The Clarion Volume 6 Number 2 (2017) PP 91-95
The Clarion
International Multidisciplinary Journal
ISSN : 2277-1697

Cyber crime : the legislative enactments and the interpretation of the judiciary with special reference to India.

Pranab Kumar Goswami
J. B. Law College, Guwahati, India

Abstract

This research paper seeks to probe into the various facets of Cybercrime and threats posed by them to Computer and Internet as such is one grey area, which has given rise to the menace of cyber crimes. The advancement of Information Technology has brought about radical changes in the modern human society, experiencing with it some unforeseen problems, taking advantage of which the law breakers explore new techniques to perpetrate their criminal activities. In fact, technology generated crimes not only affect the individuals but to the nation and also have a widespread ramification throughout the world. The paper highlights the Cyber crime scenario in India and the challenges faced by the Law Enforcement Agencies in tackling with these kinds of crimes in cyberspace especially due to the absence of territorial boundaries and also because of its transitional nature. The paper aims at identifying the problems emanating from the expanding dimensions of Cyber crimes and its impact as a whole; and also extent the role of Comprehensive Legislation, Judiciary to combat and tackle these crimes in the *e*-world to the best of its capacities with special reference to India. Efforts are made to elucidate that, there is a dire need for international Cyber crime Legislation and a Global Cyber Law to be uniformly accepted by all the countries to tackle the ambivalence threat of Cyber crime.

Keywords: Cyber crime, Cyberspace, Information Technology, Internet, Legislative Measures, Judicial Responses, Cyber Law and *e*-world.

1. Introduction

Cyber crime is an ever increasing phenomenon presently in India and also in whole over the world. Though with the dawn of technological revolution, the whole world has become a global village, yet at the same time the use of computer, internet system is creating a complex problem to Governments and individuals. Today out of 7.5 billion world population, about 3.7 billion people use this medium and in many ways, it is also used for illegal activities by the cyber criminals. The essence of a strict statutory law to regulate criminal activities in the cyber world and to protect technological enforcement system was highly on demand.

In 1996, a law discipline known as cyber law originated in United States. In order to curb cyber crime, cyber law is a must because it touches all aspects of transactions and activities concerning the internet, the World Wide Web and cyber space. As cyber law develops around the world, there is a growing realisation among different nations of the world that these laws must be harmonized and internationally best practice. So, in order to promote a legal regime to regulate and curb different criminalities taking place in cyber space, like most of the advanced and frontrunner countries, India also enacted and passed an Act known as Information Technology Act, 2000, which was considered to be a proactive piece of

Corresponding author : pranab.pkg08@gmail.com
DOI : 10.5958/2277-937X.2017.00034.X

legislation aimed to combat cyber crimes from the country.

2. Concept and scope of the domain

Cyber crime is defined as any criminal activity that uses computer either as instrumentally, target or means of penetrating further crime. It is the offence that uses the internet as a medium to commit unlawful acts. The term cyber crime is like an umbrella under which many illegal activities may be grouped together. On the basis of the nature and purpose of the offence, cyber crimes have been classified into three categories depending upon the target of the crime. It may be against an individual or person, cyber crime against property and cyber crime against Government.

The U.N. Congress on Prevention of Cyber Crime and Treatment of Offenders internationally defined cyber crime under two categories:

i) Cyber crime in a narrow sense connotes a computer crime and includes any illegal behaviour directed by means of electronic operations that target the Security of Computer system and the data processed by them.

ii) Cyber crime in a broader sense include 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 networks.

The expanding dimensions of computers and internet offered vast scope and opportunities to human beings to identify, evaluate and exchange information for the benefit of public all over the world. It provided collaboration to new environment, new culture, new business links and commercial networks virtually revolutionising all walks of human life. However, the anonymous nature of the internet has led to many disturbing activities in the cyberspace which enable the perpetrators to indulge in various types of criminal activities. The rapid growth and use of the information technology and electronic commerce have led to many cyber crime incidents at present in India.

In the Indian context, cyber crime may be defined as a voluntary and willful 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.

There is a need of international commitment, coordination and co-operation to tackle these crimes in the cyberspace. As it has become a deadliest epidemic in this millennium, it is necessary for the citizen to know the menace and also the ways to curb it with Information Technology Act, 2000 and other updated Legislative enactments.

3. Objectives of the study

Any study or research is futile without a reasonable objective. The particular topic selected for this research paper has immense importance and it is quite relevant in present day context. The growing danger from crimes committed in the cyber space using the medium of computer and internet is beginning to claim attention in India. It is high time to take adequate and proper legal measures to control and combat these criminal activities.

Mankind has certainly come across a long way and it goes unsaid that with progress come new challenges. The Information Technology Act, 2000, which saw the unification of world in many ways, also saw the arrival of cyber specific legal challenges. The absence of traditional barriers and due to the characteristics of cyber space like easier accessibility, anonymity and its superior reach, the miscreants who found the virtual world to be a perfect platform to wreak havoc. The main aim of the research paper is to highlight the various problems of cyber crimes taking place in the country and the judicial interpretation of the cyber law and also to frame the measures adopted by the legislation to tackle these complexities in the virtual world. The objectives of this research work are to touch all the facets of cyber crimes taking place at the electronic world in comprehensive ways. Some of the pin point objectives have been outlined here as follows:

i) To understand the basic concepts of the cyber world and crimes taking place in the cyber space.

ii) To discuss comprehensively the various categories of cyber crimes committed in India.

iii) To highlight the legislative provisions adopted to curb the problems related to cyber crime.

iv) To discuss the Information Technology Act, 2000 and to decipher the steps necessary to tackle the menace of cyber crimes in India.

v) To discuss the challenges before the Law Enforcement Agencies and the interpretation of the Judiciary with reference to India.

vi) To discuss the concern about International Legislature and to introduce uniform global cyber law to tackle cyber crime as a whole.

4. Research Methodology.

The methodology adopted in the preparation of this research paper is doctrinal in nature and comprises of secondary sources. The secondary sources include text books by various authoritative writers on cyber crimes and cyber laws, the Information Technology Act, websites, newspapers, internet sources, law journals, different magazines, Supreme Court law journals, articles, etc.

The methodology of the systematic investigation gives an overview of the concept of cyber crime, to analyse the problems of cyber crime in India, and also to find out the legal remedies through the Information Technology Act, 2000 and the proper legislative enactments.

5. Legislative measures adopted in the *e*-world (Information Technology Act, 2000, in specific)

The information technology advanced by computer network and internet undoubtedly pervades every aspect of Society and Governance in the present millennium. With the increased dependence of *e*-commerce and *e*-governance, a wide variety of legal issues related to use of intent 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 boundaries or geographical limitation or any physical characteristics, it poses a big challenge before the law enforcement agencies for regulating cyberspace transaction of citizen within a country's territorial jurisdiction. The anonymity of the characters of cyberspace and the 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 frame-work and regulatory measures to prevent the incidence of this particular type of criminality which is rampant in cyberspace.

The traditional laws such as the Indian Penal Code, 1860, Indian Evidence Act, 1872, Bankers Book Evidence Act, 1891, Reserve Bank of India Act, 1934, Companies Act, 1956, etc were relevant to the socio-economic and cultural scenario existing prior to the advent of information technology but these laws were found insufficient to cater the needs of new crimes emerging from the internet expansion. Notably, some of the traditional crimes like conspiracy, solicitation, securities fraud, espionage, etc. are now being committed via internet, which requires a new law to regulate these offences. It was in this background that Information Technology Act, 2000, was enacted in India primarily for facilitating *e*-commerce and prevention of illegal and unlawful activities through computer networks and internet. Prior to the enactment of this Act, the law applicable to cyber offences was the Indian Penal Code, which was enacted long back in 1860 when no one even thought of computer technology or cyber criminality. With the coming into force of Information Technology Act, 2000, it became necessary to introduce a certain consequential changes in certain provisions of the Indian Penal code as also in the Indian Evidence Act, 1872, in order to meet the new requirements of the cyberspace crimes.

The Information Technology Act, 2000, came into force with effect from 17th October, 2000. It has been amended in the year 2008 and the Amended Act is effective from the 5th day of February, 2009. The rules under the Amended Act have also been framed, which became effective from October 27th, 2009.

6. Judicial responses and the challenges before the Judiciary towards Cyber Crimes.

The computer, computer networks and internet, online culture have become an integral part of existence in this modern world. Most of the activities such as commerce, industries, banking, exchange of money, information, communication, government and non-governmental official transactions, academic pursuits, etc. are carried on through the internet. However, in spite of various advantages of the computer technology, there are also certain negative aspects, but the judicial functionaries, as well. The internet culture has given rise to a number of online disputes, differences, controversies, etc. resulting out of misuse or abuse of computer network for illegal activities. The online activities are entirely different in nature, scope and treatment and as such the resolution of cyber disputes emerged as a serious challenge for the courts of law. The Judges are at times not thoroughly conversant with the intricacies involved in them. The factors that hamper judicial sentencing in various kinds of cyber crimes are:

i) The nature of these crimes and the absence of geographical or territorial boundaries.
ii) No clarification outlined as to which court would have the exclusive jurisdiction to try the case.
iii) Variation in the legal system and procedure of different countries regarding the accountability and admissibility of cyber related cases.
iv) Uncertainty as to the exact definition of cyber crime.

Since, cyber crime cases are different from conventional crimes, the traditional adversarial system of litigation would hardly meet the ends of justice involving these crimes.

A glance at the Judicial Administration in the Indian setting would reveal that the factors which influence judicial sentencing at large include age, sex, educational background, mental frame and maturity of the offender. The motive and the circumstances under which the offence is committed and its affect on the victim or the society, also have a bearing on the sentencing of the accused. The offender's young age, immaturity and previous clean record are generally good grounds for leniency in sentencing, while recidivism, persistent association with criminals or criminal world, gravity or seriousness of the crime, attract severe punishment. However, these are mere generalization and do not in any way fetter judicial discretion in sentencing the criminals. The cases of crime in the cyberspace are constantly escalating due to computer becoming more and more user friendly for the people. The Judges, therefore, while considering the punishment can hardly afford to overlook the overall impact of various cyber crime on society as a whole. Thus, Court's decision plays a vital role in deciding a future course of action in similar cases. Since, cyber crimes are more rigorous, the general trend to obey is the prevention and control of various cyber crimes by adopting severe and stringent way of punishing the offender.

7. Findings and discussions

The paper highlights that, cyber crimes are such harmful activities in the cyberspace that cause huge damage not only to the individuals but also to the person's property or even the society, state and the country. Being radically different from the conventional crimes, the law enforcement agencies also find it difficult to tackle cyber crimes because of inadequate knowledge about the computer systems. This is the prime reason why this new variety of crime is posing a great challenge to the legal regime. 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'. The technology has extended its tentacles cutting across national frontiers whereas the law is still struggling to define and redefine the boundaries for the control of cyber crimes. Following a similar course, the cyber law particularly, the Information Technology Act, 2000, is engaged in prevention and control of cyber crimes within the country's territorial jurisdiction overlooking the facts that cyber criminality is a global phenomenon which has no territorial limits.

A nation wise survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many countries have not even initiated steps to frame laws for policing against these crimes. This divergent approach of world nations towards the desirability of cyber law posses a real problem in handling the internet crime and at the same time provides ample scope for the cyber criminals to escape detection and punishment. All the nations should therefore, realize the need and urgency for generating awareness about the dangerous nature of cyber crimes which are perpetuating illegal online activities in cyberspace. Cyber criminality is perhaps the deadliest epidemic spread over the world, which has to be curbed by adoptive global preventive strategy.

An overall view of the cyber law indicates that many countries do not have national legislation for combating cyber criminality. The cyber law radically differ from each other as a result of which, a particular cyberspace activity which is considered as a criminal offence in one country may not be necessary so in another country. This variation in law provides loopholes for the cyber offenders to escape punishment. The solution to the problems of cyber crime lies in the united efforts of nations around the world and their mutual cooperation in fighting against the cyber criminality. The technical, legal, operational and jurisdictional problems that hindered the detection and prosecution of the cyber criminals can be tackled by implementing Global Cyber Law, uniformly applicable to all the countries of the world, policing at international level and also the active cooperation of the entire International community.

8. Conclusion

The roots of cyber crime lie in the technology and critical infrastructure. Number of internet users is continuously increasing and with this growth, risk of several types of crimes is also amplified. Technology based crimes have been developing with the passage of everyday and they need to be solved with utmost priority. These crimes are not only restricted to computers but also other electronic devices like financial transaction machines, Tele-communication equipments, etc. The proliferation in registering the cyber crimes under various sections of Information Technology Act, 2000, and Indian Penal Code shows the severity of

cyber threats; however, most of the cases were still unreported because of various reasons.

Cyber crimes are varying in its nature due to enhancement in technologies. Few classifications of such crimes may look like the traditional crimes; however, many of them are recognized as different kind of crime and to be handled in a different way. Due to its diversified nature, it is very difficult to curb crimes in the cyberspace and as such the Information Technology Act, 2000, was passed with the very motive to tackle the problems of cyber crimes and to protect the internet resources of the potential victims. However, even the Information Technology Act, 2000, does not seem to be adequate to stop the cyber crimes in the *e*-world. The hardships faced to curb crimes in the cyberspace and also the lacunas in the Information Technology Act, 2000, that have led the cyber thugs and the fake identities to exploit the users of internet without fear of being punished. The information technology based global communication system has crossed the territorial boarders, thus creating a distinct field for online criminal activity in the super highway warranting attention worldwide in subscribing a Global Uniform Cyber Law to tackle with crimes related to cyberspace at best.

References

Ahmad Dr. Farooq; "Cyber Law in India (Law on Internet)", New Era Law Publications, Delhi, 3rd Edition 2008

Paranjape Prof. N.V.; "Criminology & Penology with Victimology", Central Law Publications, Allahabad-2, Reprint-2012

Paranjape Dr. Vishwanath; "Cyber Crimes and Law", Central Law Agency, Allahabad-2, 2010 Edition

Sharma Vakul; "Information Technology, Law and Practice", Universal Law Publication, 3rd Edition, 2013

https://en.m.wikipedia.org/wiki/cybercrimes Date: 25/06/2017 Time: 10:15 pm

https://www.cyberlawindia.net/cases Date: 02/07/2017 Time: 9:35 pm

https://www.ijecs.in Date: 23/06/2017 Time: 10:20 pm

https://www.cyberlawhub.com Date: 09/07/2017 Time: 9:10 pm

https://www.legalcrystal.com Date: 07/07/2017 Time: 10:30 pm

https://www.indiagovernance.blogspot.in Date: 25/06/2017 Time: 10:45 pm

https://www.indiankanoon.org Date: 18/06/2017 Time: 8:30 pm

https://www.lawmanblog/blogspot.com Date: 09/07/2017 Time: 9:35 pm