IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY OF CYBER LAWS AND ITS PERSPECTIVE

Dr D Sanjeeva Rao
Assistant Professor of Commerce,
Bhavan's Vivekananda College
Of Science, Humanities and Commerce,
Secunderabad

ABSTRACT

Law is set of rules. Cyber law is set of rules concerned with information technology. Since the beginning of civilization, human beings were always motivated by the need to progress by use of prevailing technology. Thereafter, this caused a tremendous development in the human race using the technology and advancing in every walk of life. It continues across the globe with varied approaches by way of facilitating, regulating and controlling commerce and allied fields by electronic communication. The maxim of ignorantia juris non excusat' aptly suits to the cyber law. The Parliament has passed Cyber Law, The Information Technology Act 2000 providing the legal infrastructure for all forms of electronic communication. The use of Information Technology has become the necessary of life. In this process some section of people are using the advancement of technology for unscrupulous practices and causing heavy damage to the society at large. The misuse of technology is also increasing at a great pace in the same manner as the technology is being used for the well-being of the society. The people involved in the cyber offences are investigated and punished as per the Information Technology Act, 2000. The individuals, institutions and corporate entities are protected by the provisions of Information Technology Act, at the same time they are taken to tasks in the event of wrong doing.

***Key Words**: Cyber Law, Offences, Punishment, Cyber Appellate Tribunal*

Introduction

The cyber laws are the laws governing the world of internet, which is also known as cyberspace. These laws cover the universal jurisdiction. All netizens use this space which comes under the sphere of the entire globe. Cyber law can be said to be that branch of law which deals with legal matters relating to the use of internet connected information technology. In other words, cyber law governs the Computers and internet. The growth and development of e-Commerce has launched the need for effective controlled mechanism which would frame a strong legal infrastructure for the success of e-Commerce sector. The mechanism and regulatory framework relating to the legal aspects come under the domain of cyber law. Cyber law plays a significant role because it touches all kinds of activities and transactions connected with computer and internet, World Wide Web. As per Newton's law for every action there is equal reaction, in cyber laws also for every cyber action there is equal reaction in the cyber space as framed under the cyber laws perspective and regulatory setup. Cyber Laws relate to Electronic and Digital Signature, Intellectual property, Data protection and privacy and cybercrimes.

World Wide Web and internet are interchangeably used in every walk of life. But both are not same. The global data communication network connected with software and hardware infrastructure between computers is Internet whereas Web is one of the services connected via internet. They are linked by hyperlinks and URLs (Uniform Resource Locators).

Need for the study

In today's environment every aspect has become more of techno-savvy and digital. Internet is used for Research and Development in every field. It has become a regular feature of sharing information by use of internet with respect to e-Governance, e-Commerce and e-Auctions etc. All legal matters concerned with these transactions are regulated by cyber laws. As the number of transactions and users are increasing on day-to-day basis the cyber laws play an important role. The need for Cyber Laws regulation and gained a momentum due to tremendous usage of internet.

Review of Literature

Advancement of technology paved way to rise of criminal activities and IT Act 2000 provides the ways to deal with the cybercrimes. Cyber law related issues cannot be solved overnight.

Maneesh Taneja and Dr. D.B Tiwari, (2010)" suggested that old laws are not replaced with new laws for the crime being committed. There is need to frame stringent cyber laws. Our system should provide for stern punishment so that criminal acts as a deterrent for other.

Aashish Kumar Purohit (2011) mentioned that there is need for the Cyber Security to protect the evolving ICT. The expert group should find and recommend suitable mix of solutions in critical ICT systems supporting the governance structure of the nation.

Yogal Joshi and Anand Singh (2013) considered that an Information Technology provision in the context of internet is vague. In the real world the evidences are tangible but in virtual world it is difficult to handle because of loss of evidences due to cyberspace and field of investigation in cyber crime has not gained a way to handle.

Ravikumar S. Patel and Dr.Dhaval Kathiriya.**(2013)** emphasized that though IT (amendment) Act 2008 tackles more even after its amendment IPC doesn't use the term 'cybercrime' at any point. After the year 2008 cyber crimes against individuals, property and government have increased as criminals discover loopholes within IT ACT and they perform the illegal activities.

Rohitk.Gupta, (2013) stressed on the territorial jurisdiction as the major issue which is not satisfactorily addressed in IT Act 2000. It is generally seen that the investigator generally avoids to take the complaints on the ground of jurisdiction

Prabhat Dalei and Tannya Brahme(2014) analysed that the Cyber crime is the one of the emerging trend of crime which has the prospective to destroy each and every aspect of the life as it is easy to commit but it's really hard to detect and often hard to locate in jurisdiction terms, given the geographical indeterminacy of the net.

M.M.Chaturvedi, M.P.Gupta and Jaijit Bhattacharya (2014) focused on the growth of the Indian cyber laws as it has not been achieved as all the faces which include E- courts, online dispute resolution functionality, good cyber law, cyber forensic etc. IT Act needs the revision. And there should be provision of scientific and technical professional training to lawyer in India.

Shubham Kumar et al. (2015) in "Present scenario of cybercrime in INDIA and its preventions" have discussed various categories and cases of cyber-crime which are committed due to lack of knowledge or sometimes due to the intention behind it. Writers have also suggested various preventive measures against these unlawful acts in day-to-day life. The paper starts with the data where Indian stands second top-most country in Asia in the number of cybercrimes according to International World Stats and Kumar's article/paper. Moreover, writers discussed what cyber-crime is in legal parlance. Furthermore, the paper deals with the types of cyber-crimes which include email-spoofing, phishing, identity theft, internet fraud, etc. Additionally, authors have also discussed present trends, cyber-laws in India, the penalty for damages, and basic practise for prevention.

Jigar Shah (2016) explained his work "A Study of Awareness about Cyber Laws for Indian Youth" about a conceptual model explaining how to uphold and implement the awareness programmes among internet users regarding cybercrimes. The writer starts with a brief introduction to the topic by providing statistics. Furthermore, Shah discusses the concept of cybercrimes by giving several definitions. Moreover, the paper talks about user awareness and then categories of cybercrimes. Additionally, Shah has analysed the data of every aspect.

Talwant Singh (2020) investigated the applicability of cyber law increased by IT Act (amendment) 2008. The definition part of evidence act was amended.

Statement of the Problem

In modern times, the internet usage has made the world as digitalized world and every individual, institution and organisation is affected by cyber law. Companies largely deal with their shareholders, online trading, with the help of computer network, let it be in respect of share transaction or payment of dividend. Consumers are using plastic cards for commercial transactions. Most of the population across the globe use cell phones, computers for their SMS and email to communicate. Even cybercrime cases are also evident in this process. Business transactions are replacing the conventional methods with e-Contracts and Digital signatures. Technology has brought the mercantile transactions as economical as the operations are carried at a fast pace. Cybercrimes such as online banking frauds, theft of information, virus attacks, and denial of service have increased. So an appropriate legal framework on a socio economic model is very much essential.

Objectives of the Study

1. To study the cyber law aspects of Information Technology Act, 2000
2. To study and analyse cybercrimes in various fields
3. To suggest remedial steps to overcome cybercrimes.

Scope of the Study

The present study covers the cyber crimes in various fields, investigation undertaken in the judicial process and the judicial mechanism to overcome the cyber crimes after framing the legal jurisdiction in Information Technology Act.

Methodology

The current study is based descriptive research analysis. To understand the nature and types of cybercrimes prevalent in society and how they are being addressed, the researcher felt it necessary to conduct detailed study.

Limitations of the Study

- The study does not cover all aspects of cyber laws.
- All kinds of cyber crimes are not included in the present study.
- Authorities of Information Technology are partly covered in the present study.

Cyber Law aspects of Information Technology

Cyber laws cover legal recognition of documents in e-Commerce and e-Trading activities. Cyber laws keep an eye on every activity over the internet. Cyber laws create rules for the individuals and companies to use the computers and the internet so as to protect people from being the victims of crime through undesirable activities on the internet. Cyber laws paved the way for the corporate entities entry for issue of Digital Signature Certificates.

Administrative Mechanism for Digital Signatures (Public Key Hierarchy or Infrastructure)

Controller of Certifying Authorities (appointed by Central Government)

Certifying Authorities

Subscriber (End User)

Figure 1: Hierarchy of Administrative Mechanism for Digital Signature Certificate.

Any person may make an application in the prescribed form to obtain Digital Signature Certificate to the certifying authority and it should be accompanied by prescribed fee framed by the central government. The digital signature certificate shall be granted only after the authority is satisfied about the information furnished by the applicant. Certifying authority shall also certify that it has fulfilled all other obligations relating to the security of public and private keys of the subscribers. The subscriber has to convey his acceptance of the digital signature certificate and its conditions in order to make it valid. A digital signature certificate is normally granted for one or two years after which it can be renewed.

Legal recognition of electronic records

Legal recognition of Digital Signatures

Electronic forms for dealing with government authorities

Mechanism of service providers by appropriate Govt.

IT Act facilitates e-Governance by providing for

Electronic retention of records

Audit of Electronic records

Publication of Electronic Gazette

Rules for Digital Signatures via Schedule II

Validity of e-Contracts

Fig 2: IT Act and e-Governance

Cyber Crimes

Cybercrimes are criminal activities committed by use of computers or internet.

Types of Cyber Crimes

Computer forgery: This kind of crime occurs as data is altered and processed in computerized records. However, machines may also be used as means to conduct forgery. The availability of computerized colour laser copies also created a new wave of dishonest modification or replication

Credit card fraud: Modern companies easily exchange cash with Automated Teller Machine, which causes computer based theft. Credit card identification and personal and financial credit card details are often targeted for organized crime.

Cyber Stalking: Stalking is defined as repeated acts of harassment directed at a victim, like following them, making harassing phone calls, murdering the victim's pet, vandalising their property, and leaving written messages or objects.

Cyber squatting: Most of the traders are involve in this kind of crime. Cyber squatting is by obtaining a domain name in order to collect payment from the owner of a trademark including a business name, trade name, or brand name, and it can also include typo squatting in which one letter is different either in brand name or trade name.

Cyber Defamation: Cyber defamation is defined as any negative statement intended to harm a person's company or reputation. Scandel can be used to defame someone. When defamation is carried out via computers and/or the Internet, it is known as cyber defamation.

Child Pornography: It is one of the most serious crimes. Abusers utilise the computers or Internet to reach out to and sexually abuse youngsters all around the globe. Criminals use their identities to provoke children into their traps, including contacting, steal personal data from their helpless children. These criminals lure children onto the internet in order to sexually attack them or exploit them as a sex object.

Denial of service attack: Sometimes the service provider by using computers power assault, which contributes to server denial of access to other machines. There are numerous methods used by hackers to download a server.

Data diddling: It involves altering raw data prior to the processing done by the computer and then changing it back after the processing is completed.

Data Driven Attack: A data-driven attack is a concern to system administrators as it may get through the firewall in data form and influence an attack against a system located behind the firewall.

DNS Spoofing: A type of spoofing that takes use of the Domain Name Service, which allows networks to translate textual domain names to the IP numbers used to route data packets.

Electromagnetic intrusion: It is the deliberate insertion of electromagnetic energy into transmission paths in order to confuse or deceive operators..

Email bombing: It is another kind of crime by sending massive amounts of mail to a victim, which could be an individual, an organisation, or even mail servers, causing the system or network to fail.

Hacking: Hacking is unauthorized computer access and the modification of the computer so as to enable continued access, as well as a change of the target machine set-up, without awareness of the system owners.

Phishing: Modern companies simply exchange cash with Automated Teller machine which causes computer theft.

Spoofing: In this kind of crime the machines are accessed through the network with unique access.

Threatening: The pseudo sends abusive emails or contacts the survivor in chat rooms.

Virus / worms attacks: Viruses are programmes that attach themselves to a computer or a file, and then spread to other files and computers on a network.

These kind of crimes have become very common and disturbing the whole system of administrative activity. The investigator can find this kind of criminal activities by the suspect after the event takes place. Therefore, the Information Technology applied to the government functioning by creating SMART governance.(Simplicity, Moral, Accountable, Responsive and Transparent) .The above shown figure clarifies as to how the provisions of Information Technology facilitates the e-Governance. Sailesh Kumar Zarkar, Technical Advisor and Network Security Consultant to the Mumbai Police Cyber Crime Cell, advocates the 5P mantra for online security viz., Precaution, Prevention, Protection, Preservation and Perseverance.

Conclusion

What looks neat today may not be so tomorrow. Because the world is changing with cyber attacks and cyber crimes. By adopting the Information Technology Act and its mechanism would bring down the criminal activities. The concerned authorities and Police have been given wide powers so as to combat the criminal acts. The simple way to stop crime is bringing awareness and education among the internet users and heavy punishment for such crimes. In India, the laws change from to time based on the level of crimes and the magnum of its impact. The laws must be so strong that even the user should be thinking of his changed life is miserable.

Suggestions

To start with, IT Act (amendment) Act 2008 considerably reduced the quantum of punishments for a vast spectrum of cybercrimes, this needs to be rectified and furthermore a bulk of cybercrime needs to be made a non-bailable offence. This shall be done in order to establish a deterrence effect in the minds of the criminal mass.

2. Furthermore, the legislation should include all the terminologies and various kinds of cybercrimes are required to be updated.

3. The ambiguity in respect of legal jurisdiction should be clarified in order to facilitate the enforceability towards cybercrime.
4. Rigid and suitable guidelines should be applicable towards the protection of user data in all commercial sectors as well as telecom industries.
5. Finally, a well-structured organisation of cyber forensics should be setup throughout the country with updated hardware and software facilities.

References

Aashish Kumar Purohit, (2011) “Role of Metadata in Cyber Forensic and Status of Indian Cyber Law”, International Journal of computer technology application, vol.2 (5) Sep/Oct, 2011.

IDSA Task Report, (2012) “India’s cyber security challenged” March, 2012

M.M. Chaturvedi, M.P.Gupta and Jaijit Bhattacharya “Cyber Security Infrastructure in India: A Study”pp.1-15

Maneesh Taneja and Dr. D.B Tiwari, (2010) "Cyber Law", International Referred Research Journal, vol.11 (21) October, 2010, pp. 63-65.

Prabhat Dalei and Tannya Brahme,(2014) “Cyber Crime and Cyber law in India: An Analysis” ‘International journal of humanities and Applied science’ Vol.2 (4), 2014.

Ravikumar S. Patel and Dr.Dhaval Kathiriya,(2013) “Evolution of Cybercrimes in India” International Journal of Emerging Trends & Technology in Computer Science, vol.2 (4) July – August 2013.

Rohitk.Gupta,(2013) “An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective”, 2013.

Rohit k Gupta,(2013) “An Overview of Cyber law vs. Cybercrimes”, 2013.

Talwant Singh, “Cyber Law and IT” pp. 1-4

Yougal Joshi and Ananda Singh, (2013)A Study of Cyber Crime and Security Scenario”, International Journal of Engineering and Management Research, vol.3 (3) June, 2013, pp.13-18.