



## CHAPTER I: INTRODUCTION

*"This is just the beginning; the beginning of understanding that cyberspace has no limits, no boundaries."*

—**Nicholas Negroponte**

The term 'Cyberspace' was first coined in 1980's by Science fiction writer William Gibson.<sup>1</sup> However, a clear definition of the term still seems hard to come by. In general Cyberspace represents the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication. This includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.<sup>2</sup> Further, cyberspace like physical space could also be categories in four sub concepts i.e. place, distance, size and route.<sup>3</sup>

In today's global world Internet is a mode of communication. The real power of Internet is that it is borderless and available to anyone with a computer and a telephone.

Not very long back when the scope of internet access was very limited, there was no requirement of law relating to cyberspace. The concept has been developed, recently with the advent of the internet, transmission of information and transacting of business across borders, various issues related to cyberspace cropped up on legal front.

---

<sup>1</sup> Cotton, B. and R. Oliver (1994), "The Cyberspace Lexicon: An Illustrated Dictionary of Terms from Multimedia to Virtual Reality", Phaidon Press Inc., p. 54. In words of science fiction writer William Gibson Cyberspace means a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from the banks of every computer in the human system.

<sup>2</sup>Rohas Nagpal, IPR & Cyberspace – Indian Perspective, Asian School of Cyber Law, 2008, p. 4

<sup>3</sup> Rebecca Bryant, ISSN 1393-614X Minerva - An Internet Journal of Philosophy 5 (2001): 142–143.



Earlier, traditional legal system all over the world have had great difficulty in keeping pace with the rapid growth of the internet and its impact whether positive or negative. Therefore, many countries have already laid down cyber laws to regulate this global mode of communication, India is proud to be one of them.

In India, all cyber laws are contained in the Information Technology, Act 2000. The Act was made to provide the legal infrastructure for e-commerce in India. One of the unique features of the act is that it promotes the use of digital signatures for the growth of E-Commerce and E-Governance. However, the act still does not deal with some major legal issues such as Jurisdiction, protection of domain name, infringement of copyright law etc. This led to the formation of various challenges before the Indian Legal system. Therefore, a practical approach is required to minimise the difficulties and for resolving all cyber disputes, happening in our cyberspace.

## **CHAPTER II: CYBERSPACE: ISSUES AT THE FOREFRONT**

The advent of the internet, transmission of information and transacting of business across borders, various issues related to cyberspace have cropped up on the legal front. Some of the major issues are determination of jurisdiction, cyber crime, intellectual property, cyber forensic, E-commerce, Electronic Evidence, privacy and contract. One of the greatest lacuna for resolving these issues is the absence of comprehensive law anywhere in the world. The problem is further aggravated due to the disproportional growth ratio of Internet and cyber law. Though a beginning has been made by the enactment of I.T. Act and Amendments made to Indian Penal Code, Indian Evidence Act etc, problems associated with regulation of cyber crime continue to persist.



### CHAPTER III: CHALLENGES IN CYBERSPACE

Discoveries, Inventions and spread of new Information Technologies brought about by computers, internet and cyberspace widen the scientific horizon but pose new challenges and created problems for the legal world in all aspects of law. The challenges that we facing today are not just confined to any single traditional legal system but in almost all major categories of law such as contract law, criminal law, Law of torts etc.

In India, The information Technology Act, 2000 (ITA) and amendment in several existing laws through ITA does enforce and control a level of cyber related problems. However, it has shown inadequacy of law while dealing with information technology itself. The ITA in many ways falls short of International standards. Therefore, in the era of information technology such loopholes in legal framework cannot be ignored and can lead to some impairment for individual as well as nation. New provisions added through Information Technology (Amendment) Act, 2008 could be a way out from all these challenges but several changes are still needed for the act to ensure both functional equivalence and technological neutrality. Hence, there is an urgent need to redefine the cyber laws in India as per International standards. There are few major areas in cyberspace in which many challenges have been cropped up on legal front. These area are inherent challenges, Legal Challenges, technological challenges, Political and social challenges, practical challenges etc.

#### **1) Inherent Challenges:**

In many countries the laws related to cyberspace have already been developed. U.S. and the West drafted their own legislations by either adapting their existing laws in the context of cyberspace or creating new laws in respect thereof. Determining jurisdiction and formation of e-contracts are two key issues on which traditional legal principles have been largely applied by Courts



worldwide.<sup>4</sup> India enacted its first law on IT through the IT Act, 2000 based on the principles elucidated in the UNCITRAL Model law of e-commerce. It extends to whole of India and also applies to any offence or contravention there under committed outside India by any person.

## 2) Legal Challenges:

### a) Jurisdiction

Jurisdiction is the authority of a court to hear a case and resolve a dispute. The issue of Jurisdiction is highly conflicting and debatable in cyber law as to the maintainability of any suit which has been filed. It becomes more complicated largely on account of the fact that the internet is borderless. The notion of jurisdiction is rooted in territoriality from the point of view of both the court which can properly assert jurisdiction and from the point of view of the law that should be applied while deciding the dispute. In domestic transactions, a court will always have the jurisdiction to enforce their respective laws within their physical, geographical and political boundaries but the enforcement issues throws up several challenges when it comes to international transactions due to constant change in technology in borderless cyberspace. There have been various principles and test that laid down by the court in U.S. and U.K. which elaborated the scope of jurisdiction and the same is being followed by the Indian Court.<sup>5</sup>

#### i. Conflicting Jurisdictional Problems

- In the cyberspace, there is no geographical boundary. It establishes immediate long-distance communications with anyone who can have access to any website.
- No judicial body exists to deal with legal commercial problems arising between citizens of different countries. The court while considering the scope of jurisdiction in

International transaction, the issue of applicability will always arise, another point being is

---

<sup>4</sup> For e.g. *Longarm Statutes enacted in US and Minimum Contacts test.*

<sup>5</sup> 'Minimum Contacts test' as developed by the U.S. Supreme Court in *International Shoe Co. v. Washington*, 326 U.S. 340 (1945); 'Sliding scale test' as laid down in *Zippo Manufacturing v. Zippo Dot Com*, 952 F. Supp. 1119 (D.C.W.D. Pa. 1997). 'Purposeful availment test' as laid down in *Hanson v. Deckla*, 357 U.S. 235 (1958)



that in general while court see that the jurisdiction of court will always depend upon the issue that whether the court was correct in deciding the jurisdictional issue or not. The court will strictly look upon

- There is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of law, particularly private international law.
- ii. **Where the contents of a web site are legal in one country and illegal in another:** In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.
- iii. **Position in Europe-** The Brussels convention is the controlling document for jurisdictional issue within the European Union ("E.U."). Also the fundamentals of jurisdiction within EU countries are based on statute or regulation, instead of constitutional due process applied in case laws, as in the U.S.
- iv. **Position in India-** In India, all cyber laws are governed by the IT Act. However, IT Act does not deal with some major legal issues including the issue of jurisdiction. It is well-established law in India that where more than one court has jurisdiction in a certain matter, an agreement between the parties to confer jurisdiction only on one to the exclusion of the other(s) is valid. In case there is no agreement, the respective court considers the balance of convenience and interests of justice while deciding for the forum.

#### **b) Cyber Crime**

Cyber crime is a crime committed over the Internet. It could be against the government, property and against any person in various forms. Nowadays, the law enforcement agencies are facing difficulties in dealing with cyber crime. In India, Information Technology Act, 2000 is the legislation that deals with issue related to cyber crime.



Today Cyber crime is a bigger threat to India in comparison to physical crime. In a survey conducted by National crime records Bureau, Ministry of Home Affairs shows that that cyber crime is increasing everyday in various forms.<sup>6</sup>

**c) Contractual Difficulties**

Recently, India has emerged as a major player in the computer software and resources sector. Data shows that India will have the largest number of internet-users in Asia in near future. In all e-commerce, the validity and the formation of contract is very essential. The ITA deals with some contractual aspects in E-commerce. However, several practical problems arise when we form a contract.

The Indian Contract Act, 1872 gives a statutory effect to the basic common law contractual rule that a valid contract may be formed if it is made by free consent of the parties, competent to contract, for a lawful consideration and for a lawful object and which is not void ab initio.<sup>7</sup>

In general contract, we see that the acceptor can revoke acceptance of the offer before it comes to the knowledge of the offeror, but what would be the case where an acceptance is sent via an electronic record, it may not be possible for the acceptor to revoke it before it comes to the knowledge of the offeror. However, there may be one possibility where revocation may still take place i.e. when the acceptance is sent by an electronic record and the same is sent to a computer resource which is not the designated computer resource of the offeror, but it is not clear what would prevail when both the acceptance-revocation are retrieved by the offeror at the same time. Indian courts following the traditions of common law have developed the doctrine of “last-shot rule<sup>8</sup>”. This cardinal rule states that an acceptance should be unqualified and absolute and any acceptance even with little variation is no acceptance at all.

---

<sup>6</sup> <http://ncrb.nic.in/ciiprevious/Data/CD-CII2007/cii-2007/.home.htm>

<sup>7</sup>Section 10, Indian Contract Act, 1872.

<sup>8</sup> The Last shot rule is also known as mirror image rule, according to Indian law, a contract comes into existence only when the acceptance is a mirror image of the offeror’s exact offer. Indian laws provides for ‘the mirror image



The Contract Act does not prescribe or favour any particular way of communicating offer and acceptance. It may be done by word of mouth, writing or even by conduct.<sup>9</sup> Thus, there is no requisite of writing for the validity of contracts except for cases which are specifically required by law to be in writing. Therefore, it would appear that the IT Act avoids incorporating any specific provision giving validity to online contracts.<sup>10</sup>

**d) Protection of Intellectual property**

Intellectual Property is a property that arises from the human intellect. It is a product of human creation. In broad field of IPR, there are various acts which govern intellectual property assets. In cyberspace, the problem began when unrelated party started using intellectual property of others or of famous brand with the intention to use it otherwise. Section 65 of ITA provides for protection of IPR from misuse. In the present scenario, trademark disputes pose a serious challenge, as that is one area where the major developments have taken place. One of the first issues to arise in relation to IPR due to cyberspace was with respect to domain names.

In the area of IPR violations and infringement across borders, there is yet to develop a universal law. The TRIPS Agreement is not the 'uniform' law in the area. Resort is still to be had to private international law.

**e) Electronic Evidence**

Each time a crime is committed whether in physical form or in cyber space, the success of prosecution largely depends on the quality of evidence presented at the trial, but this pose a serious challenge before the investigation agencies to collect and preserve the evidence.

---

rule' that states, an offer must be accepted exactly as offered and without modifications. A contract is formed, only when the acceptance of an offer is absolute and same as the terms of the offer.

<sup>9</sup> Section 3, Indian Contract Act, 1872

<sup>10</sup> However, the UNCITRAL Model Law has a specific provision regarding validity of contracts.

*"Article 11. Formation and validity of contracts.—(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose."*



The Indian Evidence Act, 1872 (section 3) and Information Technology Act, 2000 (section 4) grants legal recognition to electronic records and evidence submitted in form of electronic records. In a leading case of *State vs. Mohd. Afzal and others*<sup>11</sup>, The Delhi High Court held that electronic records are admissible as evidence, the court further, concluded that the person who is challenges the accuracy of computer evidence on the ground of misuse of system, then the person challenging it must prove the same beyond reasonable doubt. Mere theoretical and generic doubts cannot be cast on the evidence.

The basic principles of equivalence and legal validity of both electronic signatures and hand written signatures and of equivalence between paper document and electronic document has gained universal acceptance.<sup>12</sup> Despite technical measures, there is still probability of electronic records being tampered with and complex scientific methods are being devised to determine the probability of such tampering. For admissibility of electronic records, specific criteria have been made in the Indian Evidence Act to satisfy the prime condition of authenticity or reliability which may be strengthened by means of new techniques of security being introduced by advancing technologies.

International cooperation is required in providing electronic evidence in order to meet out the problem of international terrorism.

### **3) Technological Challenges**

Globalization and ICT (Information and Communication Technology) revolution in India has changed the form of information drastically. It made information more accessible portable and handy. Fast-shifting trends in both technologies and threats make it likely that the security issues of the IT infrastructure will only intensify in the coming years. The increasing complexity of IT systems and networks, which will present mounting security challenges for both the providers

---

<sup>11</sup> (2003 (71) drj 178)

<sup>12</sup> Krishna Kumar, "*Cyber Law: Intellectual Property and e-commerce security*," at 295.



and consumers. The expanding wireless connectivity to individual computers and networks, which increases their exposure to attack. In hybrid or all-wireless network environments, the traditional defensive approach of securing the perimeter is not effective because it is increasingly difficult to determine the physical and logical boundaries of networks.

**i. The Right of Privacy vis-à-vis Data Protection**

The right of privacy is part of Article 21 of the Indian constitution, but it is not absolute. Disclosure of private information is justified under certain circumstances.

In *Kharak Singh V. State of U.P.*<sup>13</sup>, Apex court read the right to privacy to be within the ambit of Article 21 and construed it as a fundamental right.

The exclusion of privacy protection to only those who are aware of their rights, or the formal recognition of privacy in a legal system is not a challenge faced only by India. Globally, protection of privacy has been a challenge in many countries, and even now it has an uncertain status in many parts of the world.

*The right of privacy may be infringed by:*

- Utilizing private data already collected for a purpose other than for which it was collected.
- Sending of unsolicited e-mails of spamming.
- Unauthorized reading of e-mails of others.

*The relevant sections of the Information Technology Act (ITA) relating to privacy*

- Section 43 provides protection against unauthorised access to the computer system including unauthorised downloading, extraction and copying of data.
- Section 66 provides protection against hacking.
- Section 67 gives protection against unauthorised access to data.

---

<sup>13</sup> AIR 1963 SC 1295



- Section 69 protects against cyber terrorism.
- Section 72 protects an individual's privacy and confidentiality.

#### *Data protection laws*

Though the ITA does enforce a level of data protection, it is far from flawless. The ITA in many ways falls short of International standards and data protections enacted in other countries in the world. It lacks the following:-

- The definition and classification of data types.
- The nature and protection of the categories of data.
- Data controllers and data processors have distinct roles.
- Clear restrictions on the manner of data collection.
- Clear guidelines on the purposes for which the data can be put and to whom it can be sent.
- Standards and technical measures governing the collection, storage, access to, protection, retention and destruction of data.
- It does not provide strong safeguard and penalties against the aforesaid breaches.

#### **4) Political and social challenges**

Nowadays, we find that Media plays an important role in democracy to make people aware about information related to government policy and the grievances which people have. But at the same time it also encroaches on privacy.

Recently, India has adopted new technologies by way of social networking sites like orkut, facebook, twitter etc., where people of same interest groups come together as a community. In such communities lots of people share information of the latest happenings, express their views, criticize on certain issues etc. All these activities can elevate sensitive issues, which may lead to communicable imbalance in the society.



Blogs are increasingly popular in today's world. Through blogs, people can express their thoughts and views on public and government sectors, so there is possibility that sensitive information may be forged and its original intension may be lost.

#### **5) Practical Challenges**

##### *Regulating Cyber Cafes*

The data collected by National crime record bureau suggest that India is under urgent need to redefine its laws on cyberspace. Cyber cafes have emerged as base for cyber crime. Now even terrorist are using cybercafés to communicate with each other. The mushrooming of cyber cafes in the city, which provide the secrecy through cabins, has also made the porn literature easily accessible to the people specially the teenagers. There are various cases in which it was reported that local cyber cafes have been used for sending threatening mails to Chief Minister of a state, Prime minister, President and high officials. Earlier, cyber cafes were required to create detailed records about their customer's browsing habits, but after widespread protests and public outcry, the same was dropped.

##### *Dispute settlement*

The IT Act provides various modes of dispute settlements. However, citizens are not aware of various kinds of commonly committed cyber offences, procedure for filing a case, resolving a dispute. There is also a lacuna of trained judges and skilled investigators.

##### *Contractual Aspect*

This unprecedented growth of internet calls for a legal framework for e-commerce in India. IT act deals with some contractual aspect in E-commerce. However, several practical problems still exist when we form a contract.



## CHAPTER IV: DISPUTE RESOLUTION METHODS

### i. India

The ITA laid down civil and criminal liabilities for contravention of provisions of the Act and it also provides various means of dispute resolution. For instance it created the office of Adjudicating Authority to adjudge contraventions. Further, Chapter X of IT Act creates a Cyber Appellate Tribunal to oversee adjudication of cyber crimes. However, in a case where there exists an arbitration agreement, the court is under obligation to refer the parties to arbitration in terms of the arbitration agreement.

In *Taylor v Taylor*,<sup>14</sup> It was well recognized that if a statute has conferred a power to do an act and has laid down the method in which that power has to be exercised, it necessarily prohibits the doing of the act in any other manner than that which has been prescribed.

Recently, India has taken various practical initiatives for the disposal of cyber disputes. In March 2001, the Central Bureau of Investigation (CBI) set up the Cyber Crime Investigation Cell (CCIC) to investigate offences under the Information Technology Act, 2000 and other high-tech crimes<sup>15</sup>. In April 2002, India and the United States launched a Cyber Security Forum to collaborate on responding to cyber security threats. Mumbai Cyber lab is a joint initiative of Mumbai police and NASSCOM.

### ii. International Approach

Cyberspace does not recognise geopolitical boundaries. Parties from anywhere in the world can transact business with someone located anywhere else. They do not have to and may not know where the other party is domiciled, where the other party is physically at the time the transaction is being consummated or what the legal regime is at such location. A dispute may arise at any

---

<sup>14</sup> (1876) 1 Ch. D 426

<sup>15</sup> <http://cbi.nic.in.cyber>.



time, specially when different nations apply different laws to similar disputes. Therefore, parties are required to have dispute resolution mechanism which meets their needs.

International agreements and cooperation is required for various dispute resolutions in International arena. Arbitration and mediation could be a first resort for dispute resolution, reason being it has an international treaty i.e. New York Convention on the Recognition and Enforcement of Foreign Awards which provides for ready enforcement of an award in the territory of virtually all trading nations of the globe. Further, the new arbitral procedures of the World Intellectual Property Organisation (WIPO), Council of Europe convention on cyber crime, the virtual magistrate and the Cyber Tribunals are steps towards meeting these needs. For instance recently, India has established a *Cyber Security Forum*<sup>16</sup> to collaborate with United States to collaborate on responding to cyber security threat.

---

<sup>16</sup> Plenary Meeting of India - US Cyber Security Forum, Ministry of External Affairs on India, April 30, 2002



## CHAPTER V: CONCLUSION/SUGGESTIONS

It is important to note that the Internet as with all path-breaking technological developments gives us all the opportunity to act as a global community, advertise and operate across all frontiers, over borders and beyond the control of any national government, but it also created serious problems, challenges for the legal world in all aspects of law due to its borderless nature.

- a. We need to promote and facilitate the fair use of cyber space among general masses, to educate civil society groups about the legal constitutional issues, to assure citizens regarding their concern on privacy, personal liberties, to make citizens aware of various kinds of commonly committed cyber offences such as Fraud, Identity Theft, Hacking, Phishing etc. and freedoms and also there is an immediate requirement of skilled investigators and trained judges for fair and effective dispute resolution.
- b. India needs to identify the possible areas of conflict and operational problems, to address various questions; issues' relating to cyberspace and the most appropriate way to start is the creation of a comprehensive legislation which should address broad area of cyberspace taking into consideration sectoral, institutional and individual requirements. The proposed Communication Convergence Bill, 2001 could be a milestone in answering all these questions.
- c. The amendments in several laws by the IT Act are a good beginning but several changes are still needed for the act to ensure both functional equivalence and technological neutrality.
- d. International agreements by way of convention and cooperation are required for various dispute resolutions in International arena.