Cyber Crimes In India – A Study On Prevention And Control Strategies

1satish Kumar Ganta, 2dr.K.I.Pavan Kumar
1Research Scholar, KLU College of Law, KL (Deemed to be University) KLEF, Vaddeswaram, Andhra Pradesh, India.
2Associate Professor, HOD, KLU College of Law, KL (Deemed to be University) KLEF, Vaddeswaram, Andhra Pradesh, India.
Corresponding author: gskumarphd@gmail.com

ABSTRACT
Cyber Crime is not a matter of concern for India only but it is a global problem and therefore the world large has to come forward to curb this menace. This paper examines the statutory provisions with regard to cyber crimes in India and it analyzes the global perspectives of cyber crimes and to examine the laws relating to global cyber crimes and it further discusses the grey areas under the Information Technology Act, 2000. The present research study is said to be doctrinal in its nature. An academic attempt has been made under take the comparative analysis of various cyber laws that exist across the globe. In the context of increasing dimensions of computer related crimes, there is every need for adopting appropriate legal measures of regulatory nature and the law enforcement mechanism is to be geared up in order to tackle the cyber crime problem with stern hands. A common cyber crime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality. The internet users must have adequate knowledge and awareness about the nature and gravity of these crimes and the dangers fraught by them. Regulatory control through rigid laws is another measure of preventing the cyber crimes. New prevention strategies like the ‘intrusion management’ may be used for detection, testing and investigation of cyber crimes.

KEY WORDS: CyberCrime, Cyber Law, Statutory provisions, IT Act, 2000

I. INTRODUCTION
The Internet changes everything. It upsets our notions of how things should be, how countries should be governed, how companies should be run, how teachers teach and children learn, and even how housewives make new recipes. It mixes up our conceptual framework of what we think we know about the world, about each other and about ourselves. It is liberating, exciting, challenging and terrifying all at the same time. To a majority of the people, the Internet remains mysterious, forbidding, incomprehensible and frightening.

Further complicating cyber crime enforcement is the area of Legal Jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of Internet crime without cooperation from other nations. Law enforcement agencies around the world are working together to develop new partnership, new forensic methodologies and new responses to cybercrime in order to ensure safety and security on the Internet. Due to its global dimensions and borderless nature, new and innovative responses are required to the issue of cybercrime or e-crime or computer crime.

Cyber Crime may be stated as “unlawful acts wherein the computer is either a tool used to perform the crime or it becomes a target of crime or sometimes both.” Cyber Crime is neither defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008. Under the Indian Penal Code, 1860 and a few other legislations meaning of crime or offence has been elaborated which is not done in this act. Hence, to define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms, any offence or crime in which a computer is used is a cyber crime”. Certain Acts of Information Technology Act -2000 and the I.T. Amendment Act 2008 were enforced with reference to banking and financial sector transactions.

www.turkiphysiotherrehabil.org
II. STATEMENT OF THE PROBLEM

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called ‘cyberspace’. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. There is hardly any human activity that is not touched by the internet.

A legal framework for the cyber world was conceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The IT Act amends some of the provisions of our existing laws i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing cyber crimes, but the problem is that still this statute is more on papers than on execution because lawyers, police officers, prosecutors and Judges feel handicapped in understanding its highly technical terminology. Since cyber crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. As a result of the rapid adoption of the internet globally, computer crimes are multiplying like mushrooms. The law enforcement officials have been frustrated by the inability of the legislators to keep cyber crime legislation ahead of the fast moving technological curve. At the same time, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world’s public and private networks. This research work will also take a comprehensive view of the governmental efforts being done in India and abroad to stop such crimes and will look closely on their success and failures. An effort will also be made to vigorously analyze the various perspectives of IT Act, 2000; its ins and outs including its shortcomings and the possible means and ways to overcome them.

III. OBJECTIVES

- To examine the statutory provisions with regard to cyber crimes in India
- To analyze the global perspectives of cyber crimes and to examine the laws relating to global cyber crimes.
- To analyze the grey areas under the Information Technology Act, 2000

IV. RESEARCH METHODOLOGY

The present research study is said to be doctrinal in its nature. An academic attempt has been made to under take the comparative analysis of various cyber laws that exist across the globe. The required data has been extracted from the decided cases across various courts of judicature under their published formats.

Cyber Crime and its Definition

The term “Cyber Crime” is said to be the umbrella term as it constitutes various illegal activities which are grouped together. The tool with which the aspect of cyber crime is committed is said to be the technology aspects and the perpetrators of these cyber crimes are mostly intellectual and technically equipped persons with multi various skill sets having the through and distinctive understanding of the computer and internet applications. With the emergence of modern times, the term cyber crime has metamorphosed into aspects like cyber terrorism, cyber stalking, email-bombing, email-spoofing, cyber defamation and cyber pornography etc. In short, the term cyber crime means any lawful act wherein the computer is either a target or a tool or both.

Cyber crimes may precisely be termed as those branches of crime in which the computer is either on object or subject of conduct constituting the crime or it may be even both. Thus, all activities that utilizes computer as an tool or instrument or target of an appliance for perpetrating further crime, falls under the ambit of cyber crime. The exact definition of cyber crimes has been defined in statute under any law or established statute as yet. The Information Technology Act, 2000 under the Indian context does not contain the exact definition of cyber crime.

Statutory Provisions with regard to Cyber Crimes in India under IT Act, 2000 and IT (Amendment) Act, 2008

Broadly, the IT Act, 2000 comprises the aspects of digital and electronic signatures, electronic governance, electronic contract, regulation of certifying authorities, electronic signature certificates, electronic subscriber, penalties, compensation and adjudication. The said act covers the aspects of Cyber Appellate Tribunal (CAT) and the offences and punishments for computer related offences.

www.turkjphysiotherrehabil.org
The main reason for the enactment of IT Act, 2000 is the increased usage of communication technology in performing the transactions of the business and entering into agreements and contracts, as it was felt easier and faster than the traditional practices of paper documentation. Another important reason for the enforcement of the IT Act, 2000 was the United Nations Commission on International Trade Law (UNCITRAL) and its model law on electronic commerce in the year 1996 and its effort to attain the uniformity in the laws that govern commerce across the world.

The main objective of the IT Act, 2000 is to provide legal recognition of digital signatures and electronic records. The Act provides the legal recognition to the procedures executed by way of electronic data interchange (EDI) and other forms of electronic communication. The IT Act in India provides the legal recognition to the business contracts and it creates the rights and obligations through electronic media and establishes a regulatory body in order to supervise the authorities of certification that issues digital signature certificates. The IT Act further creates civil and criminal liabilities for the contravention of the provisions under the act and it prevents the misuse of the transactions of e-business nature.

Cyber Law in the Global Context

With the advent of rapid innovations in computer technology and internet activities over the years, the problems of cyber crimes has attained magnanimous proportions and emerged as a global issue. It has posed a new format of problems for law enforcement agencies across the globe. Due to its devastating effect on a worldwide platform, it has attained the cause of serious concern for the legal fraternity and to formulate strategic ways and means to counter the cyber criminality.

The internet operations comprising the global nature do not recognize any geographical boundaries. This promotes the cyber criminals to operate beyond their national territory without their physical presence at the crime scene. Hence, the cyber crime problems calls for greater international cooperation and support. The development of universal law that governs the transactions of cyber space would make it much easier to decide about the applicability of the law to regulate a particular activity of online nature. It really demands a coordinate action for all alike including the institutions, people, governments and industries and above all the nations. As the cyber crime activity as an international ramification, it has to be handled through unanimum and common legal strategy which possess the universal recognition and acceptance.


Many countries have adopted cyber law in their legal regimeto meet the challenges against the internet criminal activities. Some countries has substantially updated their cyber laws while others have partial updated them. The prosecution of international cyber criminals was uncertain as the existing domestic cyber laws of various nations comprise structural variations and gaps.

Weak enforcement mechanisms for protecting the network information and inadequate legal protection of digital information enables the cyber crime perpetrators to carry on their criminal activities through online across the geographic boarders undeterred with least chances of their being nabbed or apprehended.

The UN reporton the extent of progress made by the nations across the world in updating their cyber crime laws shows that 24 percent of the world countries have fully updated their cyber laws while 20% have partially updated their cyber laws and 56 percent of the nations have not updated their cyber law as yet.

Grey Areas under the IT Act, 2000

Information Technology had played the significant role in the human life. The aspects of e-communication, e-commerce, e-governance, e-banking and e-contract haddeliberately substituted the paper based
communication. Though, there are various advantages under the electronic mode of operations, there exists certain disadvantages in the mode of electronic transactions. Thus, by analyzing the various provisions under IT Act, 2000 there are certain specific lacunae that exist within the perimeter of the IT Act. The IT Act, 2000 does not cover the significant issue of jurisdiction which is very crucial, and fundamental aspect deciding the place of filing the complaints. The IT Act does not touch the authenticity of evidentiary value of the e-mail at the receiver hands. The IT Amendment Act, 2008 does not specifically contain any significant provisions for the protection of intellectual properties like such as patents, trademarks and copy rights etc., in the digital medium. The aspect of e-commerce is mainly routed in domain names. But the IT Act remains silent about the infringement of domain names, spamming, typo-squatting, cyber squatting and security of information at various levels. The IT Act does not cover the provisions like policies of crossing border taxation at international level if the contracts are signed at international level through online. Under section 77 (B) of IT Amendment Act, 2008, any offence punishable with imprisonment of three years or above shall be cognizable but the failure to surrender license under Sec. 33 is non-cognizable offence.

Under section 79 of IT Amendment Act , 2008, no specific directions were given to intermediary to install any appropriate software so as to prevent the transmission of pornography material or obscenity any infringed material. It is necessary that the intermediary shall be given specific direction for facilitating the installation of relevant software for preventing the said obscene material being transmitted over the networks. The liability must be strictly decided.

The IT Act covers only certain category of contraventions and cyber crimes. The IT act only covers around 23 offences where as 8 existing offences were substituted. Certain offences like watching porn websites and chat room abuses were not yet covered. The offences mentioned in the act are not exhaustive and the term cyber crime and cyber offence were not clearly defined under the said Act. The IT Act does not cover important documents like contract of sale of immovable property, negotiable instruments, will, power of attorney and trust. The IT Act do not extend its hands over the statutory bodies and they are not bound to accept documents of electronic nature under the Act. It is important to mark that section 9 under the IT Act, 2000 is the biggest loop hole as the main objective of the Act was to facilitate governance and section 9 provides that one can insist any government offices to interact in the electronic formats. Hence, it is to be made mandatory for the statutory bodies like the government agencies to accept the electronic documentation format. The IT Act does not draw any limitations or parameters for its implementation process and procedures. The executive and the judiciary members are not tech savvy or computer experts and they are not sensitized fully towards technology and hence the question of implementing the provisions of IT Act does not arise. In order to implement the provisions of the act specifically, the members of the prosecution, judicial and police officials must be sensitized towards the technology.

V. CONCLUSION AND SUGGESTIONS

In the context of increasing dimensions of computer related crimes, there is every need for adopting appropriate legal measures of regulatory nature and the law enforcement mechanism is to be geared up in order to tackle the cyber crime problem with stern hands. The delay procedures in the investigation process may allow the criminals under cyber crimetodemolish or destroy the important evidentiary data in order to evade detection which may cause a significant loss with the victim or the internet user. A common cyber crime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality. The process of cyber crime prevention essentially requires proactive support and cooperation of industries, institutions, citizens and the government agencies alike. Therefore, a sound and effective strategy for prevention of cyber crimes necessitates mobilization of community participation in combating this menace. This requires the participate role of all those who perceive that the growing incidence of cyber crimes is a potential danger to the society as a whole. It also calls for self protection initiatives by the people vulnerable to cyber crimes. The internet users must have adequate knowledge and awareness about the nature and gravity of these crimes and the dangers fraught by them. Regulatory control through rigid laws is another measure of preventing the cyber crimes. New prevention strategies like the ‘intrusion management’ may be used for detection, testing and investigation of cyber crimes.

REFERENCES


www.turkjphysiotherrehabil.org