. However, India has, enacted e-commerce laws. India enacted the Information Technology Act, 2000 India is an excellent example of how legal systems mature with the passage of time in order to provide the required boost to e-commerce. E-commerce law in India is the Indian Information Technology Act, 2000.

United Nations' Definition of Cyber crime-

This is age of information technology and there are no physical boundaries which can govern cyber law. Hence it makes more sense to have an international definition of cyber law so…

United Nations' Definition of Cyber crime-

Cyber crime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber crime was broken into two categories and defined thus:

a. Cyber crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or

network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.
Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

2. Cyber law

Many believe the Internet to be full of natural anarchy, so that a system of law and regulation for the Internet seems contradictory. However, cyberspace is, in fact, governed by a system of law and regulation called cyberlaw. There is no single exhaustive definition of the term cyberlaw. One broadly accepted definition of cyberlaw is a generic term that refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of people in cyberspace comes within the domain of cyberlaw. The first use of the term cyberspace was in 1984 by author William Gibson inhis science fiction novel . It described the virtual world of computers. Today, cyberspace is how most people describe the world of the Internet. Though far from the immersive virtual reality of the fictional version, and often regarded as an overused buzzword, cyberspace has become synonymous with the Internet. However, cyberspace is not the World Wide Web alone. The rapid growth of technologies and the Internet made it clear that no activity on the Internet can remain free from the influence of Cyberlaw. Publishing a web page is an excellent way for any commercial business or entity to increase its exposure to millions of people, organizations and governments worldwide. This feature of the Internet is causing much controversy in the legal fraternity. Cyberlaw is also a constantly evolving process. As newer opportunities and challenges are surfacing, cyberlaw is being modifying to fit the needs of the time.

3 Cyber law in India(IT Act 2000)

The Parliament of India passed its cyber law in the form of the Information Technology Act, 2000, which provides the legal infrastructure for e-commerce. The Act received the assent of the President of India and became the law of the land on17 October 2000. The objective of the Information Technology Act, 2000 would be to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information. The act also facilitate electronic filing of documents with various government agencies and further to amend 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. The Act thereafter stipulates numerous provisions in order to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act further states that unless otherwise agreed to, the acceptance of a contract expressed by electronic means of communication shall have legal validity and enforceability. The Act would facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles to electronic commerce that result from the celebrated uncertainties relating to writing and signature requirements over the Internet. The objectives of the Act also aim to promote and develop the legal and business infrastructure necessary for implementing electronic commerce.

The Act stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify the electronic record by the use of a public key of the subscriber. It contains details about e-governance and provides, among other things, that where any law provides that information or other matters shall be in writing, typewritten or printed form, then, notwithstanding anything contained in such a law, that requirement should be satisfied if the information or matter is:

(a) Rendered or made available in an electronic form;

(b) Accessible to make it usable for subsequent reference.

That chapter also provides details about the legal recognition of digital signatures.

The various provisions give further elaboration about the use of electronic records and digital signatures in government agencies. The Act also refers to publication of rules and regulations in an Electronic Gazette. It gives a scheme for the regulation of certifying authorities. The Act provides for a controller of certifying authorities who shall perform the function of supervising the activities of certifying authorities as well as setting standards and conditions governing the certifying authorities. The controller also specifies the various forms and the content of digital signature certificates. The Act acknowledges the need to recognize foreign certifying authorities

and it further details the various provisions for granting the license to issue digital signature certificates. The duties of subscribers are also covered. The Act also covers penalties and adjudication for various types of offences and mentions the power and qualifications for the adjudicating officer. A provision foresees a Cyber-Regulations Appellate Tribunal where appeals against the orders passed by Adjudicating Officers could be referred. The tribunal would not be bound by the principles of the Code of Civil Procedure, but would follow the principles of natural justice and have the same powers as a civil court. Any appeal against an order or decision of the Cyber-Regulations Appellate Tribunal would be made to the High Court. It covers various offences and stipulates that the investigation must be by a police officer only, and that officer should have the rank of deputy superintendent of police or higher. These offences include tampering with computer source documents, publishing obscene information in electronic form, breach of confidentiality and privacy, misrepresentation, publishing a digital signature certificate that is false in certain particulars and publication for fraudulent purposes.
Hacking and penalties if found guilty have been defined in Section 66. For the first time, punishment for hacking has been designated as a cyber crime. The Act also provides for constituting the Cyber-Regulations Advisory Committee, which would advise the government about any rules or other matter connected with the Act. The Act also has four schedules which amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them conform with provisions of the IT Act.
Overall, the Information Technology Act, 2000 is considered to be a commendable effort by the government to create the necessary legal infrastructure to promote and encourage the growth of electronic commerce. India has incorporated some aspects relating to cyber crime into its cyberlaw.Certain acts have been stipulated as cyber crimes with punishment in the form of imprisonment and fines.

4 Some features of law in online business

Digital Signature Certificates
Certifying authority to issue Digital Signature Certificate**. -** (1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.
(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:
Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate; the applicant holds a private key, which is capable of creating a digital signature; the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:
Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection

Secure Electronic records and secure digital signatures

Legal recognition of digital signatures. **-** Where any lay provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.
Explanation.- For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, means affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Secure digital signature.- If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was – (a) unique to the subscriber affixing it;
(b) capable of identifying such subscriber;
(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which related in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

law for Certifying Authorities

Certifying Authority to follow certain procedures.- Every Certifying Authority shall,- (a) make use of hardware, software, and procedures that the secure from intrusion and misuse;
(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
(d) observe such other standards as may be specified by regulations.

Recognition of foreign Certifying Authorities. - (1) Subject to such conditions and restrictions as may be specified, by regulations, the Controller may, with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any Certifying Authority as a Certifying Authority for the purposes of this Act.
(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
(3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1), he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

5 Advantages of law in online business

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.
From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
Digital signatures have been given legal validity and sanction in the Act.
The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. The Act now allows Government to issue notification on the web thus heralding e-governance.

The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
Under the IT Act, 2000, it is possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

6 Challenges of law in online business in India

Another issue that requires attention is the fact that law enforcement agencies and the police need to be duly trained about the various issues relating to e-commerce laws. While some acts have been designated as cyber crimes in India, with punishment by imprisonment and fine, a large number of cyber crimes that have already emerged still have not been regulated by the e-commerce laws of India.
Since the enactment of the Information Technology Act 2000 in India, there is the start of some awareness about cyber law and cyber crime related issues. However, given the vast size of the country and the enormity of the task at hand, all existing actions have had virtually minimal impact. There is a need for the government to come up with strong training and awareness programmes on all related issues pertaining to cyber law and cyber crime. The crucial sectors that are to be targeted have to be identified as a matter of policy and then appropriate programmes have to be targeted. The Government needs to target all statutory authorities who have been constituted under the Information Technology Act for training and orientation. These statutory authorities include the Adjudicating Officers as well as the various Certifying Authorities. Adjudicating Officers are the relevant statutory authorities who have been given the power to grant damages by way of compensation up to the amount of Rs. 10 million, if certain specified unauthorized acts take place pertaining to computers, computer systems or computer networks. At present the Adjudicating Officers in India are not aware about how to proceed in adjudicating claims for damages by way of compensation. This is due to the way in which the Central Government by means of notification has only stipulated the Information Technology Secretaries of different states as the Adjudicating Officers. By designating technocrats to perform quasi-judicial functions without giving them appropriate training or orientation, only leads to complications of problems. This has resulted in a scenario where the

adjudicating officers are not oriented to perform their quasi-judicial functions. The Government of India also needs to plan and implement special awareness and orientation programmes for police officers. The Information Technology Act 2000 stipulates that cyber crime in India shall only be investigated by a police officer not below the rank of Deputy Superintendent of Police (DSP). Given the practical reality where a DSP in India, as a high ranking police officer, is already burdened with other critical issues and pressing problems and responsibilities, cyber crime investigation and prosecution becomes an extremely low priority for them. There is no orientation given to the police officers in an organized, systematic basis. Special training programmes are needed for those police officers who are designated to deal with cyber crime.

For the legal profession, there are various areas, which require maximum Capacity-building. Lawyers in India are not very aware of information technology legal provisions and there is a compelling need to educate them. Lawyers need to be trained appropriately about various relevant issues relating to e-commerce law and the technical nuances of the law.

Judges also need to be duly trained about the various legal issues pertaining to the Information Technology Act, 2000. People in the lower and middle level judiciary are almost completely unaware of the various nuances and other technical details concerning such e-commerce laws. This area needs to be seriously and urgently addressed.

Cyber law training also needs to be given to the government departments and the relevant officers engaged in e-commerce and e-governance activities. This is essential, as the preamble of the Information Technology Act specifically states that the objective of this law is to promote e-commerce and electronic filing of documents with government agencies. Nothing much has been done to facilitate access by consumers to the tribunal court alternatives for e-commerce disputes. The Indian e-commerce law has only provided that one statutory authority be established, namely adjudicating officers. At the time of writing, only one case has been filed in India before the adjudicating officer for grant of damages by way of compensation under the Indian Cyber law. This industry and the public at large have been generally unaware of the provisions and remedies stipulated under the law. Until such time as the government starts massive capacity-building programmes and initiatives, the situation is likely to continue to remain the same. Various institutes in India conduct courses on cyber law for lawyers, students and other professionals. However, most of these courses are pure commercial ventures and the quality of knowledge and awareness imparted is not up to the standard and often leaves much to be desired. With the media reporting cyber law related issues ,as well as various cases conducted under the law, awareness about crimes conducted over the Internet has been slowly increasing. As time flies fast, e-commerce continues to grow with each passing day. However, a look at the existing laws shows that it will take a large amount of time and effort for South

Asian countries to effectively put their legal regimes in agreement with the existing international best practices and procedures.

7 Future of law in online business in India

India's Cyber Law is Outdated

India's Information Technology Act of 2000 is completely outdated and not fit to deal with cyber crimes. It is said that the law was promulgated years ago primarily to bolster the e-commerce business and not intended to deal with cyber crime issues.

Improvements to be made

1. Rules Needs Reform:

India, which is riding on the success of its fledging Business Process Outsourcing industry, will soon feel the pinch with many multinational companies having a second thought to set up a shop in a country where the cyber law is completely outdated.

2. Unfit to Deal with Today's Crimes:

The Federation of Indian Chambers of Commerce and Industry said IT law clauses relating to transmission of obscene material through electronic media should be changed.

3. Changes recommended:

when the law was framed, there were no technologies like MMS or sophisticated devices like mobile phones Latest News about mobile phones with cameras. The IT Act is struggling to cope with the change in modern technology.

India poised to tighten data protection law (future)

India is likely to have a tighter data protection and privacy regime in place later, after bowing to pressure from Western users of outsourcing services. The National Association of Software and Service Companies (NASSCOM) in Delhi is confident that new measures will be passed as law in the coming session of India's parliament, Opponents of offshore outsourcing to India have often cited the absence of a data protection and privacy law in India as a strong reason for stopping the movement of call centre and BPO work to the country.

Rather than have a separate law to deal with data security and privacy issues, the government is considering an amendment to its Information Technology Act of 2000. NASSCOM is in the process of inserting new clauses in the IT Act 2000, and these are being reviewed by the government. The act in its existing form only covers unauthorized access and data theft from computers and networks, with a maximum penalty of about $220,000, and does not have specific provisions relating to privacy of data. The new clauses are likely to enable the act to conform to the so-called adequacy

norms of the European Union's Data Protection Directive and the Safe Harbor privacy principles of the US, according to NASSCOM.
The adequacy norms allow the EU to declare that third-party countries have levels of data protection that conform to European standards and thus allow data on EU citizens to be transmitted outside of the union.
India is negotiating with the EU to get it to recognise India as a country that offers an adequate level of protection for personal data. Until a tighter data protection legal regime is in place, foreign customers are relying upon contractual obligations to impose obligations for protecting and preserving data, according to Duggal.
Even though the government has delayed the implementation of a legal framework for prosecution of data and privacy breaches, Indian BPO companies have implemented processes such as the BS7799 standard for information security management.
Standards such as BS7799, and the ISO17799 standard for information security, restrict the quantity of data that can be made available to employees of BPO and call centers.

8 Conclusion

The Indian experience has shown that it is easy to enact law on paper. However, it is extremely difficult to enforce laws in actual practice. There are numerous challenges that require appropriate awareness among citizens about e-commerce laws. This is so because at the end of the day, the e-commerce laws are basically targeted to protect and help those citizens .It is also necessary for ensure that there is adequate training of the relevant departments and government officials who would draft and implement policies relating to e-commerce.

References:

Ecommerce Times By: Harbaksh Singh Nanda Date: December 23, 2004

Na. VIJAYASHANKAR

http://www.hinduonline.com/

http://www.hinduonnet.com/thehindu/br/2003/04/29/stories/2003042900070300.htm

Tuesday, January 17, 2006
by: Praveen Dalal

http://www.ipfrontline.com/depts/article.asp?id=8507&deptid=6

http://www.ipfrontline.com

http://www.vakilno1.com/bareacts/informationtechnologyact/informationtechnologyact.htm

http://www.legalserviceindia.com/cyber/itact.html

http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf

India's Information Technology Act, 2000

By Pavan Duggal (editorial advisor, Inomy.com, and advocate, Supreme Court of India)

Source: Inomy.com 11/06/2000