CHAPTER-I

INTRODUCTION

Nature has gifted human beings with, mind and brainpower which distinguishes them from other creatures and makes man superior among other living creatures of the universe. The progress of human civilization eventually led to the discovery and inventions of new ideas beginning from the need for survival to luxuries of modern life.

Cyber law is the law governing computer and the Internet Technology. It does not need stating that new communication systems and digital technology have made dramatic changes in our life styles. In today's highly digitalized world almost everyone is affected. A revolution is being witnessed in the way people are transacting. Almost all transactions in shares are in demat form. Almost all companies extensively depend upon their computer networks preserving their data in electronic form consumers are using credit card for shopping. Most people are using e-mails, cell phones and SMS messages for communications. Businesses and consumers are increasingly using computers to create transmit and store information in the electronic form instead of the traditional paper documents. Digital signatures and e-contracts are fast
replacing conventional method of transacting business. With the coming of the computer age the industry has seen a quantum leap in quality, quantity and speed. There is modernisation of life style. However the technology is still developing and unfolding. It is the human mind which generates within men desire for knowledge and capacity for reasoning which culminates into the growth of modern science and technology.

Science as a branch of knowledge is a study of natural phenomenon by way of observation, identification, description, experimentation and systematic investigation and a thrust for reasoning to find out truth beyond usual concepts. Undoubtedly, it has given new dimensions to human capabilities. Science and technology have substantially contributed to the development of human society. Technology may precisely be defined as the application of science or knowledge or any method of accomplishing or applying such knowledge for any particular task using a technical process. Thus it is' the human innovation in action that involves generation of knowledge to extend human capabilities or satisfy emerging human needs and wants. It is therefore, evident that technology brings out changes in the natural world through scientific application of knowledge for material comfort of human beings. As such, the development of science and technology has universally benefited the world by providing all comforts of life. Human
activities in the present day world are directly or indirectly affected by science in many ways. The invention of radio, telephone, television, super-computers etc. and all other technical mechanisms are essentially the outcome of the science and technological developments. Today, we are living in the age of computers, which occupies a significant place in our day to day life.

**Advent of Information Technology**

Ever since the emergence of civilisation men has always struggled for progress, exploring out new modes and technologies for better conditions of survival. Of all the significant advances made by the mankind, the invention of computer is perhaps the most noteworthy achievement which has not only made the human life easier and comfortable but acts as a substitute for human mind for storage of knowledge. From the functional point of view, the computer has even excelled human mind as a source of storing knowledge and information.

The emergence of computer networking has greatly facilitated access and storage of information eliminating constraints of distance and time in communication. They have provided an excellent method of
transmission of information across the world with the result the world has now virtually become a global village.¹

**The History of Computing machines**

The history of modern computer may be traced back to 2000 B.C., that is about four thousand years ago, when the first mechanical device called abacus was developed by the Chinese for being used as a calculating machine. Centuries later, many similar devices were developed but it was in 1642 A.D. that Blaise's calculating machine became the most popular calculating device which could be used by dialing numbers 0 to 9 on its dial disk. Subsequently, Joseph Jaquard a French weaver devised a loom in 1820 that used punch cards to direct the weaving patterns.

It was Charles Babbage (1791-1871) who is called the father of modern computers for his invention of an automatic computing machine designed to do additions at the rate of 60 per minute. It also had a memory where the machine was programmed by instructions coded initially on punched cards and then stored internally.² Later, Babbage, who was a Professor of Mathematics in U.K., invented the first general purpose computer which he called as the Analytical Engine.

The historical evolution of computer will remain incomplete without the mention of Augusta Ada King, a disciple of Babbage, who contributed to the machines design of computer. Her thorough understanding of the machine and its mechanism led to the development of instruction routine which was fed into the computer.

Babbage's analytical engine as improvised by Augusta Ada King consisted of over 50,000 components and input devices in the form of perforated cards containing operating instructions in stored memory of 1000 numbers upto fifty decimal digits. It also consisted of a 'mill' with a controlled device that allowed processing instructions in any sequence and output devices to produce printed results.

Subsequently, an American inventor, Herman Hollerith (1860-1929) further developed the Jacquard's Loom concept to computing. But instead of using Babbage's machine, he used cards to store data information fed into the machine which compiled the results mechanically. Each punch on a card represented one number and a combination of two punches represented one letter. As many as 80 variables could be stored in single card. Besides speedy compilation of

---

3 Augusta Ada King (1815-1842) was the Countess of Lovelace and daughter of well known English poet Lord Byron. She earned fame as the first woman computer programmer.

results, punch cards served as a data storage mechanism and helped in elimination of computational errors. Hollerith introduced punch card reader and founded his Tabulating Machine, in 1896, which eventually transformed into International Business Machine (IBM) around 1924.

Thereafter, a German engineer Konard Zuse devised a computer Z-3 to be used in aeroplanes and missiles which helped the Germans to strengthen their, strategic potential against the British Allied Forces during World War II. As a counter strategic measure, a more powerful computer called Collossus was developed by the British engineer which had secret code breaking mechanism that could easily decode German messages. Thus these two developments were essentially an outcome of the World War II which were instrumental in accelerating the progress of computer technique in time to come.

Taking inspiration from the importance of computers for defence services, American scientist Howard H. Aiken (1900-1973) who was working with IBM, developed an all electronic calculator which was used by the American Naval Forces for creating ballistic charters. It was called Automatic Sequence Controlled Calculator. A year later, John Von Neumann (1903-1957) designed a computer which he named as

---

5 World War II (1939 to 1945).
Electronic Disket Variable Automatic Computer (EDVAC) with a memory to hold stored program as well as data. It consisted of a central processing unit, which allowed functioning of the computer to be controlled and co-ordinated from a single source.

The advances made in computer technology during mid-fifties of the 20th century brought more sophisticated and efficient computers which were much smaller, faster and more reliable than the earlier ones. They became so popular that most companies, business enterprises, industries and even the Government in U.S.A. switched over to computerization in next decade.

The credit of producing a commercially usable computer goes to Remington Rand Corporation. It was initially launched in 1951 and called Universal Automatic Computer (UNIVAC). A decade later, Rand Paul Baran of the Rand Corporation was requested by the U.S. Air Force to study and device a computer which could maintain its command on missiles and bombs in the event of nuclear attack. It was to be a military network which could survive a nuclear attack. This lead Baran to prepare a switched network.
In 1965, most of the large business houses, firms and industrial establishments routinely switched over to IBM computers for maintaining their records and processing their financial information through computer because of its vast storing capacity and cost effectiveness.

Though these newly developed computers contained transistors as a replacement for vacuum tube, they generated considerable heat which often damaged their internal parts and also affected their sensitiveness. In order to eliminate this problem, Jack Kilby of United States developed the integrated circuit in 1968 which combined three electronic components into one small silicon disk made from quartz. Later, semiconductors were also squeezed in the form of a single chip. The device came to be known as ARPANE\textsuperscript{6} (Advanced Research Project Administration Network). Thereafter, the first e-mail program was created by Ray Tomlingson of BBN in 1972. By this time computer had become more user friendly because the software package therein offered an array of applications even to a non-technical user.\textsuperscript{7} With the advance of time there was thrust on having computers smaller in size so as to be easily portable, as a result of which laptops and even pocket computers were introduced which are commonly in use these days.

\textsuperscript{6} ARPANET was developed by U.S. Department of Defence in 1968.
\textsuperscript{7} IBM introduced personal computers (PC) in 1981 for use in homes, offices, educational institutions etc.. They could be linked together or networked to share memory space and communicate with each other.
As a medium of communication, computer has brought about revolutionary changes in transmitting information and has increased the capacity to store, search and retrieve any information through its application. The internet system has enhanced our capacity to communicate over long distances on the frequency waves without the need for any physical connectivity. It has not only made human life easier and comfortable but virtually acts as a substitute for human mind so far storage and assimilation of knowledge and information is concerned. From the functional point of view, the computer has even excelled human mind. The expansion of internet network enables a person to visually see and talk to a person who is sitting thousands of kilometres away in any part of the world.

**Internet**

The terms internet and world wide web (www) are often misunderstood. Although these days the terms are used interchangeably, they in fact mean two different things. The internet is the vast computer network that stores and carries information around the world, the www is the collection of documents that is accessed on the internet through a particular computer language. Put very simple, the *web needs the internet the internet does not need the web.*
**History of Internet in India**

Internet was initially available in India through ERNET. It was made available for commercial use by the Videsh Sanchar Nigam Limited (VSNL) in August 1995. Initially, it started with dial-up in six cities on August 14, 1995 and gradually developed as a potential source of e-commerce in India. The role of fibre optics communication from Integrated Service Digital Network (ISDN) has accelerated the growth of internet in the new millennium. A year later, rediff.com was launched by Shri Ajit Balkrishnan and thus India's first cyber cafe was started in 1996. Thereafter, India's first online banking was launched by ICICI Bank in 1997.

With the introduction of Internet Service Provider Policy (ISP) in 1998, the monopoly of VSNL on Internet came to an end. Satyam Infoway (Sify) was the first ISP which started functioning in India. It will be of historical importance to mention that the first incidence of data being hacked by the teenagers from the Bhabha Atomic Research Centre (BARC) took place in 1998, which was perhaps the first recorded Internet crime in India.

---

8 India ranks 33rd in the world in terms of e-commerce and on-line shopping.
9 Satyam Infoway (Sify) was incorporated in 1995 and was registered under different domain / names.
The expanding dimensions of internet\textsuperscript{10} offered vast scope and opportunities to human beings to identify, evaluate and exchange information for the benefit of public\textsuperscript{11} all over the world. It provided new environment, new culture, new business links and commercial networks virtually revolutionising all walks of human life.

The diffusion and proliferation of information through internet has no doubt proved to be a boon to mankind but at the same time it has its dark side as well. The increased use of computers and Internet has provided scope for new variety of crimes known as cybercrime. Since these crimes are committed through internet in cyberspace they know no geographical limitations, boundaries or distances and the perpetrators of crime remain invisible. As a result of this, these crimes have a potential of causing harm and injury which is of unimaginable magnitude.

With a view to countering internet and computer related crimes, the Indian Parliament enacted a new legislation, namely, the Information Technology Act, 2000, which may be said to be a milestone in India's Internet journey to tackle the problems created by the development of information technology. The Act came into force on October 17, 2000. It

\textsuperscript{10} In 2006, there were about 40 million net users and Internet cyber cafes and more than ten lakh persons engaged in online share trading.

\textsuperscript{11} The Indian Railways launched on-line site in 2001 and Air Deccan was the first airline to start on-line to start on-line air ticketing 2004.
deals with various cybercrimes\textsuperscript{12} related to internet and cyberspace, particularly unauthorised access, virus attacks, denial of access or any contaminant causing damage to computer software etc. But there are still certain grey areas that exist in the cyber law mainly because Information Technology Act is primarily meant to be a legislation to promote e-commerce and therefore, it has not proved very effective in dealing with newly emerging cybercrimes. However, the Government of India appointed an expert Committee in 2005 to look into the lacunae and shortcomings in the Act and suggest necessary amendments therein. It was on the recommendation of this Committee that the Information Technology (Amendment) Bill 2006 was introduced in the Parliament\textsuperscript{13} on December 15, 2006 and finally passed by both the Houses on December 24, 2008.

The Information Technology (Amendment) Act, 2008 (Act 10 of 2009) received Presidential assent on February 5, 2009. Rules have also been framed under the amended Act which became effective from October 27, 2009.

\textbf{Cybercrime}

The offences which take place on or using the medium of the Internet are known as cybercrimes. These include a plethora of illegal

\textsuperscript{12}Chapters IX and XI of the Information Technology Act, 2000.
\textsuperscript{13}Information Technology (Amendment) Bill, 2006.
activities. The term 'cybercrime' is an umbrella term under which many illegal activities may be grouped together. Because of the anonymous nature of the internet, there are many disturbing activities occurring in the cyberspace which may enable the perpetrators to indulge in various types of criminal activities which are called cybercrimes.

The weapon with which cybercrimes are committed is technology and therefore, the perpetrators of these crime are mostly technically skilled persons who have thorough understanding of the internet and computer applications. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail, bombing, cyber pornography, cyber defamation, polymorphic virus, worms etc. Some conventional crimes may also be cybercrimes if they are committed in or through the medium of internet. The examples are theft, mischief; cheating, fraud, misrepresentation, pornography, intimidation, threats etc. which are all punishable under the Indian Penal Code.

As regards exact definition of cybercrime, it has not been statutorily defined in any statute or law as yet. Even the Information Technology Act, 2000 does not contain the definition of cybercrime. However, cybercrimes may precisely be said to be those species of crime in which computer is either an object or a subject of conduct constituting
the crime or it may be even both.\textsuperscript{14} Thus any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime.

The foregoing definition of cybercrime clearly indicates that there exists very thin line of demarcation between conventional crime and cybercrime. The sine qua non for cybercrime is that there should be an involvement at any stage, of the virtual cyber medium i.e. the computer.

A simple yet sturdy definition of cybercrime would be, "unlawful acts wherein the computer is either a tool\textsuperscript{15} or a target\textsuperscript{16} or both". Thus cybercrimes are the crimes directed at a computer or a computer system or a computer network.

Cybercrime as defined internationally by the U.N. Congress on Prevention of Cyber Crime and Treatment of Offenders\textsuperscript{17} comprises two categories as follows:

\textsuperscript{14} Pawan Duggal: Cybercrime (2003) p. 17.
\textsuperscript{15} Cybercrimes which involve computer as a tool are usually modification of conventional crimes such as drug-trafficking, on-line gambling, financial fraud or forgery, cyber defamation, pornography, intellectual property crimes, cyber stalking, spoofing etc.
\textsuperscript{16} Cybercrimes where computer is a target include sophisticated illegal activities such as unauthorised access to networks or computer systems, e-mail bombing, Trojan attacks, data diddling, denial of service attack, Internet time theft, logic bombs, virus or worm attacks.
\textsuperscript{17} Tenth U.N. Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.
1. Cybercrime in a narrow sense connotes a computer crime and includes any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

2. Cybercrime in a broader sense includes all computer related crimes and consists of any illegal behaviour 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.

In the Indian context, cybercrime may be defined as a voluntary and wilful act or omission that adversely affects a person or property or a person's computer systems and made punishable under the Information Technology Act, 2000 or liable to penal consequences under the Indian Penal Code.

It must be stated that cybercrimes may also involve conventional criminal activities like theft, fraud, forgery, mischief, defamation etc., all of which are subject to punishment under the Indian Penal Code. Besides, the abuse of computer, computer system or internet has given rise to a number of new crimes which were unknown prior to the emergence of computer technology, but are made punishable under the Information Technology Act, 2000. It would therefore, not be correct to say that the
crimes that are punishable under the I.T. Act alone are treated as 'cybercrime' insofar as the Indian Penal Code also covers many such crimes like e-mail spoofing, sending threatening e-mail, cyber defamation etc.\textsuperscript{18}

As to a precise definition of cybercrime, some, authorities hold that it is a misnomer because there is no recognised statutory definition of such crime. They argue that the concept of cybercrime is not radically different from that of a conventional crime because both include conduct whether act or omission, which causes breach of law and entail punishment.

The term cybercrime usually refers to a wide range of criminal activities which specifically relate to computers and telecommunication infra-structure that support their use. However, it is generally accepted that the term "cybercrime" encompasses within it any prohibited act committed through the use of, or against digital technology. It would therefore, be evident that the focus so far has been on functional definition of cybercrime rather than a universally acceptable legal definition of it.

\textsuperscript{18} Suri R.K. & Chhabra T.N : Cybercrime (Reprint, 2003) p. 45
**Scope of Cybercrime**

Presently, cybercrime is an ever increasing phenomenon, not only in India but all over the world. The incidence of this crime is directly proportional to the level of progress made by a country in computer technology. The report of the United Nations International Review of Criminal Policy on Prevention and Control of Computer Crime\(^\text{19}\) stated that more than 50 per cent of the websites in United States, Canada and European countries have experienced breach of security and threats of cyber terrorism which threw a serious challenge before the law enforcement agencies. A new trend that has developed in recent years is that the militants are going for terror training. The internet has become a key teaching-tool for militants who are using it to educate recruits in cyber terrorists' training camps.

Gabriel Weimann, an internet and security, expert who teaches in the University of Mainz in Germany and has studied militants use of websites for nearly a decade, while addressing the internet security personnel said that websites and chat rooms used by militant Islamic Groups like Al-Qaida are not only used for dissemination of propaganda, but also for terrorist education. He said, "Al-Qaida has launched a

\(^{19}\) U.N. Report on International Review of Criminal Policy and Prevention & Control of Computer Related Crime (October, 2005)
practical website that shows how to use weapons, how to carry out a kidnapping and how to use fertilizers to make a bomb.\textsuperscript{20}

The terrorist's attack on India's Parliament' on December 13, 2001, is yet another glaring instance indicating how computer networks are being misused for destructive activities by the anti-nationals. The Bureau of Police Research & Development (B.P.R. & D.), Hyderabad, on analysing and retrieving information from the laptop recovered from' the two terrorists who attacked Parliament, sent to the Computer Forensic Division experts of the B.P.R. & D. Delhi. It was the laptop which contained several evidences that confirmed the motives of the two terrorists, namely, the sticker of the Ministry of Home that they had made on the laptop and pasted on their Ambassador car to gain an entry into the Parliament House and the fake ID-card that one of them was carrying with the Government of India emblem and seal. The emblems of three lions were carefully scanned and the seal was craftily made alongwith the fake residential addresses of Jammu and Kashmir. The detective forensic investigation showed that they were all forged and scanned from the laptop of the accused.\textsuperscript{21}

\textsuperscript{20} Gabriel Weimann was addressing a Conference on Internet Security at the headquarters of Germany's Federal Police Office (BKA) (as reported in Times of India, Delhi edition, dated November 23, 2007)

\textsuperscript{21} One of the prime accused in the case Afzal has been sentenced to death by the Supreme Court and the President of India.
The computer related crime has already become an area of serious concern for most of the countries of the world, and India is no exception to it. The prime factor that has to be taken into consideration while deciding whether a particular computer related activity be reckoned as cybercrime is that a distinction must be drawn between what is unethical and what is illegal. It is only when an activity is truly illegal; it should be treated as crime and the prosecution of the offender must be sought. Therefore, criminal law should be implemented with restraint in determination of cases which relate to cyber law.22

In the absence of an internationally recognised definition of cybercrime or computer crime, there has been a great deal of debate amongst the legal experts on the term 'computer misuse' and 'computer abuse', which are frequently used in the context of cyber crime. However, the practice in vogue in this regard is to hold that the two terms have different implications. The criminal law applicable to cybercrime must make a distinction between incidental misuse of a computer system, negligent misuse and intentional access to or misuse of computer system and it is the later, which should be treated as a crime and not the former two. As a corollary of this distinction, it is the abuse of computer system which should be treated as criminal behaviour punishable under the law

and not the behaviour which causes annoyance or discomfort to the computer user

**Cyber Laws: A New Beginning**

Cyberspace is an emerging digital medium and requires a set of laws to regulate human behavior in the cyberspace. The body of such laws can be referred to as cyber laws. It is obligatory to note that the basic objective of cyber laws is to regulate human behavior and not technology. Cyber laws are technology intensive laws, advocating the use but not the misuse of technology. The idea is to articulate that the rule of law exists in cyberspace.23

Cyberspace requires cyber law. It would be a misnomer to suggest that cyber laws are meant to check the human behavior in cyberspace only. Any physical act; which gets translated into violation of any right of a person in digital medium (cyberspace), would be treated as cyberspace violations. Let us not forget that it is the technology platform and its application, which separates cyberspace from physical world. For example, A, a person with a criminal intent uses computer or computer network to defraud another person, B then in such a case A. could be

23 Vakul Sharma "Introduction to the Cyber World and Cyber Law ", pages no 6-19.
punished under cyber law provisions. It was his actions in the physical world, which got manifested in the cyberspace.

**Defining Cyber Law**

The word "cyber law" encompasses all the cases, statutes and constitutional provisions that affect persons and institutions who control the entry to cyberspace, provide access to cyberspace, create the hardware and software which enable people to access cyberspace or use their own devices to go 'online' and enter cyberspace.

If one examines the aforesaid definition, basic concept of cyber laws revolves around the phrase: 'access to cyberspace'. How one can access cyberspace? The requirement from the point of user is:

(a) A computer system with a modern facility, a telephone line and an Internet hours usage pack from a network service provider; or

(b) A computer system with a modem facility and a broadband connection from a network service provider.24

Without such basic hardware and software tools, one cannot access cyberspace. Public and private institutions in the form of Government(s), hardware manufacturers and software application providers act as a gatekeepers of cyberspace. Access is granted to those, who have got the

---

24 Id at 8.
necessary tools to access cyberspace. With a click of a mouse or punching keystrokes, gates of cyberspace are opened for the users'. It is just a 'click-of-a-mouse' that separates an individual from physical space to cyberspace. Any illegal, wrongful or dishonest act committed in cyberspace would be covered under the cyber law provisions. Let us take an example of a person, X. By click of a mouse, he moves to a website based in New York and purchases goods; again by a click of a mouse, he moves to a website based in Hong Kong and purchases goods; and once again by a click of a mouse, he moves to a website based in Paris. Suppose X has used a forged global credit card to make purchases in New York, Hong Kong and Paris. Did X commit an offence? Yes, he did, but this would fall under the category of 'cyber fraud', rather than a case of a physical fraud and X would be tried under the cyber criminal provisions.

In other words, the effectiveness of cyber law comes from the fact that it legally binds actions of any individual using computer, computer system or computer networks. In the above example, it was actions (of X), which were in the form of set of commands given to computer by means of a click of a mouse or a keystroke. Computer executed the command as given by X. From the legal perspective, it was a cyber fraud perpetuated by the X. The computer acted as it was under the control of X. Nevertheless, cyber law would extend its jurisdiction over both man
and machine (computer) and thus by implications it legally binds all individuals and machines accessing cyberspace.\(^{25}\)

**Building Blocks of Cyber Law**

Cyber law is a new branch of law and is growing very fast. It is imperative that one should know the three basic building blocks of cyber laws, namely:

(a) Netizens,
(b) Cyberspace,
(c) Technology;

(a) **Netizens**

Cyber law has introduced a very important concept of netizens. Who are they? Which country, they belong to? Are they recognized as citizens under the Constitution of their country? Do they have fundamental rights? Do they have fundamental duties, as well?

A Netizen is an inhabitant of the world wide web (Internet). He is the one; who inhabits the Net and uses it as an extension of his day-to-day physical world. He replicates his physical world actions, like socializing, buying, selling etc. in an online medium. He transcends geographical space and time by a click of a mouse. He recognizes no man-made or geographical boundaries. There is no end to what a netizen can do. The

\(^{25}\)Ibid.
most interesting facet of being netizen is that he could be anonymous, nameless and faceless person, if he wants to and yet can indulge in all kind activities.

A netizen differs from a citizen in the sense that a netizen unlike a citizen has no constitutional guarantees. No Constitution recognizes netizens as citizens and grant them constitutional rights and duties. Constitution of a country is meant or specific geographical area. It is meant or the people that reside within that geographical area. Netizens being the traveler of digital highways are basically nameless, faceless nomads crisscrossing the worldwide for convenience. But one should not forget that in cyberspace, netizens exist, citizens don't It is for these netizens, cyber laws have come in to existence.

(b) **Cyberspace**

Cyber law is for cyberspace. But cyber laws would not only regulate whatever being done in the cyberspace only. Since, it is difficult to separate out between the physical space and the cyberspace, it is only logical that cyberspace to include the activities, which have happened in the physical space just prior to entry into cyberspace.\(^\text{26}\)

\(^{26}\) Supra note 23 at 8.
Cyberspace is a key building block of cyber law. In fact, one of the most important facets of cyber law is to act, as a bridge between the physical space and the cyberspace, in order to regulate interface between man and machine. Cyberspace in that way is a manmade machine world reshaping itself periodically. The question is should it be regulated by physical set of laws already in existence or should be regulated by new set of laws? It is important to note that, the present of cyber laws are an extension of physical laws in cyberspace. These are 'analogy-seeking' laws. For example if law of contract exists between a buyer and seller in the physical world, then the same law of contract to be taken into account, if there is e-commerce involving a buyer and a seller in electronic market place.

Cyber space is connected to physical environment by what is technically known as partals, which allow people to see what is inside it. They may be one way such as television, two way such as telephone, or multi ways such as internet. Briefly stated cyberspace may be described as a conceptual colleguem where world's information resources come together without being seen or sensed.27

Interestingly, netizens are even purchasing virtual properties on the world wide web. For example, Second Life is a 3 D virtual world entirely created by its residents. Believe it or not, it is inhabited by millions of residents from around the globe! Even ebay.com conducts land auctions of parcels of land available on Second Life on regular basis.

(c) **Technology**

Cyber laws are technology intensive laws. They revolve around technology and its applications. Cyber laws establish norms of accepted human behavior in cyberspace.

Presently, there exists two-technology school of laws: one is called, Technology Specific School and the other one, Technology Neutral School. The debate is what sort of laws should be adopted and why? Technology Specific School argues that the law should recognize only one given set of technology or technology standard. That is, law treats other standards as illegal, non-binding and thus not permissible. The main advantage of this School is that it creates a single technology platform for the entire community. The main disadvantage of this School is that it kills technological innovations and helps in creating monopolistic business, which is bad for the community.
Technology Neutral School argues, that the law should remain neutral when it comes to giving due recognition to any technology or technology standards. It treats all technologies or technology standards at par. Law does not discriminate between the technologies. The main advantage of this School is that helps in providing efficient and useful technologies for the community.

The main disadvantage of this School is that it creates a multiple technology platforms and may increase the cost of assimilation of technology for the entire community.\(^{28}\)

It is important to note that both technology specific law and technology neutral laws may co-exist at any given point of time. Often it is seen that the developed countries with a wider technology users' base have multiplicity of technology platforms, whereas the developing countries with a narrow technology users' base have one common technology platform to begin with.\(^{29}\) The reason is that in a developing country, technology is at a premium and hence the users are few, whereas in a developed country there are large numbers of users and there is technology maturity and hence are multiplicity of technology platforms. For example, technology specific law grants legal validity to digital signature created using a specific technology only. Digital signatures

\(^{28}\) Ibid.

\(^{29}\) Supra note 23 at 9.
created using any other technology not prescribed under law would be considered as invalid. A technology neutral law regime would not impose any such restrictions. Digital signatures or (Electronic Signatures) created by any technology would welcome.

In India, we follow a technology specific regime. Under the law (The Information Technology Act, 2000), digital signatures using prescribed asymmetric cryptosystem standard is considered legally valid. Use of any other standards would render the said digital signature invalid. When this Act came into existence, the technology usage was quite low, but with the passage of time in India technology maturity has increased and that's why in the new Information Technology (Amendment) Bill, 2006 advocate's migration towards the technology neutral regime.

**Jurisprudence of Indian Cyber Law**

The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore). Minor errors in the Act were rectified by
the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002. An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act in regard to protected systems and application for the issue of a Digital Signature Certificate.\(^{30}\)

The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques.

Information Technology (Use of Electronic Record and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies.

On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and

\(^{30}\) Rohas Nagpal “7 years of Indian Cyber Law” (e-Book). Page no. 3-5.
security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.

**Information Technology (Certifying Authority)**

Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA.

Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001.

Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002.

The Cyber Regulations Appellate Tribunal (Procedure) Rules. 2000 also came into force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of
the Adjudicating Officers The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications and experience of Adjudicating Officers, whose chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.\(^{31}\)

The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws (ASCL). The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the

---

\(^{31}\) Supra Note 30 at 4.
IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers. The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of 'adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this the Central Government passed an order dated 23rd March 2003 appointing the "Secretary of Department of Information Technology of each of the States or of Union Territories" of India as the adjudicating officers.'

The Information Technology (Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003.

An important order relating to blocking of websites was passed on 27th February, 2003. Computer Emergency Response Team (CERT-
The Indian Penal Code (as amended by the IT Act) penalizes several cybercrimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act). In case of bank records, the provisions of the Banker's Book Evidence Act as amended by the IT Act are relevant. Investigation and adjudication of cybercrimes is done in accordance with the provisions of the code of criminal Procedure and the IT Act. The Reserve Bank of India Act was also amended by the IT Act.\textsuperscript{32}

**Cybercrime : Evolution or Neo-Criminology**

The advancement in computer technology and internet has brought in its wake a new variety of crimes and provided ever-increasing opportunities for the criminals to indulge in illegal activities unabated, and computer crimes are no exception to it. The last quarter of the twentieth century witnessed several sophisticated ways through which the perpetrators of cybercrime found it easy to penetrate into the systems of software and internet to commit cybercrimes, which may be characterised

\textsuperscript{32} Supra Note 30 at p.5
as the new specie of white collar crime. These crimes have global ramifications sabotaging the national economy and business ventures. They are not restricted to any geographical area or territory and may be committed within a fraction of a second affecting victim(s) who may be thousands of miles away. The peculiar feature of these neo-crimes is that while perpetrator knows what he is doing, the victim may remain completely unaware or ignorant throughout without knowing that he has been victimised by the unknown perpetrator of the crime. It therefore follows that these new variety of crime have thrown a big challenge before the law enforcement agencies and they are required to evolve a neo-criminological approach to handle these internet crimes.

The challenges posed by the computer related neo-crimes are immense. They cannot be efficiently tackled by the traditional procedures adopted the police and other enforcement agencies but need an altogether new strategy based on modern tools and techniques.

Yet another issue that needs re-consideration in the context of cybercrime is that the conventional concept of *mens rea* which has been an essential ingredient for a crime is hardly applicable to offences like hacking, e-mail bombing, spoofing etc. when they are committed by teenagers who are generally minors. As a matter of fact, the cybercrimes
which these teenagers commit are so harmful to the society that the
damage caused by them is irreparable, yet they remain out of purview of
the criminal law jurisdiction because of their minor age. These issues
therefore, need a neo-criminological approach for combating cyber
criminality which is expanding its tentacles with new developments in
information technology and computer science.

**Cyber Law-a separate discipline**

Cyber law may be defined as the law governing cyberspace which
is a non-physical terrain created when two or more computers are
networked together. Online systems create a cyberspace\(^33\) within which
computer users can communicate with one another. Considered from this
point of view the term cyber law refers to law relating to computer,
computer networks and includes all ' activities that take place in relation
to information stored, exchanged or retrieved using the computer
system.\(^34\)

Ever increasing use of computers and internet have provided
enormous scope for the computer abusers to carry on their illegal
activities for personal gain, avenge rivalry or for political or commercial
purposes and innocent persons , become potential victims of their

---

\(^33\) Cyberspace is not restricted to internet alone, but in its wider sense, it includes computers, computer
networks, software data etc.

criminal acts. Therefore, a separate law to prevent and control cyber criminality was the need of the time. Reacting sharply against cybercrime and criminals, many countries have enacted cyber laws that specifically deal with cybercrimes, while others have made these crimes as punishable offences under their existing penal statutes.

It hardly needs to be reiterated that cyberspace recognises no territorial boundaries therefore, a person skilled in computer operations in India can easily dupe a person having bank account in U.S.A. by transferring millions of rupees in another bank in England within no time, with the help of his laptop and a cell phone.35

Again, extremely fast mobility and anonymity in cyberspace further facilitates the cyber criminals to remain unidentified and untraceable for the offence committed through computer networks.36 The violation of rights to intellectual property and right to privacy are other vulnerable areas where cyber criminals usually operate, which requires special cyber laws to deal with and apprehend these criminals.

36 Ibid.
Cyber Law in India

There was no separate and independent cyber law in India prior to the enactment of the Information Technology Act\textsuperscript{37} 2000 and all the computer related crimes were tried under the traditional law of crimes i.e. the Indian Penal Code, 1860. However, the information technology advanced by computer networks started having its impact on every aspect of society and governance in the new millennium. With the increased dependence on e-commerce and e-governance, a variety of legal issues related to use of computers and internet or digital processing devices such as violation of IPR's, piracy, freedom of expression, jurisdiction etc. emerged which could not be redressed by the existing laws because the cyberspace has no geographical limitations nor does it have any physical characteristics such as sex, age etc. This posed practical problems, before the law enforcement agencies in regulating cyberspace transactions of citizens within the country as also the countries abroad. Though in practical terms an internet user is subject to the laws of the State within which he/she operates, but this general rule runs into conflict where the disputes are transnational in nature.

It is true that at the time when computer technology was in its developing stage, no one ever contemplated that it can be discretely

\textsuperscript{37}The’ Information Technology Act, 2000 received the accent of the President of India on June 9, 2000 and came into force w.e.f. October 17, 2000, it consists of 94 Sections in 13 Chapters and four Schedules.
misused by internet users for criminal purposes but experience has shown that the world of internet too has a dark side as it gives rise to new variety of crimes called the cybercrime. It is in this backdrop that Information Technology Act was enacted by Indian Parliament. The objectives of the Act as contained in the statement of the objects as follows:

"An Act 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 commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate, electronic filing of documents with Government., agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

A plain reading of the statement of objects of the Act would reveal that the Information Technology Act was primarily introduced to facilitate and promote e-commerce,\(^38\) which had gained momentum due to the switchover from traditional paper-based methods of information.

\(^38\) E-commerce refers to transactions out by means of electronic data interchange and other means of electronic communication which involve the use of alternative to paper-based methods of communication and storage of information.
communication system to that of computer networks. The Preamble of the Act sought to:

1. provide legal recognition for e-commerce;
2. facilitate e-filing of documents with the Government agencies;
3. amend the Indian Penal Code; 1860, Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act 1934\(^{39}\) and:
4. ensure efficient delivery of government services by means of reliable electronic records.\(^{40}\)

The Act thus provides for a legal framework so that legal sanctity is accorded to all the electronic records and other activities carried out by electronic means.

It must be stated that the Information Technology Act\(^{41}\) 2000 enacted by the Parliament is essentially based on the Model Law on e-commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) to which India is a signatory member. The working of the Act in subsequent years brought to light certain lacunae and shortcomings inherent therein which obstructed its smooth operation.

\(^{39}\) Infra Chapter VII.
\(^{40}\) Consequent to the passing of the Information Technology Act, 2000, the Government of India framed rules under the Act for regulating the application and providing guidelines for certifying authorities.
\(^{41}\) The rules made under the Act were called the Information Technology (Certifying Authorities) Rules, 2000 which came into force on October 17, 2000. Another set of rules called the Cyber Regulation Appellate Tribunal (Procedure) Rules, 2000 were also enforced on the same date.
and therefore, it was amended in 2002 and again proposed to be amended by the Information Technology (Amendment) Bill, 2006 which was cleared by the Parliament on December 24, 2008 and received the assent of the President of India on February 5, 2009 to be enforced as the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009). The Amendment Act seeks to plug the loopholes in the existing Information Technology law so as to make it more effective.

**Global Concern for a Uniform Cyber Law**

Despite sincere efforts on the part of United Nations to bring out a comprehensive cyber legislation which could be uniformly applicable to all the countries for the prevention and control of cybercrimes, the response of member States has not been very encouraging as there is no unanimity of opinion as regards concern for control and minimisation of these crimes. The obvious reasons for this variation in approach towards cyberspace crime are the difference in the organisational set up of various legal regimes. Although there have been a number of International conventions and treaties to work out a common legal strategy for the prevention of borderless cyber criminality, but these efforts have not succeeded for want of desired co-operation and initiative from the member nations.
Further, there being no uniformity as to the concern and sensitivity of countries to cybercrimes due to variation in their socio-economic and cultural conditions, the countries which are not much affected by these crimes are bound to react differently than those which are seriously affected by them. Under the circumstances, it is futile to expect a uniform approach of all the countries towards prevention and control of cybercrime. Perhaps, this is the main reason for lack of active cooperation on the part of different countries to support a global cyber legislation which could be uniformly applicable to all the countries' of the world. Though a cyber law on a global scale is yet to evolve, the urgency of such a law is being increasingly felt by countries all over the world due to the growth of internet which provides innumerable opportunities for criminals to engage in a variety of criminal activities which have transnational or international repercussions.