EFFICACY OF EXISTING LAWS IN COMBATING CYBER CRIMES IN INDIA: A CRITICAL STUDY

ABSTRACT OF THESIS
SUBMITTED TO THE KUMAUN UNIVERSITY, NAINITAL UTTRAKHAND FOR THE AWARD OF DEGREE OF Doctor Of Philosophy IN LAW

Under Supervision of Submitted by
Dr. J. S. Bisht Mrs. Vatsla Sharma
Associate Professor LL.M.
Faculty of Law
SSJ Campus, Almora
Uttrakhand

DEPARTMENT OF LAW
KUMAUN UNIVERSITY, NAINITAL UTTRAKHAND (INDIA)
2014
ABSTRACT

The eminent English jurist Salmond has rightly observed that law seeks to regulate the conduct of individuals in the society.\(^1\) It is therefore, the result of progress and development of the society. The evolution of law can be historically traced back from the origin of civil society. With the gradual development of society, people started living and working together, forming groups which eventually led to the formation of the State. There was need for regulating the conduct of individuals inter se; therefore, State formed the rules of governance which later came to known as ‘law’.

Thus development of law is a process which continued with the changes and advancement in the societal circumstances. Law is generally made to meet the needs of the society and therefore, it is a dynamic concept which undergoes changes with the changing needs of the society. The modern technological evolution has enabled human society to prosper and progress but at the same time has given rise to new problems which were hitherto not known to mankind and cyber criminally is one such grey area which emerged only a few decades ago. The tremendous progress made by computer technology during the last quarter of the 20\(^{th}\) century has now made it possible for the people to visually chat, send messages, transmit information and conduct business with a person in any part of the world through internet. The computer as an innovative mechanism has increased our capacity to store, search, retrieve and communicate data as also accessibility to information which has made it possible for us to communicate with any person, anywhere, anytime in the world.

---

1. Fitzgerald P.J. Salmond on Jurisprudence (12th ed) p.3
Need for a Cyber Law:

The information technology advanced by computer network undoubtedly pervades every aspect of society and governance in the present new millennium. With the increased dependence of e-commerce and e-governance, a wide variety of legal issues related to use of internet as well as other forms of computer or digital processing devices such as violation of intellectual property, piracy, freedom of expression, jurisdiction etc. have emerged, which need to be tackled through the instrumentality of law.

Since cyberspace has no geographical limitations or boundaries nor does it have any physical characteristics such as, sex, age, etc., it poses a big challenge before the law enforcement agencies or regulating cyberspace transactions of citizen within a country’s territorial jurisdiction. Though in practical terms, an internet user is subject to the laws of the State within which he/she goes online but this general rule runs into conflict where the disputes are international in nature.

It is true that at the time when computer technology was at its developing stage, no one ever contemplated that it can be indiscreetly misused by the internet users for criminal purposes. Because of the anonymity of its character and least possibility of being detected, the cyber criminals are misusing the computer for a variety of crimes which calls for the need for an effective legal framework and regulatory measures to prevent the incidence of this peculiar type of criminality which is rampant in cyberspace.
Cyber Crime:

Commenting on the information technology revolution which has transformed the world into a global community, Waleter B Wriston observed, “technology has made us a ‘global community’ in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long” ².

The advancement of technology has brought about radical changes in the modern society. But human experience has shown that every technological change brings with it some unforeseen problem, taking advantage of which the law breakers explore new techniques to perpetrate their criminal activities. In fact, technology-generated crimes not only affect individuals or a nation, but have a widespread ramification throughout the world. Internet is one such gray area, which has given rise to the menace of cybercrimes. The computer based global communication system has crossed the territorial borders thus creating a distinct field for online criminal activity warranting global attention.

Cybercrimes have emanated from development of computer network. Internet in the present millennium has become all pervasive and omnipresent. It has also brought with it new problems hitherto unknown to humanity. Internet in sense is analogous to the “high seas” which no one

owns yet people of all the nationalities use it. The term ‘cybercrime’
encumbers within it a variety of criminal activities taking place in the
cyberspace through the media of global communication and information via
internet.

It is an inevitable evil having its origin in the growing dependence of
mankind on computers in modern life, the reason being that the computers
despite being high technology devices are extremely vulnerable. Thus,
whenever any crime or criminal activity takes place with the use of
computer, it constitutes a cybercrime. It is for this reason that ‘cybercrime’
has been defined as “an unlawful act wherein the computer is either a tool or
a target or both”\textsuperscript{3}.

**United Nation’s Definition of Cyber crime**

Cyber crime spans not only state but national boundaries as well.
Perhaps we should look to international organizations to provide a standards
definition of the crime.\textsuperscript{4} At the Tenth United Nation Congress on the
Prevention of Crime and Treatments of Offenders,\textsuperscript{5} in a workshop devoted
to the issue of crimes related to computer networks, cyber crime was broken
into two categories and defined thus:

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

\textsuperscript{3} Supra Chapter 1.
\textsuperscript{4} Talwant Singh: Cyber Law and Information Technology,
file:///C:/DocumentsasSettings/Administrator/Desktop/Cyber Law-... visited at 10/13/2010 at 6:21 AM
\textsuperscript{5} Tenth U.N. Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.
(b) Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

The term ‘cyber crime’ is a misnomer. This term has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. Cyber crime has not been defined in Indian Penal Code, 1860 because it was drafted in 1860 when computers were non-existent. Cyber crime is an amalgamation of two words: ‘cyber’-related to internet or other electronic networks and ‘crime’-a criminal activity. Literally, the word cyber means “connected with electronic communication networks, especially the internet.” Cybercrimes are such harmful activities in the cyberspace which may cause damage to a person, property or even the State or society as a whole. There are many cybercrimes which are being committed by offenders all over the world using computer technology.

The first recorded cyber crime took place in the years 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 BC in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of series of steps in the weaving of special fabrics. This resulted in a fact amongst Jacquard’s

---

7 According to Oxford Learners Dictionary.
employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from use of the new technology. This is the first recorded cyber crime

**Element of Cyber crime:**

For fixing criminal liability there must be *actus reus* and *mens rea* i.e. wrongful act and wrongful intention. Wrongful act in itself is not sufficient for punishment because there is a legal maxim viz. *actus non facit reum nisi mens sit rea* i.e. act only does not constitute a crime unless the act is done with guilty intention.

In case of computer *actus reus* may include touching keyboard and mouse, trying to get access to data stored by another person under his password or using computer to gain access to her computers or informations stored therein. These examples show the wrongful act. However, these acts cannot be easily proved.

*Mens rea* may include, e.g., intention, recklessness, or negligence etc. In case of computer *mens rea* can be determined if the user knew that using computer for gaining access to information stored therein was unauthorized. Intention to secure access to programmes or data is enough.

**Conventional crime vis-à-vis Cyber crime:**

There is apparently no distinction between conventional and cyber crime. However, on a deep introspection we may say that there exists a fine limit of demarcation between the conventional and cyber crime, which is appreciable. The demarcation lies in the involvement of medium in cases of
cyber crime. The *sine qua non* for cyber crime is that there should be an involvement, at any stage, of the virtual cyber medium.\(^9\) Cyber crimes are different from conventional crime, as they can be easily committed from distant place, difficult to detect and even harder to prove them. It is very difficult to identify the culprit, as the net can be accessed from any part of the globe. The cyberspace is wide open for the cyber criminals for criminal activities.\(^{10}\)

Being radically different from the conventional crimes, the law enforcement agencies find it difficult to tackle cybercrimes with the existing infrastructural mechanism because of lack of adequate knowledge about the computer operating systems. This is the main reason why this relatively new variety of crime is posting a challenge to the legal regime. The problem has been further aggravated by the introduction of internet.

**Nature of Cyber Crime**

The term ‘cyber’ is derived from the term ‘cybernetics’ which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crime committed in cyberspace relating to machines or devices or cyber technology related crimes are to be treated as cyber crimes. Information technology and electronic commerce are widely used to facilitate crime or to commit crime. In wider sense cyber crime is a crime on the internet which includes hacking, cyber theft, forgery, flowing of viruses, cyber

\(^9\) Ashish Pandey: Cyber crimes Detention and prevention, 2006, p- 1.2
\(^{10}\) Anant D. Chinchure: Cyber (Computer) Crimes- a conceptual Analysis, Criminal law Journal 2010.
pornography. Cyber crimes are computer related as well as computer generated crimes. This is increasing every moment which is the cause of global tension. Therefore, law agencies must have detail knowledge and understanding about varying nature of cyber crime.\textsuperscript{11} Cyber crime is a threat to national and international socio-economic, political and security system.\textsuperscript{12}

**Reasons of Cyber Crime**

Hart in his work “The Concept of Law” has said “human begins are vulnerable so rule of law is required to protect them”.\textsuperscript{13} Applying this to cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reason for the vulnerability of computers may be said to be capacity to store data in comparatively small space, Easy to access: Complex, negligence and loss of evidence.

**Stages of computer crime:**

In general penal code, there are four stages for commission of an offence is intention, preparation, attempt and commission. Similar to this, there are also stages in the commission of a computer crime. K.P.C. Gandhi in his article “An introduction to computer related crime”\textsuperscript{14} suggested the four stages in the commission of computer crime which are as follows-1. Planning, 2. Execution, 3. Concealment and 4. Conversion.

\textsuperscript{11} M.Dasgupta: Cyber Crime in India (A comparative study), 2009, p-8.
\textsuperscript{13} Hart H.L.A: The Concept of Law, p-73
Typology of Cyber Crimes:

Typology of cyber crime is based upon on role of computer in cyber crime, on perpetuators of cybercrime, on victim, and on content. Various categories of cybercrimes are as follows:

a. **Hacking:** Hacking means unauthorized access to a computer system.\(^{15}\) It is the most common type of Cyber crime being committed across the world. The word., hacking has been defined in section 66 of the Information Technology Act, 2000 as follows, “whoever with the intent to cause or knowingly that he is likely to cause wrongful loss or damage to public or any person, destroys or alters any information residing in computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking”

b. **Malicious Programs:** Malicious programs such as virus, worms, trojan horses, logic bombs, hoaxes etc. intend to cause harm to its victims.\(^{16}\)

c. **Online Forgery:** Online forgery is an offence which needs little effort as compared to offline forgery. It is not usually restored to for money but it is also employed for “glory or a spirit of devilment, cocking a snook at experts and purchasers”.

d. **Intellectual Property crimes:** Intellectual property consists of a bundle of rights.\(^{17}\) Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright

---

17. The holder of the intellectual property has certain rights that are vested in him alone, unless he chooses to assign them to someone else.
infringement, trademark and service mark violation, theft of computer source code, etc.

e. **Cyber Fraud:** The term “cyber fraud” is not defined in the Information Technology Act 2000 in India. However, according to D. Bainbridge, the phrase ‘Computer Fraud’ is used to describe “stealing money or property by means of a computer that is using a computer to obtain dishonestly, property including money and cheques, credit card services, or to evade dishonestly some debt or liability.

f. **Cyber-terrorism:** Cyber-terrorism is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a Government or its people in furtherance of political or social objective.18

g. **Cyber Pornography:** Internet Pornography, or Cyberporn, is the use of the Internet (e.g., porno websites, peer-to-peer file sharing networks, chat rooms, electronic bulletin boards) to distribute pornographic material. The presence of pornographic material on a public and global network such as the Internet raises serious concerns for parents, teachers, institutions, and governments.

h. **Online Gambling:** It is also called Internet gambling. The habitual and professional gamblers have plenty of opportunities to satisfy their craze for gambling on the internet. There are millions of websites that offer online gambling.

i. **Cyber Defamation:** Defamation with the advent of computers where certain defamatory information is published or posted through email

18Shashank Manish: Regulation of Cyber Crime in India, Cri LJ November, 2008- Journal Section, p-308.
or chat rooms with an intention to defame the reputation of the person is called cyber defamation. Cyber defamation is not different from conventional defamation\textsuperscript{19} except the involvement of a cyberspace medium in the former.

j. **Cyber Stalking:** According to Oxford dictionary, “stalking” is defined as “pursuing stealthily”. Cyber stalking involves following a person’s movements across the internet by posting messages frequented by the victim entering the chat-rooms or constantly bombarding the victim with e-mails etc.

k. **Salami Attacks:** A salami attack is a series of minor data-security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a Salami Attack.\textsuperscript{20}

**Global View of Cyber Crime:**

Cybercrimes being global in character, generally affects the person far away from the place of offence, may it be in the same country or some other country. It therefore, requires policing at international level as also the active co-operation of the international community. The European Convention on Cybercrime\textsuperscript{21} was indeed a praiseworthy attempt as it laid down guidelines to be followed by the member States in combating cybercrime. The Convention suggested measures to be initiated by the States for restructuring their cyber laws to meet the new challenges.

---

\textsuperscript{19} Section 499 of Indian Penal Code, 1860.
\textsuperscript{21} Effective from June, 2001
The Convention not only dealt with the changes and improvements in the substantive part of criminal law but also referred to the procedural aspect which must be taken into consideration while restructuring the existing law to meet the current needs of developing technology. It has been generally accepted that procedural aspect of criminal law is the main hurdle in tackling the problem of cybercrime effectively but at the same time, the substantive part of cybercrime also needs to be redefined to fight against ongoing cyber criminality.

Out of a variety of cybercrimes, the European Convention has chosen ten specific cybercrimes and urged the member States to include them in their information technology laws and provide a concrete mechanism to fright against them. But it is rather unfortunate that many cybercrimes of a particular country are not treated as crime under the criminal law of other countries, which really poses a problem when cross-country cybercrimes are involved. The solution to this problem lies in enacting a global cyber law uniformly applicable to all the countries of the world. The crux of the matter is that universally accepted standard cybercrime preventive laws should not vary from place to place. In other words, uniformity be ensured with reference to substantive cyber laws of various nations.

An overall global view of cyber law indicates that many countries do have their national legislation for combating cyber criminality, but they radically differ from each other as a result of which, a particular cyberspace activity which is considered as a criminal offence in one country

---
22. Section 1, Chapter II of the European Convention document which contains Articles 2 to 13 defining ten cybercrimes under five separate titles.
may not be necessarily so in another country. This variation in law provides loopholes for the cyber offenders to escape punishment.

Therefore, there is dire need for international cybercrime legislation which could be uniformly acceptable by all the countries to tackle the problem of cybercrime. Not only that, there should also be an international policing agency for countering cyber offences. The solution to the problem therefore, lies in the concerted and united efforts of nations around the world and their mutual co-operation in fighting against cyber criminality.

Broadly speaking, the law enforcement agencies all over the world are confronted with four major problems while dealing with cybercrimes in a network environment. The detention and prosecution of cyber criminals online is hindered by the challenges, which may be technical, legal, operation and jurisdictional.

As regards technical challenges, cybercrimes such as hacking of a website, stealing data stored in computers, espionage, exchange of pornographic material, blackmailing etc. involve detection of source of communication which is a complicated task. Therefore, the cyber criminals find it easy to impersonate on the internet and hide their identity.

The menace of cyber criminality is not confined to one or two countries but the whole world is facing this gigantic problem as a “technological scorn”. India is no exception to this computer generated menace. However, as a measure to prevent and control internet crimes, the Parliament enacted the Information Technology Act, 2000 which came into force on October 17, 2000. Information Technology Act, 2000 is the only
Act which gives legal recognition to computers and matters related thereto. The Information Technology Act, 2000 has for the first time brought cyber crime, punishment and procedure for probing it within a legal framework.

Object of the IT Act, 2000

The electronic transactions like other parts of the globe, are in vogue in India, however they were without legal sanctity before the enactment of IT Act, 2000. The increasing growth of electronic commerce, popularly called e-commerce, made it necessary to have legal protection to such transaction. The Indian Parliament took a step of seminal importance by passing the Information Technology Act, 2000. This Act seeks to achieve various objects, which are discussed succinctly as under:

1. To respond and give effect to the United Nations’ call to all States to give favourable consideration to Model Law when they enact or revise their laws so as to facilitate harmonization of the laws governing alternatives to paper based methods of communication and storage of information.

2. To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly called as “electronic commerce” which involves the use of alternatives to paper based methods of communication and storage of information.

---

23 This fact was admitted by the Parliamentary Affairs Minister Shri Pramod Mahajan in Parliament. (Hindustan Times 16 May, 2000).
24 Farooq Ahmad: Cyber Law In India (Law on Internet), 3rd Edn, 2008, p-34
3. To facilitate electronic filing of documents with the Government agencies so as to promote efficient delivery of government services by means of reliable electronic records.

4. To facilitate electronic storage of data;

5. To facilitate and give legal sanction to electronic fraud transfers;

6. To give legal recognition for keeping books of account by Bankers in electronic form;

7. To amend the Indian Penal code, 1860, the Indian Evidence Act, 1872, the Banker’s Book evidence Act, 1891, and the Reserve Bank of India Act, 1934.

The Act totally has 13 chapters and 90 sections (the last four sections namely section 91 to 94 in the ITA 2000 dealt with the amendments to the four acts namely, the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker’s Book Evidence Act 1891 and the Reserve bank of India 1934).


‘Computer’ means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic, and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer
software, or communication facilities which are connecter or related to the computer in a computer system or computer network.\textsuperscript{25}

The important chapters of Information Technology Act, 2000 are IX, X and XI. Chapter IX dealing with penalties, compensation and adjudication is a major significant step in the direction of combating data theft, claiming compensation, and introduction of security practices etc discussed in section 43. This section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like viruses or damages or disrupts any computer or denies access to a computer to an authorised user or tampers etc….he shall be liable to pay damage to the person so affected. Earlier in the Information Technology Act, 2000 the maximum damages under this head was Rs. 1 crore, which was since removed in the Information Technology (Amendment) Act, 2008. The essence of this section is civil liability. Criminality in the offence of data theft is being separately dealt with later under section 65 and 66. Thus the new Section 43-A dealing with compensation for failure to protect data was introduced in the Information Technology (Amendment) Act, 2008.

Adjudication powers and procedures have been elaborately laid down in section 46 and thereafter. The Central Government may appoint any officer not the rank of director to the Government of India or a state Government as the adjudicator.

\footnote{25Section 2 (i) of the Information Technology Act, 2000.}
Chapter X of the Act deal with the Cyber Appellate Tribunal (CAT). The Act establishes a judicial body to adjudicate upon matters arising within the Act called the CAT. It is a fact-finding and as well an appellate authority. This is a judicial body meant solely to adjudicate upon the contraventions of the IT Act and also handle prosecution of the cybercrimes. This is a body which acts like a court and has all the powers of a civil court established under the Civil Procedure Code, 1908 relating to recall of records, examination of witnesses, issuing summons and warrant, etc. Appeal is taken from the CAT to the High Court concerned and hence, the body sits between the adjudicating officer and the High Court. The cyber cases whether civil or criminal are new to the legal world and their area is also global hence, as many provisions of such laws are virgin, the CAT is a pioneer body and all its judgments and rulings would be a trendsetter.

Chapter XI of the Information Technology Act, 2000 has been entitled “Offences”. Broadly speaking, it deals with various offences done in the electronic format, offences concerning computers, computer system and computer networks, (computer crimes) as also those, which come within the ambit of cybercrimes. These offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police, The real power of today’s internet is that it is available to anyone with a computer and a telephone line. Internet places in an individual’s hand the power of information and communication. This power is being misused by devious mind for criminal purpose. Cybercrimes constitute one of the most important challenges facing cyberspace today. The Act categorically defines relating to

---


{17}
cyberspace such as tempering with computer source document, hacking with computer system, breach of confidentiality and privacy etc.

The important sections are as follows:

Tampering with source document is dealt with under section 65. Section 66 deals with computer related offences. Section 66 is amended by Information Technology (Amendment) Act, 2000 as follows:

Section 66A deal with punishment for sending offensive messages through communication service, etc. Section 66B deals with punishment for dishonestly stolen computer resource or communication device. Section 66C deals with punishment for identity theft. Section 66D deals with punishment for cheating by personation by using computer resource. Section 66E deals with punishment for violation of privacy. Section 66F deals with punishment for cyber terrorism. It may be observed that all acts under section 66 are cognizable and non-bailable offences. Section 67 deals with punishment for publishing of transmitting obscene material in electronic form. 67A deals with punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form. Section 67B with punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. Section 67C fixes the responsibility to intermediaries that they shall preserve and retain such information.

Amendments to Certain Statutes:

The Information Technology Act, 2000, to further acceptance and use of documents, evidence and transfer of funds through electronic means, has
amended the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act, 1891 and Reserve bank of India Act, 1934 vide the First, Second, Third and Fourth Schedule respectively. The Act has introduced and given legal sanction to electronic record and documents. It permits the use of electronic record in government and its agencies with a view to promote electronic governance. To give a push to electronic contracts, provisions have been made for attribution, acknowledgement and dispatch of electronic records.

**Analysis of Information Technology Act, 2000:**

The Information Technology Act, 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialized field. The Act has however during its application has proved to be inadequate to a certain extent. The reason may be that it was passed without public debate and in a hurry. The main purpose of passing of Act was regulating E-commerce and not curbing cyber crimes although it has tried to somewhat regulate these crimes by amending various Acts. Several offences such as cyber harassment, cyber nuisance, defamation, cyber stalking have not been properly taken care of. The Act is neither comprehensive nor exhaustive and even does not define “cyber crime”. There is another deficiency in the Act of 2000 as it has defined hacking under section 66 in such a way that it is capable of misapplication. On point of jurisdiction also the Act of 220 is silent. Since cyber crimes are a global phenomenon there must be clear law

---

on points of territorial and other jurisdictions of Indian Courts. The present section 75 regarding jurisdiction is not sufficient because it depends on outside sources for exchange of materials and evidence.

**Information Technology (Amendment) Act, 2008**

With the passage of time and advancement in technology new methods of committing crime using Internet and computer surfaced, the need was felt to amend the IT Act, 2000. New forms of cybercrimes had appeared on Indian scene posing a challenge before the law makers who were faced with two hard options, namely, either to drastically amend the existing law to give it some teeth or to helplessly see it openly outraged and violated by the cyber criminals and others.

At this critical juncture was brought the draft of the Information Technology Amendment Bill, 2006 which was introduced on December 15, 2006 in the Lower House of Parliament. It was scrutinized by an Expert Committee which suggested several changes. The gravity of the issue of emerging cyber crimes on national and global scales had worried the lawmakers so much that they refer it to the Standing Committee of Parliament to finally suggest changes necessary to make the enactment more effective and in agreement with India’s international obligations as an IT power.

**Efficacy of the Existing Cyber Law**

The IT Act, 2000 was amended by the IT (Amendment) Act, 2008. The object of the Amendment Act was to strengthen the existing legislation to curb the cybercrime by abrogating the infirmities of the IT Act and to
make it a suitable legislation for combating the cybercrime effectively. However, it is apposite to state that the Amendment Act could not address the legislative weaknesses of the law. This segment deals exclusively with the infirmities and shortcomings which the Amended Act is suffering from and to ascertain as to how the existing cyber law can be strengthened to make it efficacious and effective to counter the escalating menace of cyber crimes being committed against the individuals, institutions, society at writ large and the governments.

While there are many legislations not only in many Western countries but also some smaller nations in the East, India has only one legislation—the IT Act, 2000.\textsuperscript{32} The IT Act, 2000, though a landmark legislation to deal with the cybercrime in India but the Act could not provide exhaustive measures to counter the rising trend in the cybercrime, for despite the amendment incorporated in it to attune it with the need to curb the cybercrime in view of the technological development in the area of information technology, a number of crimes and important issues have been left unaddressed. Many of the cyber crimes like cyber squatting with an evil attention to extort money, Spam mails, ISP’s liability in copyright infringement, data privacy issues have not been given adequate coverage in the legislative scheme of the Act.

**Criticism of section 66A:** The phraseology of Section 66A is too vague and tantamount to abuse. The provision is violative of Articles 14, 19(1)(a) of the Constitution of India.\textsuperscript{33} Section 66A is breach of fundamental rights. It is absolutely draconian as it gives the authorities an occasion to misuse and


\textsuperscript{33} KRISHNA MOHAN VENIGALLA : THE HINDU, Posted on: May 17, 2013 at 10:22 IST.
deprive citizens of their personal liberty. If section 66A is allowed to be continued in the Act, it will foreclose debates and discussion which is inherently essential for the democracy to survive. Its chilling effect is already visible—the jailing of a professor in Kolkata, a businessman in Tamil Nadu and two young women in Mumbai, for casual cyber writings, or simply forwarding of received material. Today, netizens are victims, but next journalists will be threatened, as most of their writings are uploaded to the Net, too. This is a potential tool in the hands of rulers to curtail the voice of opposition. It is fatal for the freedom of speech of netizens in general and the press in particular. The executive should delete it from the IT Act or refrain from using it.\textsuperscript{34}

**Judicial Response to combat Cyber Crimes:**

The internet culture in its wake has give rise to a number of online disputes, differences, and controversies etc. resulting out of misuse of abuse of computer networks for illegal activities. Though disputes as such are not new to human society as they are known to have existed ever since the dawn of human civilization, but the distressing factor is that disputes relating to online transactions are entirely diverse in their nature, scope and treatment and therefore, the resolution of these cyber-related disputes has emerged as a serious challenge for the courts of law because of the details involved in them with which the Judges are not thoroughly conversant.

\textsuperscript{34} Madabhushi Sridhar (coordinator, Centre for Media Law and Public Policy, NALSAR University of Law, Hyderabad): 66 Shades of Black, Business Today, Edn: December 3, 2012.
A cursory glance at the judicial administration in the Indian setting would disclose that the factors which influence judicial sentencing by and large include age, sex, educational background, mental frame and maturity of the offender. His motive and the circumstances under which the offence was committed and its consequence on the victim or the society also has a bearing on the sentencing of the accused.

The offender’s young age, immaturity and previous clean record are generally good reason for leniency in sentencing while recidivism, persistent association with criminals or criminal world as also the gravity or seriousness of the crime, attracts severe punishment. However, these are mere generalizations and do not in any way bind judicial discretion in sentencing the criminals. The Judges while considering the punishment can hardly afford to overlook the overall collision of crime on society as a whole. Court’s decisions therefore, play a very important role in deciding a future course of action in related cases\textsuperscript{35}.

Although the case law available on cybercrime is far scantier as compared with the traditional crimes, it is constantly growing due to computer becoming more and more user-friendly with the people. The courts have generally shown a tendency to treat cyber criminals guilty of premeditated crime as probable danger to society and therefore, they are unenthusiastic in mitigating the sentence of such offenders.

Judiciary plays an important role in combating cyber crime. Dr. L. Prakash Case\textsuperscript{36} on cyber crime is very significant where the Court convicted

\textsuperscript{35}Paranjape N.V.: Criminology and Penology (13th ed.) page 246-47
\textsuperscript{36}Fatima Riswana v. State of Tamil Nadu, Cri App. 63/2005 decided by Supreme Court on Jan, 2005.
the accused under section 67 of the Information Technology Act, 2000. The accused was arrested by Chennai police for making cyber pornographic images of his clients forcefully. In Mr. Jayesh S. Thakkar v. State of Maharashtra, the petitioner wrote a letter dated 29th May 2001 to the Hon’ble Chief Justice of Bombay High Court about a pornographic site on the internet, and this letter was *suo motu* treated as writ petition.

**Conclusion and Suggestions:** Capacity of human mind is unfathomable. It is not possible to eliminate cyber crimes from the cyber space. History is the witness that no legislation has succeeded in completely eliminating crime from the globe. The on possible step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime. Undoubtedly in India the Information Technology Act, 2000 is a historical step in the cyber world. Further it cannot deny that there are certain grey areas which need to address and change the present Act to make it more effective to combat cyber crime. There is saying ‘prevention is better than cure’ and every internet user take precaution while using net and remember the 5P mantra for online security Precaution, Prevention, Protection, Preservation and Perseverance.

In view of the expanding dimensions of computer-related crimes, there is need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cybercrime with stern hands. Even a short delay in investigation may allow cyber criminals enough time to delete or erase the important data to evade detection, which may cause huge loss to the internet user or the victim. That apart, the

---

peculiar nature of cybercrimes is such that the offender and the victims do not come face to face, which facilitates the criminals to carry on their criminal activities with sufficient sophistication without the fear of being apprehended or prosecuted. It is for this reason that a multi-pronged approach and concerted efforts of all the law enforcement functionaries is much more needed for effective handling of cybercrime cases. A common cybercrime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality.

The process of crime prevention essentially requires cooperation and active support of citizens, institution, industries and the Government alike. Therefore, a sound strategy for prevention of cybercrime necessitates mobilisation of community participation in combating this menace. This calls for participative role of all those who perceive that the growing incidence of cybercrime is a potential danger to society as a whole. It also calls for self protection initiatives by the people who are vulnerable to cybercrimes. They must have adequate knowledge and awareness about the nature and gravity of these crimes and the dangers fraught by them. Obviously, media has an important role to play in warning people against the possible dangers and evil effects of cybercrimes on victims as also the nation and the safety measures which are necessary to combat this hi-tech criminality.

Regulatory control through effective laws is yet another measure of cyber crime prevention. It is possible to exercise control over these crimes by effective implementation of law by enforcement agencies. The legal preventive measures may help in reducing the incidence of cybercrimes provided they get community’s active support in exposing the criminals.
Some other suggestions to prevent and reduce the incidence of cybercrimes at domestic level are as follows:

1. Net Security be tightened up,
2. Use of encryption technology,
3. False e-mail identify registration be treated as an offence,
4. Self-regulation by computer and net users.
5. Use of voice-recogniser, filter software and collar-ID for Protection against unauthorised access,
6. Development of cyber forensics and Biometric Techniques,
7. Need to establish a Computer Crime R & D Centre,
8. Need for Increased Awareness among Victims of Cyber Crimes,
9. Education and Awareness of Computer and Cyber Crimes,
10. Need for a Universal Legal Regulatory Mechanism, etc.

***