International Journal of Research in Social Sciences
Vol. 9 Issue 4, April 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CYBER LAW AND PRACTICES – ISSUES AND CHALLENGES

Dr.N.C.Patnaik
Principal, Lingaraj Law College, Berhampur.

ABSTRACT

World is passing through the unprecedented phase of metamorphosis in the area of information technology that has made dramatic changes in the daily routine of our life. With the development of science and technology human being all over world live a comfort life and conveniently enjoy fruits of its. The evolution of information technology gave birth to the Cyber space wherein internet provides equal opportunities to all the people to access any information, data, storage, analyses etc with the use of high technology. A number of frauds are committed at website, people are charged by the misuses of information technology and the security of electronic record is also at stake indeed the cyber criminals have put challenges to all law makers and others for the control of cyber crimes rampant all over the globe.

This paper contribute an understanding of the cyberspace and how far the present law in India is successful in dealing with the issue and what way is the legal structure logging to curb the crime. This paper delineates the legislative response to cyber crime in India with an analysis of the Information Technology(Amendment) Act, 2008 focusing on the new crimes introduced by the amendment on the touch stone of cybercrime categories. This paper deals with eth varies aspects and practices of cyber law and jurisprudential approach on various aspects and finally with the scope of innovation and future task it ends with a conclusion and suggestions.

=====

Introduction

Crime is a social and economic phenomenon and is old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment". The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin "the criminal quality of an act cannot be discovered by reference to any standard but one; is the act prohibited with penal consequences". Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. Cyber crime is the latest and perhaps the most complicated problem either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime. Cyber crime are computer related as well as computer generated crimes which are increasing day by day. Cyber crime is a term used to broadly describe criminal activity in which computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attack. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

The world 1st computer specific law was enacted in the year 1970 by the German State of Hesse in the form of 'Data Protection Act, 1970' with the advancement of cyber technology. With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. It is under these circumstances Indian Parliament passed its "Information Technology Act, 2000" on 17th October to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishment in the field of cybercrimes.The technological development has given rise to a cyber world constituting cyber space. Cyber Space is witnessing considerable advancement with the rapid increase in the information technology.It is always hard to determine or predict something in the future in an accurate manner.

There is a possibility to consolidate the technological advancements in the past. The internet users are increasing tremendously every year and at the same time there is also rise in the number of people using mobiles and smart phones.

In India, there has been a surge of approximately 350 percent of cybercrime cases registered under the Information Technology (IT) Act, 2000 from the year of 2011 to 2014, according to a joint study by the Associated Chambers of Commerce and Industry of India and consulting firm price water house Coopers. The Indian Computer Emergency Response Team (CERT-In) has also reported a surge in the number of incidents handled by it, with close to 50,000 security incidents in 2015, noted the Assocham-PWC joint study.Calling the Internet a “virtual world” and a “world which is invisible in away”, the Supreme Court observed that the fundamental right of expression includes “the right to be informed and the right to know and the feeling to protection of expansive connectivity” the Internet officers on the click of a button.

In 2016 security codes of around 32 lakh debit cards were breached and several users reported unauthorized transactions from locations in China. Events like this have prompted the government to have a customized cyber security policy for each ministry and department.

Objective of the study

Cyber crime is based on trust and public policy with the society who handle the cyber space business in India. Cyber crime increase an alarming proportionate by sending shock news through the cyber infringement and the current study aims at to analyse the concept of cyber crimes in society by presenting illegal data and to review the cyber crime in different aspects through legal interpretation.

Research Methodology

The secondary data has been taken from different sources. The method of study of this paper will be explanatory and descriptive in nature. In addition to above, the paper deals with secondary sources based on Internet, Journal, Literature Review, Law Reports, Case study and other relevant documents.

Meaning of Cyber Crime

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity and include everything from electronic cracking to denial of service attack. Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Cybercrimes includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

Classification of Cyber crimes

Cyber crimes which are growing day by day, it is very difficult to find out what is actually a cybercrime and what is the conventional crime so to come out of this confusion, cybercrimes can be classified under different categories which are as follows:

1. Cyber Crimes against Persons:

There are certain offences which affect the personality of individuals can be defined as:

- **Harassment via E-Mails:-** It is very common type of harassment through sending letters, attachments of files and folders i.e. via e-mails,. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc increasing day by day.
- **Cyber Stalking:** It means expressed or implied a physical treat that creates fear through the use of computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

- **Defamation:** It is an act of imputi9ng any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer network activities endanger the sovereignty and integrity of the nation.
- **Cyber Welfare:-** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorised Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Cyber crimes against society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. This offence includes:

- **Child Pornography:-** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:-** It may be trafficking in drugs, human beings, arms, weapons etc which affect large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:-** Online fraud and cheating is one of the most lucrative business that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs etc.
- **Financial crimes:-** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending

bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

- **Forgery:-** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.
- **Hacker Attack:-** Fred Cohen, a Ph.D student at the University of Southern California wrote a short program in the year 1983, as an experiment, that could "infect" computers, make copies of itself, and spread from one machine to another. It was beginning and it was hidden inside a larger, legitimate program, which was loaded into a computer on a loppy disk and many computers were sold which can be accommodate at present too. Other computer scientists had warned that computer viruses were possible but Cohen's was the first to be documented. A professor of his suggested the name "virus". Cohen now runs a computer security firm.
- **Internet Hacker:-** Wang Qun, who was known by the nickname of "playgirl" was arrested of an internet hacker in China. He was a 19 year old computing student, arrested in connection with the alleged posting of pornographic material on the homepages of several government run websites. Wang had openly boasted in internet chat rooms that he had also hacked over 30 other web sites too.

Social Media and Challenges

One of the biggest problem cyber law is encountering is related to development of jurisprudence relating to social networking. Increasing adoption and usage of social media are likely to bring various legal, policy and regulatory issues. Social media crimes are increasingly gaining attention of relevant stake holders. Misuse of information, other criminal and unwanted activities on social networking platforms and social media are raising significant legal issues and challenges. There is a need for the countries across the world to ensure that rule of law prevails on social media.

Emerging trends and challenges in cyber law

Cyber law is likely to experience various emerging trends with the increasing usage of digital technology.

The various emerging trends include:

a. Challenges in Mobile Laws.
b. Legal issues of Cyber Security.
c. Cloud Computing and Law.
d. Social Media and Legal Problems.
e. Spam Laws.

a.Challenges in Mobile Laws:- Today there are lots of activities in the mobile ecosystem. The increasing competition has introduced new models of mobile phones, personal digital assistors (pda) tablets and other communication devices in the global market.

The intensive use of mobile devices has widened the mobile ecosystem and the content generated is likely to pose new challenges for cyber legal jurisprudence across the world.

There are no dedicated laws dealing with the use of these new communication devices and mobile platforms in a number of jurisdictions across the world as the usage of mobile devices for input and output activities is increasing day by day.

While the increasing mobile crimes, there is an increasing necessity to meet the legal challenges emerging with the use of mobile devices and ensure mobile protection and privacy.

b.Legal Issuess of Cyber security:- The other emerging cyber law trends is the need for enacting appropriate legal frameworks for preserving, promoting and enhancing cyber security.

The cyber security incidents and the attacks on networks are increasing rampantly leading to breaches of cyber security which is likely to have serious impact of the nation.

However, the challenge before a lawmaker is not only to develop appropriate legal regims enabling protection and preservation of cyber security, but also to instill a culture of cyber security amongst the net users.

The renewed focus and emphasis is to set forth effective mandatory provisions which would help the protection, preservation and promotion of cyber security in use of computers, allied resources and communication devices.

With the growing activities of cyber crime across the world, there is a need for enacting a appropriate legislative, regulatory and policy framework pertaining to cyber security. The International Conference on Cyber law, Cyber crime and Cyber security which took place in November 2014 in India highlighted significant issues affecting cyber security and came up with various recommendations for international stakeholders. It is likely that countries of the world have to deal with issues pertaining to attacks and intrusions into computer systems and networks from location outside the territorial boundaries of the country. It has the potential of prejudicially impacting the sovereignty, integrity and security of the country. Thus there is a need for the nations across the world to amend their existing IT Legislations which would help the protection, preservation and promotion of cyber security in the use of computers and communication devices.

c.Cloud Computing and Law:- With the growth in internet technology, the word is moving towards cloud computing. The cloud computing brings new challenges to the law makers.

The distinct challenges may include data security, data privacy, jurisdiction and other legal issues. There pressure on the cyber legislators and stakeholders would be to provide appropriate legal framework that could benefit the industry and enable effective remedies in the event of cloud computing incidents. . Cloud computing being a popular phenomenon among corporate is likely to bring forth issues like data protection and data confidentiality. The relevant stakeholders including lawmakers and governments across the globe need to provide appropriate legal, policy and regulatory framework pertaining to legal aspects concerning cloud computing.

d.Social Media and Legal Problems:- the social media is beginning to have social and legal impact in the recent times raising significant legal issues and challenges. A latest study indicates the social networking sites responsible for various problems. Since the law enforcement agencies, intelligence agencies target the social media sites, they are the preferred repository of all data.

The inappropriate use of social media is giving rise to crime like cyber harassments, cyber stalking, identity theft etc. the privacy in social media is going to be undermined to a great extent despite the efforts by relevant stake holders.

The challenges to the cyber legislators would be to effectively regulate the misuse of social media and provide remedies to the victims of social media crimes.

Social Media Litigations are also likely to increase concerning the association or nexus with the output of social media.

The litigation regarding defamation, matrimonial actions are popularly increasing and with the data, information resident on social media networking there is an emerging trend of various other litigations in the coming years.

e.Spam Laws:- There is considerable growth of spam in e-mails and mobiles. Many countries have already become hot spots for generating spam. As the number of internet and mobile users increase the spammers make use of innovative methods to target the digital users. It is therefore necessary to have effective legislative provisions to deal with the menace of spam. In the initial years, spam seemed to be targeted at computers but has now also targeted mobile phones. E-mail spam is the most common form of spamming. Mobile phone spam and instant messaging spam also exist. In majority of the countries there is no such anti spam law, which has led to the further growth of spam. There is an increased need for the countries to come up with regulatory and legal framework for spam as many countries have already become hotspots for generating spam.

Case study:-

1. Two managers of Chennai based Radiant Software a Computer Education Company were arrested for an alleged violation of the licensing terms of Software. The top management team had to obtain anticipatory bail to avoid arrests until a compromise was worked out.

2. Napster, a very successful E-Eenture was hauled to the Court and beaten to death for having caused violation of Copyright of music companies. Despite willing customs and working technology, the business of the company had to be shelved under an enormous loss to the promoters.
3. There are many websites in India which could be held to be infringing the Patent rights of somebody abroad and asked to shut down or pay compensation putting an end to their entrepreneurial dreams.

There are some of the trends in Cyber Law which are based on the analysis of emerging cyber law jurisprudence. With the growing pace of technology, it may not possible to overrule any new trend in the technology which might have direct or indirect impact on Cyber Law.

There may be various interesting and important challenging threats emerging in the jurisprudence of cyber law.

Combating Cyber Crime

Today world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyber attacks such as corporate security breaches, spear phishing, and social media fraud. Complementary, cyber security and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs as essential role in achieving our nation’s cybersecurity objectives by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. The Department of Homeland Security (DHS) works with other federal agencies to conduct high impact criminal investigation to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods and broadly share cyber response bests practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.

Conclusion

To conclude it is suggested that cyber crimes should be dealt under international crimes, similar to that of piracy under the law of seas, which may be tried internationally. However, the formulation of an international model law on cyber crimes could be one of the more practical approaches.

If you are designing computer software you actually are designing the core component that would create a Cyber World itself and all aspects of laws in Cyber World would be attracted to it.

Therefore, a Technologist working on computer or allied devices or networks needs to be equipped with the fundamentals of the laws surrounding these devices or systems. Ignorance of law is no excuse in the eyes of law.

The Information technology revolution has provided the opportunities for greater access to information and democratization of societies, this development has benefited not only legitimate users but those which seek to harm others on the personal and political level. Despite the progress being made in many countries, most terrestrial law to prosecute cyber crimes. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large scale economic and social effects. Self protection remains the first line of defense. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security. Firms, governments, and civil society should work cooperatively to strengthen legal framework for cyber security.

Reference

1.The Hindu, Page-16 dated. 21/11/2016.
2.The Hindu, Page-7 dated. 14/07/2017.
3.International Journal of Advance Computer Science and Application,
Vol.II, No.10,2011
4.http://www.cyberlawindia.com.
5.http://www.cyberlaws.net.
6.Law Profile, Vol.3, Issue-1, January 2012.
7.Law Z, Vol.11, No: 10, Issue 134, October 2012.