How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .

CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE

Dr. Ravinder Kumar
Assistant Professor, School of Law
NIILM University, Kaithal, Haryana
ravigrowkkr@gmail.com

Abstract

New communication systems and digital technology have made dramatic changes concerning the style of living of a person. A revolution is noticed in the mode of transacting business. Businesses and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in the electronic form has many advantages. It is cheaper, easier to store, retrieve and above all speedier to communicate. Even though the people are aware of these advantages even then they are reluctant to conduct business or conclude any transaction in the electronic form due to a lack of an appropriate legal framework. The two principal obstacles that stand in the process of facilitating electronic commerce and electronic governance are the requirements of writing and the signature for legal recognition. At present many legal provisions assume the existence of paper-based records and documents and records which should in reality at present bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony since electronic commerce eliminates the need for paper-based transactions, hence many countries have switched over from traditional paper-based commerce to e-commerce.[1]

Keywords:- Cybercrime, Computer, Problem, Information, Business, Internet, Law, Cyber Crime Denial of Services (DoS) Defacement of Web-sites, Spam, Computer, Virus and Worms Pornography, Cyber Squatting, Cyber Stalking, Phishing, Revolution, Generations, ARPANET.

Introduction:

In this era of Internet and Information Technology, the rapid development of information and communication technology over the past decade have brought about a change in the mode in which information is communicated and has thus revolutionized business practices. In other words Indians achievement in then IT section is remarkable and really a matter of pride but the associated problems that is causing serious concern is the rapid raise in cyber crimes with increased use of computers and internet in homes and offices, there has been a proliferation of cyber crimes in India. Cyber Crime which is 'Internet Crimes' or 'Computer Crimes' is any criminal activity that uses a computer either as an instrument target or a means for perpetuating further crimes on offences or contraventions under any law. These offences involved not only the use of the computers but the internet, cyberspace and the tools and techniques of WWW (World Wide Web) as well. While the world wide scenario or cyber crimes looks bleak the situation in India is also not better. Major Cyber Crimes reported in India are Denial of Services, Defacement of Web-sites, Spam, and Computer Virus and Worms, Pornography, Cyber Squatting, Cyber Stalking and Phishing. Especially, cases of Spam, Hacking, Cyber Stalking and E-mail Fraud are rampant in India. In the first half of 2006 itself around 1000 Indian websites were attacked.[2]

[1] . Nitant P. Trilokekar, "A practical Guide to Information Technology Act, 2000" at.303

[2] G. Rathinasabapathy and L. Rjendran; Madras Veterinary College Library, Vepery, Channai-600007, TN

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .

The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life. There is a great talk about the cyber crimes nowadays.

The crimes such as frauds, forgery are traditional and the abuse of computer and the related electronic media has given birth to gamut of new types of crimes generally known as Cyber-Crime which has some peculiar features.

Cyber Crimes which are known as 'Computer Crimes', 'Internet Crimes' can be defined, "any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes or offences or contraventions under any law".
The Cambridge Dictionary defines Cyber Crimes as "Crimes committed with the use of computers or relating to computers, especially through the internet."

These offences involve not only the use of computers but the internet, cyberspace and the tools and techniques of World Wide Web as well. A simple definition of these crimes would be "unlawful acts wherein the equipment transforming the information be it a computer or a mobile is either a tool or a target or both."

Joseph Marie Jacquard, who devised a loom which was capable of doing repetition of a series of steps in weaving of special fabrics, was discouraged by his own employees by acts of sabotage as they were feared that their traditional employment and livelihood were threatened by his device. This incident is treated as the ever first Cyber Crime in the history which has taken place in 1820.

The global reach of the internet, the law marginal cost of online activity, and the relative anonymity of users have changed the balance of forces that have previously served to keep in check certain undesirable behaviors in the physical world. These characteristics of cyberspace have lowered the cost of perpetrating undesirable behavior by eliminating certain barriers to entry, lowering transaction costs, and reducing the probability of getting caught. It is very important to understand the development of computers, internet and cyber laws. According to NCRB, which released the statistics late on Monday, "During 2017, 56.0% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by sexual exploitation with 6.7% (1,460 cases) and causing disrepute with 4.6% (1,002 cases)[3]

OBJECT AND PURPOSE OF THE STUDY

This study is basically intended to deal with a novel area of knowledge which is still at a developing stage due to these reasons it becomes in imperative to take into account the historical background of the subject. In developed countries like USA, UK and France, the position in this regard has been taken into account in detail with more emphasis on the process of growth and development of the law on the subject. The position has also been examined of these issues on the developing countries and a separate chapter has been in operated in this study in order to have in depth the study of the subject in the wider prospective. The existing law and the real practice have been dealt with together so as to identify the contradiction and deficiencies involved which forms the basis of this study and in the conclusion part of this study it has been intended to bring out consistency and uniformity on the basis of conclusion and suggestions with in this research work. It will not be out of context to say that on the basis of this study other researchers could do research further so that utility of this subject could be to the maximum possible extent with well defined diminutions so as to ensure the best possible outcome of this research work.

HISTORICAL BACKGROUND AND DEVELOPMENT OF COMPUTERS

"A computer is a machine that handles data. Data are facts that gathered and entered into the computer. The computer stores, retrieves, sends, receive analysis and synthesize the data to produce information. Information is any collection of words, numbers and symbols,

[3] https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202017%20-%20Volume%201_0_0.pdf

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

organized so that it is meaningful to the person using it".[4]

The Industrial Revolution changed human society on a massive scale. To live in the rapidly changing period between 1890 and 1920, for instance, was to live with the dizzying introduction of electricity, telephones, radio, automobiles and airplanes. Like the Industrial Revolution, the Computer Revolution is bringing dramatic shifts in the way we live, perhaps even in the way we think. This revolution, however, is happening a great deal more quickly then the Industrial Revolution. The computer revolution is unfinished; it will probably roll on into the next century.

In the USA in 1946 it was developed by the team of an experts led by Prof. Eckert and Mouchly at University of Pennsylvania. Taking pioneering machines such as ENIAC as representing the first generation of computer technology, early estimates as the market forte computer now appear ludicrously low. One pioneer has suggested in this regard that a single machine would satisfy the computing need of the U.K. whilst the chairman of 1BM considered that there might be world market for five machines.

Over the past six decades, the computer revolution has grown to change the way people work and to effect many aspects of their every day lives. The development of new types of computer hardware and software has contributed to the spread of computer applications. Gaining computer literacy has become to priority of students. Organizations of all sizes are putting the computers to work. It seems like every body is using the computers. People in all walks of life need to know about computers if they are to function efficiently in information.

COMPUTER GENERATIONS

There is no clear-cut pattern of development after EDSAC emerged. The history is tied up in a tangle of technological advances, University research and company amalgamations. In order to simplify matters and at the same time provide a framework for the growth of the computer industry, we shall look at the so called 'generations' of computers. The custom of referring to the computer era in terms of generations came into wide use after 1964.

(i). 1st Generation Computer (1951-1958) (ii). 2nd Generation Computers (1959-1964)
(iv). Fourth Generation Computers. (1971-Present) (iii). 3rd Generation Computers (1965-1971)
(v). Generation less Computers (vi). Future Computers

HISTORICAL BACKGROUND AND DEVELOPMENT OF INTERNET

These days the internet seems to be everywhere web addresses appear on television ads and billboards. There are T.V. shows and magazines devoted to the internet. And every new computer program that comes out has some internet features. The next thing, your computer desktop will connect you just as easily to internet resources as it does to the files on your hard drive.[5]

So, we first to know what is Internet? From where it was started? The Internet (Interconnected Networks) is a term that refers to thousands of interconnected logical networks linking millions of computers world wide. It is a global information system formed by combining smaller network to create a single larger network. It is international network of network. The internet refers to logical connection blow the computers and not physical connection. It came into being in late seventies and early eighties with the development of TCP/IP.

The history of the internet dates back to the 1960s. The Advanced Research Projects Agency of United States Department of Defense developed a network of computers called ARPANET. This network connected only Military and Government computer systems. Its

[4]. Basandra, S.K. "Computers Today" at 1-2
[5]. The ABCs of the internet 2nd Edition, Christian Crumlish BPB Publications, New Delhi-110001.

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .
purpose was to make these systems secure in the event of a disaster war. Soon after the creation of ARPA NET, Universities and other institutions developed their own computer networks. In due course of time, these networks were eventually merged with ARPA NET to form the internet. By the early 90's, anyone with a computer, modem and internet software was able to link up with the internet. Now, the internet connects a hundred thousand networks the entire world over.

CRIMES IN CYBERSPACE-MEANING OF CYBER CRIMES

With new mediums of communication, business and societal activities, growth of newer and varied kinds of crime is inevitable. Computers with the aid of internet have today become the most dominant medium of communication, information, commerce and entertainment. The internet, with all the benefits of anonymity, reliability and convenience has become an appropriate breeding place for persons interested in making use of the net for illegal gainful purposes, either monetary or otherwise.

Since anything related to the internet was being prefixed with the word 'Cyber', the most appropriate term to reflect the new criminal phenomenon was Cyber-Crimes. Cyber: A prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. Anything related to the internet also falls under the cyber category.[6]

The definition of a crime has always been regarded as a matter of involving complicated process. Here we can give some definition of cyber crime or computer crime, to understand the topic. Some of the commonly spelt out definitions of computer crime are:

"Any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of computer."

"Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data."[7]

The states and Federal Government have defined "Cyber Crime activities to include the destruction or theft of computer data and programs to be computer crime."

The Cambridge dictionary defines Cyber Crimes as "Crimes committed with the use of computers or relating computers, especially through the internet."[8]

A generalized definition of Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both."[9]

GROWTH AND DEVELOPMENT OF CRIMES IN CYBERSPACE

The internet has brought about several advantages and utilities which one would not have even dreamt of a couple of years ago. It has provided opportunity for education, business, scientific research, entertainment and much more. Persons from far off countries and continents are linked to each other as if they are next door neighbors and are able to exchange information and views within seconds, living aside all geographical and time zone barriers.

The global reach of the internet, the low marginal cost of online activity, and the relative anonymity of users have changed the balance of forces that have previously served to keep in cheek certain undesirable behaviors in the physical world. These characteristics of cyber space have lowered the cost of perpetrating undesirable behavior by eliminating certain barriers to entry, lowering transaction costs, and reducing the probability of getting caught.

Since the internet's strength and purpose is facilitation of communication traditional crimes such as conspiracy, solicitation, securities fraud and even espionage can be committed via the internet.

---

[6]. http://www.pcwebopedia.com/TERM/C/Cyber.html (last visited on 16.02.2004).
[7]. Suresh T.Vishvanathan, 'The Indian Cyber Law'. at.81
[8]. The CAMBRIDGE DICTIONARY.
[9]. Nag Pal R-What is cyber crime?

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

In fact, as internet grows develops and opens up to more people, we could be seeing many types of other crimes. The inability to trace the identity of the users of the internet is one of the characteristics of the internet, which makes it susceptible to crimes. Also the wide variety of information that can be transferred, the open unregulated nature of the internet. The irrelevance of geography means that the internet provides fertile ground for criminal enterprises.[10] *A laptop was used to down load the logo of the Ministry of Home Affairs from ministry's website and was pasted on the car in case of Parliament Attack.*[11] In the latest scenario in the terrorists threatens the Indian Government by email to attack on some most important places in India?[12]

2. CLASSIFICATION OF CYBER CRIMES

Cyber Crimes have set in a debate as to whether a new legislation is indeed to deal with them or existing legal regime is flexible enough to effectively deal with this new form of criminality. There is school of thought that believes that cyber crimes are not in any way dissimilar to the ordinary crimes like trespass, larceny or conspiracy with a difference that a computer has been used as a medium or instrument for commission of crime.[13]

FOUR MAJOR CYBER CRIMES

(A). Against Individuals

(i). E-Mail Spoofing (ii). Spamming-
(iii). Cyber Defamation (iv). Harassment and Cyber stalking-

(B). Against Property-

(i). Credit Card Fraud (ii). Intellectual Property crimes
(a). Software Piracy (b). Copyright infringement
(c). Trademarks violations (d). Theft of computer source code
(iii). Internet time theft

(C). Against Organization

(i). Unauthorized Accessing of Computer-
(a). Changing/Deleting Data (b). Computer Voyeur
(ii). Denial of Service (iii). Virus Attack (iv). E-mail Bombing
(v). Salami Attack (vi). Logic Bomb (vii). Trojan Horse
(viii). Data diddling

(D). Against Society-

(i). Forgery (ii). Cyber Terrorism (iii). Web Jacking

3. LEGAL DIMENSIONS OF INFORMATION SECURITY

Legal dimensions of information Security in India

Following are the parameters of information security in context to the Information Technology Act, 2000.

The status of 'secure' for the electronic record is important to admit the record as evidence. Thus, every record that is electronic or stored on the computer or any magnetic media is not 'secure'. Records that are capable of manipulation either by the owner/originator or by any other person will not qualify for the adjective of 'secure'. Thus financial accounting package showing the ledger account in a case where date of entry is important, will not qualify as a secure electronic record if the package permits back date entries. In contrast, the banking system which are date sensitive not permitting back dated entries without an audit trial have a better status of security but under this Act, the application of digital signature is further requirement.

---

10. "Internet Crimes, Effectiveness of the Laws in Force." SCJ. Vol-I, p. 41.
11. "Learn About 'Cyber Law'. The Tribune, Jan 7, 2002
12. "Tight Security in Chennai" E-mail Thread. The Tribune, Nov 25, 2007.
13. Watkins, Computer Crimes : Separating the myth From Reality, C.A. Magazine, Jan.1981

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .

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:-

(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 his linked to the electronic record to which it relates in such a manner that if the electronic was altered the digital signature would be invalidated then such digital signature shall be deemed to be a secure digital signature.

The digital signature is defined to be super only when it has the essential features of a digital signature i.e. unique to the subscriber, capable of being associated (identified) with the subscriber linked to the electronic record in such a manner that any alteration will be detected. In the Information Technology Act, 2000 the law makes such features mandatory to permit the digital signature declared as 'secure' and thus recognized by law.

The Central Government shall for the purpose of Information Technology Act, 2000 prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including

(a) the nature of transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transaction engaged in by other parties;
(d) the availability of alternatives offer to but rejected by any party;
(e) the cost of alternative procedure; and
(f) the procedures in general use for similar types of transaction or communications.

The Information Technology Act, 2000 gives authority to the Central Government to prescribe security procedure to transactions they alternatives etc. At the time of passage of Information Technology Act a detailed information technology security procedure and guidelines were issued along with the rules. These detailed requirements are critical for allotment of license to the certifying authority as well as renewal of license.

Legal dimensions of information Security in World

It has become essential now a day for the data users to protect the data. Although technical methods are available but legal development and evolution of laws relating to data protection or Information Security is developing with the pace of technical methods. So many Acts like UK Data Protection Act, 1998, Principal of Data Protection, Freedom of Information and Protection of Privacy Act, 1996 and Children Online Privacy Protection Act, 1998 are the few Acts which have taken birth by the legislators in the world a comparative study done by researcher on few of such laws are as follows-

(a) UK Data Protection Act, 1998

In United Kingdom the Data Protection Act, 1998 applies to almost all data users who control the contents and use of personal data from or within the UK. As regards residence in UK the Registrar of Data Protection has pointed that a company could be considered as 'resident' in UK for the purpose of Income Tax. In any case it may be represented (in UK) by a servant or agent who will be required as a data users.

The Rules provide that anyone processing personal data must comply with the eight enforceable principles of good practice. The data must be-

(i) fairly and lawfully processed;
(ii) processed for limited purpose;
(iii) adequate, relevant and not excessive;
(iv) accurate;
(v) not kept longer then necessary;
(vi) processed in accordance with the data subject's rights;
(vii) secure;
(viii) not transferred to countries without adequate protection.[14]

[14] Section 4 UK Data Protection Act, 1995

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .

(b) United Nation Guidelines in relation to Data Protection

The UN has also issued guidelines on the subject which is discussed here under-

(i) Principle of lawfulness and fairness
(ii) Principles of accuracy
(iii) Principles of the purposes-Specification
(iv) Principle of Interested Person Access
(v) Principle of Non Discrimination
(vi) Power to make exceptions
(vii)Principle of security
(viii) Supervision and Sanctions
(ix) Transponder Data Flows
(x) Field of Application[15]

(c) European Directive on Data Protection

The European Data base directive was issued in March, 1996. It is stipulated to be implemented by Legislation in member states with effect from Jan. 1, 1998. this process is in the course of completion in all members countries. The main objectives of the directive are-

(i) to provide grater protection of data basis, seen to be insufficiently protected throughout the European Union, and
(ii) to harmonize the law on database protection throughout the member countries, to insure the proper functioning of the market and to ensure that harmonized intellectual property law does not prevent the free moment of goods and services with the community. To protection or rights are stipulated-

-copyright protection, and
-sui generies protection[16]

(d) American Initiatives on Information Security[17]

In May 1996 prior to the December 1996 WIPO Diplomatic Conference, Congressman Moorhead introduced on Congress a Bill to protect database. In October 1997 after the various international meetings of experts since December 1996 Diplomatic[18] Conference, Congressman Coble introduced a further Bill.

4. STATUTORY PROVISIONS ON CYBER CRIMES AND RELATING LAWS

In India, the internet was launched in the 49th year of independence. Since then, there has been no looking back. Widespread use of computer and internet in business, administration, education, information and interpersonal relations, there are need for regulating it. Though India has a written Constitution and a comprehensive written legal system, the existing laws in India were not amenable to interpretation in the light of the emerging cyberspace as all of them were related to the political , social , economic and cultural scenario of the pre cyberspace. Moreover, the concern for legal validation of e-commerce and e-governance demanded the cyber laws be enacted. This gives the birth to the **Indian Information Act, 2000.**

4.1 INFORMATION TECHNOLOGY ACT 21 OF 2000

The Information Technology Bill was passed by the both the Houses of Parliament, and it received the assent of the President on 9th June, 2000 and became the I**nformation Technology Act, 2000 (21 of 2000)**.

Here, the relevant provisions from the **Information Technology Act, 2000** relating to the study. The provisions in the Act are under given in which are direct related to the Cyber Crimes in which the main definitions and other provisions of authentication of electronic records, digital signature and security procedures in the transactions in the form of e-commerce, etc.

[15] Suri R.K. & Bakshi P.M. Bharat's Cyber and E-Commerce Laws' at 64-65
[16] Article 7, European Data Base Directive Issued in March, 1996
[17] Bill H.R. 3531 (104th Congress) May 23, 1996 (Moorhead)
[18] Bill H.R. 2652 (105th Congress) Oct. 9,1997 (Coble)

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .

4.2 INDIAN PENAL CODE (45 OF 1860) (RELEVANT PROVISIONS) As Amended by the INFORMATION TECHNOLOGY ACT, 2000

Section 91 of the Act provides that the **Indian Penal Code, 1860** shall be amended in the manner specified in the First Schedule.

Indian Penal Code- Amendment, nature-

The **Indian Penal Code** deals with law of crimes which deals with offences, *inter-alia* relating to the documents writings and handwritten signatures are the two more important ingredients of the paper document. The manner of writing signing in an electronic communication is quite different. What purpose a paper document serves in a paper based communication, the electronic record in an electronic communication.

4.3 INDIAN EVIDENCE ACT, 1872 (RELEVANT PROVISIONS) As Amended by the INFORMATION TECHNOLOGY ACT, 2000

4.4. THE RESERVE BANK OF INDIA ACT, 1934 Relevant Provisions As amended by the INFORMATION TECHNOLOGY ACT, 2000.

Section 94 of the Act provides that the **RBI Act, 1934** shall be amended in the manner specified in the Fourth Schedule.

RBI Act, 1934 Amendment and Nature

RBI Act, 1934 has been amended to facilitate electronic fund transfers between the financial institutions and the Banks. A new clause (pp)[19] has been inserted in section 58(2) regarding the regulation of fund transfer through electronic means between the banks or between the and other financial institutions including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfer and the rights and obligations of the participants in such fund transfer.

The Act seeks to put in place a system of checks and balances to regulate the Net and to secure its use by individuals and organizations. The Act has provisions that embrace the laws of cyber contracts, cyber crimes, virtual properties, and laws on intellectual property rights in cyber space and netizens' rights. For the first time in the history of Indian law, electric documents, wills, trust deeds, power of attorney and any contract relating to conveyance of immovable property still remain legally unrecognized.

ANALYSIS OF THE STATUTORY PROVISONS

Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

FUTURE PLANS

The government is also planning to set up a centralized mechanism at the eight landing stations for the country to block websites as and when it pleases.[20] Indian law enforcement has entered an agreement with the popular social networking site Orkut to track down what it deems to be "defamatory content".[21]

On November 1, 2007, The Economic Times reported that the Government of India was considering a ban on "posting of private and personal videos on internet and mobiles" to tackle cyber crime and piracy.

The **IT Act** has a limited scope. It does not cover all the issues, which have cropped up by the introduction of Internet. While going through various provisions of the **IT Act**, it appears that many provisions lack harmony and it is quit possible that practical difficulties in applying these provisions will ensue in the future. The machinery to prevent cyber crimes is

[19] Inserted by the Information Technology Act, 2000

[20] Cyberporn Penal Set Up, HC wants Minors Protected, Sunil Thacker invited as a special invitee (Times of India, Sep.30 2001)

[21]. Rude encounters with Internet censorship; The Hoot on the blocking of Yahoo! Groups in 2003.

Corresponding author **Dr. Ravinder Kumar**

Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

not well equipped The Cyber Appellate Tribunal is a one-man commission, having law degree an essential qualification. Whereas Information Technology involves highly complex technical issues beyond the comprehension of an ordinary person who does not possess understanding of this technology.

5. CYBER CRIMES AND JUDICIAL ACTIVISM

5.1. Various Kinds of Crimes and Judicial Activism

The effectiveness of a judicial system rests on a bedrock of regulations- regulations which define every aspect of a system's functioning- and principally, its jurisdiction. A court must have [22] jurisdiction, venue[23], and appropriate services of process in order to hear a case and render an effective judgment. Jurisdiction is the power of the court to hear and determine a case. Without jurisdiction, a court's judgment is ineffective and impotent. Such jurisdiction is essentially of two types, namely subject matter jurisdiction and personal jurisdiction, and these two must be conjunctively satisfied for a judgment to take effect. Here in this chapter we will discuss the main Cyber Crimes and judicial activism. How the judiciaries interpret the Cyber Crimes?

5.2. COMPUTER VIRUSES AND JUDICIAL ACTIVISM

Sending viruses that destroy computer is a mischief. In India computer viruses and worms may just be the modern plague that afflicts the upcoming millennium. People are sending viruses as main attachments or download from sites that destroy the computers.

Though the **Information Technology Act, 2000** does not refer to mischief directly, section 65 of the Act penalize for "tempering with computer source codes as the listing of programs, computer commands, design layout and program analysis of computer recourse in any form" This is more appropriate as it provides a punishment (maximum imprisonment up to 3 years or maximum fine unto Rs. two lac) which is commensurate to the crime. However, due to its limited application, its limited application, the prosecution shall have to rely on section 425 of the **Indian Penal Code.**

In USA the most likely avenue of prosecution is the **Federal Computer Abuse Act of 1994** amending the earlier 1986 **Computer Fraud and Abuse Act**. The new Act outlaws the transmission of a program, information, code or command that causes damage to a computer, computer system, network, information data or program[24]. In Scotland, where most offences remain rooted in the Common Law, the offence of malicious mischief was held applicable in a case where conduct presented the profitable exploitation of property (in this case a nuclear power State) even though no physical damage was caused.

In England, the cases of **Cox *v.* Riley** and **R. *v.* Whiteley** provided authority fro application of the **Criminal Damage Act, 1971** two forms of computer related conduct. This Statute provides that

"A person who without lawful excuse destroy or damage any property belonging to another, intending to destroy or damage any such property.....shall be guilty of an offence."

5.3 HACKING AND JUDICIAL ACTIVISM

Initially hacking began as something cyber prank. It was considered witty among young software professionals to break into other people's computer and leave funny massages. But as the Internet gained the popularity and huge monetary transactions started taking place on-line. Some hackers realized that there was money to be made. Cyber criminal started breaking into computer system of banks and siphoning off money, while other stole credit cards details and fraudulently used this information to make quick buck.

[22] Christian M. Rieder, "U.S. Subject Matter Jurisdiction for Copyright Infringements on the Internet".
[23] See, Black's Law Dictionary 653 (pocket ed. 19996)
[24] U.S. Computer Fraud And Abuse Act, 1994, Section 1030(a)5(A)

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

However, there may be situations which may limit the effectiveness of the legislation. In the case of **DDP *v.* Bignell**, a police officer obtained access to data held on the police national computer in order to identify the owner of motor vehicle. The information was sought for owner's personal interest and was not connected with his duties as a police officer.

5.4 CYBERFRAUD AND JUDICIAL ACTIVISM

The word "fraud" has not been defined in the **Indian Penal Code**. However, Section 25 of Indian Penal Code defines the word 'fraudulently' by saying that there can be no fraud unless there is an intention to defraud. The word 'fraud' is clearly defined in section 16 of the **Indian Contract Act, 1872**. However, the definition can not be made applicable to criminal law. The Indian Courts have defined fraud as an act of deliberately deception with design of screwing something by taking unfair advantage of another. In general fraud is used in three different ways viz.

(a). to deprive a man of his right, either by obtaining something by deception or by taking something wrongfully without the knowledge of the owner;

(b). to withhold wrongfully from another what is due to humor to wrongfully present one from obtaining what he may justly claim; and

(c). to defeat or frustrate wrongfully another's right to property.[25]

It is deception in order to gain from another's loss. It is cheating if intended to get an advantage

As a response of failure of the prosecution in **R *v.* Gold**, the legislature enacted the **Computer Misuse Act, 1990.** According to which unauthorized access to a computer is offence. However, conduct must be aggravated by other acts such as the removal of property; otherwise no criminal offence will be committed.[26]

5.5. DIGITAL SIGNATURE AND FORGERY AND JUDICIAL ACTIVISM

In **Ajay Aggarwal *v.* Union of Indian**[27] The appellant, an NRI was carrying a business in Dubai. The forgery took place partly in India and partly in Dubai but the court has that cognizance of such forgery could be taken in India.

5.6. IDENTITY THEFT AND JUDICIAL ACTIVISM

In America, victims are not liable for the bills accumulated up by the imposters, under Federal Law. But in India, we still do not have any effective legislation to deal with this problem and it has the potential to cause untold misery to many. The victims will have to undergo the anxiety and hustle of spending months, even years, regarding their financial health and restoring their good credit history. And this is only possible if the court believes them and discharges them of all liability. A recent study conducted in America by the U.S. government Accounting office[28] showed that there were at least 4,00,000 victims a year and rising.

5.7. HARASSMENT AND STALKING AND JUDICIAL ACTIVISM

In India, the leading case law on harassment at the workplace is that **Vishakha *v.* State of Rajasthan**[29] In India before the **Vishakha** case there was no law referring to harassment especially at the workplace. The judges of the Supreme Court laid down certain guidelines. In a very recent case it was laid down that sexual harassment at the workplace includes any action or gesture which outrages the modesty of female employee. For corporate harassment, a corporate technology policy should state restrictions on computer use for personal business, excessive Web Surfing and even gambling. It should make the employees

[25] K.D. Gaur, "A Text Book on Indian Penal Code" at 20.
[26] Paras Diwan,"E-Commerce Law" at 336.
[27] (1993) 3 SCC 609.
[28] "Identity Fraud" 1998 at 40, Report No. GGB-98100 BR
[29] (1997) 6SCC 241.

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

aware that they can bind the company to a contract, incur tort liability and possible even criminal liability.

In **Ramesh Chandera Arora *v.* State**[30] the accused took indecent photographs of a girl and threatened her father, in letters written to him with publication of the photographs until 'hush money' was paid to him. The Supreme Court held that he was guilty of criminal intimidation. Extending this situation to photographs sent over e-mails, the treat would be the same in my opinion. The main problem that arises then is the proof that the accused sent such photographs.

5.8. JUDICIAL ACTIVISM ON INTERNET PORNOGRAPHY AND GLOBAL ATTEMPTS TO REGULATE IT

The legal response to photography on the Internet has sensitive, been swift and well intention but has, unfortunately backfired. The U.S. Government introduced the **Communication Decency Act, 1996.** Under Clinton administration which attempted to restrict access by minors to patently offensive descriptions of sexual or excretory activities. In particular, the **CDA** specified that it applied to material available above an "interactive computer service" which induced the Internet. Immediately upon its passage, it was contested by Civil Liberation Groups on the ground violated the First Amendment to the US Constitution. Their agreement proved persuasive and **Renu *v.* American Civil Liberties Union**[31]**.** The U.S. Supreme Court declared much of the Act unconstitutional as violating freedom of speech and press.[32]

Ranjit D. Udeshi *v.* State of Maharastra[33] is an important case which defined 'obscenity' in the Indian context. Obscenity is defined as things that deprave or corrupt those whose minds are open to such immoral influences. It also stated that intention was not needed.[34]

5.9. DEFAMATION ON NET AND JUDICIAL ACTIVISM

The case of **lurance Godfrey *v.* Demon Internet Limited**[35] involves the first, judicial decision within England and Wales which concerns a defamatory statement made via e-mail through an Internet Usenet discussion group. The case is also the first one to take into account the liability of an Internet Service Provider under section 1 of the recently enacted **Defamation Act, 1996.**

5.10. ROLE OF JUDICIARY IN DETRMINATION OF JURISDICTION IN CYBER CRIME CASES

Jurisdiction can be divided into three broad categories-

(a) Jurisdiction to prescribe (Legislative Jurisdiction)
(b) Jurisdiction to adjudicate (Judicial Jurisdiction)
(c) Jurisdiction to enforce (Executive Jurisdiction)

(A). Cyber Jurisdiction in Criminal Cases (B). Issues of Jurisdiction in Cyberspace
(C). Judicial Activism and Cyberspace Jurisdiction (D). Indian Context of Cyber Jurisdiction

6. CONCLUSION AND SUGGESTION

The evolution of computer and Internet has changed the scenario of business, society and legal frame work as a whole world. This era of technologically commercialization and globalization has proved vastly beneficial to all walks of life as well as it has touched every segment of society in one or the other respect. With the introduction of computer and Internet the Trans-National and trance-continental barriers have been drastically vanished. The information and communication revolution throughout the world is challenging the

[30] (1996) 1 SCR 924.
[31] No. 96-511, 1997 US LEXIS 4037 (26th June 1997).
[32] Douglas W. Vick, "The Internet and First Amendment" at 414.
[33] AIR 1965 SC 881.
[34] C.K.Kakodar *v.* State of Maharashtra (1969) 2 SCC 687.
[35] 4(2) 260-267, 1999 (July) C.N. 1998G-No. 30.

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017

How to Cite:
Dr. Ravinder Kumar (Dec2017) CRIMES IN CYBERSPACE - PROBLEMS AND PROSPECTIVE
InternationalJournalofEconomicPerspectives,11(1), 323-335
Retrieved from: http://ijeponline.com/index.php/journal .
established institutional and legal practices of the nations and forcing them to amend their methods to that legal practices relating to information and communication tasks and challenges become understandable for all classes of society including the lowest strata of society.

India is a virgin territory, if hackers or computer cartels break into computers and telecommunications system, they can create havoc. The recent studies shows that the real threat is mostly from insiders, with employees having access to computer systems and at the same time external threats are also on rise in the area of Cyber Crimes.

There is a major drawback of adverse publicity, loss of public confidence, and the possible adverse change of managerial standards of care. The computer records may be manipulated to create false debits and credits. Bank mangers and other official institutions should come forward and report such crimes straightway to the concerned authorities but they are reluctant.

Corresponding author **Dr. Ravinder Kumar**
Submitted: 26Oct2017, Revised: 09 Nov2017, Accepted: 25Dec 2017