Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
ISSN : 2395-7069 General Impact Factor : 2.4668, Volume 04, No. 03, July-September, 2018, pp. 25-27

CYBER CRIME: A LEGAL PERSPECTIVE

Nishant Chaudhary[*]
Dr. Nidhi Mehta[**]

ABSTRACT

Cyber crimes are recently developed on a rapid scale due to wide and deep penetration of internet. The IT (Information Technology) Act 2000, and its amendment in 2008 along with several other policies and laws are unable to provide protection to people from cyber crime in large population country like India. We need to create awareness and capacity building among masses for achieving efficient and effective results. This paper contributes in helping to understand the capability of current laws in dealing with cyber crime, their loopholes and what is the way forward to fix the loopholes so that a better crime-free society could be established.

KEYWORDS: *Digital literate, Online Shopping, Social Media, Online Privacy.*

Introduction

Where the risk is low and rate of return investment is high, people always take the advantage of this type of situation and due to this cyber crime takes shape[1]. Moreover, the invisible nature of crime makes it difficult to find criminal, due to this cyber crime is increasing day by day. In India, there are several factors which are responsible for increasing the rate of cyber crime such as widespread poverty, huge unemployment, eagerness to make quick money among youth, lack of awareness among people, loopholes in laws, lack of trained officials in investigating agencies, etc. Therefore, law enforcing agencies must have proper training and awareness regarding different forms of cyber crime. For the same purpose Information Technology Act was enacted in 2000 and it was later amended in 2008 for incorporating certain changes of cyber space.

What Is Cyber Crime?

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials.

Emergence of Information Technology Act, 2000

Cyber crimes are recently developed on a rapid scale due to wide and deep penetration of internet. People to fulfill their interest sometimes use illegal and dishonest means. Cyber crime is preferred by these people due to its inherent advantage like crime could be committed anywhere in the world by just sitting in the room. Rapid increase in online shopping, wide use of social media like facebook, whatsapp, etc , online banking, etc is the basic cause of cyber crime exponential growth in last few years. In spite of this people are hesitant to report cyber crime to authorities. Even if someone complaint then cyber cell of police is hardly efficient enough to resolve such issues. This is a very complicated situation and required to be dealt with immediate and concrete action.

[*] Research Scholar, Department of Sociology, University of Rajasthan, Jaipur, Rajasthan, India.

[**] Research Supervisor & Assistant Professor, Department of Sociology, University of Rajasthan, Jaipur, Rajasthan, India.

The law IT (Information Technology) Act 2000 was enacted to deal with emerging challenges of cyber crime along with several other policies and rules, but rapid changes in technology and great expansion of internet poses a challenge in large population country like India to control cyber crime. We need to create awareness and capacity building among masses for achieving efficient and effective results.

How to prevent Cyber Crime

Rapid and deep penetration of internet have made life much easier like online shopping, online banking, e-services, etc but it also created number of security problems such as by just clicking one button money from bank account could be theft. Thus, there are some methods of information technology to prevent cyber crime and making people digitally literate.

Various Common Measures to Control Cyber Crime

- **Encryption:** This is a common and widely used method to prevent data theft. In this method plain text can be converted to cipher text and the recipient could decrypt it again into plain text by using a code. In this manner only the sender and recipient could have access to data and no outsider could access to it.
- **Syncronised Passwords:** The passwords are created, and are only valid for very short duration. They can be used for one time login. Some other methods are voice recognition, digital signature, biometric, etc.
- **Firewalls:** It creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed. It would only let the data to flow in computer which is recognised and verified by one’s system. It only permits access to the system to ones already registered with the computer.
- **Digital Signature:** Are created by using means of cryptography by applying algorithms. This has its prominent use in the business of banking where customer’s signature is identified by using this method before banks enter into huge transactions[6].

Problems Underlying Tracking of Offence

Mostly in cyber crime the main problem is to identify the person involved in crime. The law enforcement agencies find it difficult to trace the identity of criminal on their own and they require cooperation of governments, various institutions, etc. There is not a established mechanism to ensure coordination among various agencies. This situation got even more worse when certain institutions lack necessary skill and knowledge to deal with cyber crime

How much Information Technology Act 2000 is capable of curbing cyber crime?

The Information Technology Act is the main law dealing with cyber crime in India. Though there are other provisions also like in Indian Penal Code and other rules but this is the Act which is enacted to specifically deal with cyber crime. This Act was amended in 2008 to incorporate certain new provisions to enhance its efficiency. But despite of all this effort still cyber crime is increasing at a rapid pace. There is grave under-reporting of cyber crimes in the nation. Cyber Crime is committed every now and then, but is hardly reported. The cases of cyber crime that reaches to the Court of Law are therefore very few. There are practical difficulties in collecting, storing and appreciating Digital Evidence. Thus the Act has miles to go and promises to keep of the victim of cyber crimes. It is a fact that Information Technology Act, 2000 though provides various types of safeguards but is doesn’t provide complete safety against cyber crime. For instance, according to the Indian Computer Emergency Response Team (CERT-In) there were 34 incidents of Wannacry and Petya ransomware in 2017.

Conclusion and Suggestions

Awareness, guidance and counseling may contribute effectively in minimizing cyber crimes and online frauds. We need to bring “change” in people who are already involved in such illegal activities through enforcing strict laws and reforming them by humanistic approach. The importance of internet in today’s world is very high and we cannot imagine our life without it. But cyber criminals have taken advantage of this situation and trying to exploit for their gain. To control their activities, the Information Technology Act 2000 came into existence but rapid changes in techniques and methods of criminals keep on creating new challenges. The Act needs to be updated periodically to cope up with emerging challenges of online world.

There is an urgent need take some measures such as making people digitally literate, ensuring coordination among various agencies dealing with cyber crime, improving expertise by providing training and appropriate exposure to staff of these agencies, etc. There is also need of a collaborated and concentrated effort at global level to frame a law which is applicable to every person on the globe which is efficient and effective to deal with cyber crime all over the world.

In the upcoming years internet is going to play a major role in our life. In our day to day activities we are going to depend more and more on internet. So the increase use of technology will also lead to increase in crime rate. The cyber crime cases have to be dealt firmly in order to create a crime free society. For the same, not only laws related to cyber crime must be strengthened and updated but also they need to be implemented in letter and spirit through competent law enforcement agencies in a digitally literate society.

References

- A. rashtogi, Cyber Law, Information Technology Act 2000. 1st ed. Lexis Nexis; 2014. p. 1-17.
- Barkha, Mohan UR. Cyber law and crimes. IT Act 2000 and Computer Crime Analysis. 3rd ed. 2011, p. 1-8.
- Dileep Vangeskar, 'Cyber crime & Law', 1st ed., 2002, Concept Publications, New Delhi.
- H.D.Sankhalia & Himani Rajdor, 'Cyber Crime a Challenge', 1st ed., Sage Publication, New Delhi
- Information Technology Act 2000. 2017. Available from: http://www.dot.gov.in/act-rules/information-technologyact-2000
- International Journal on Cyber Law and Cyber Crime Communication. 2014 Sep; 2(9):1-4.
- Suresh sharma & Hanuma singh, 'Cyber Crime & India', 1st ed., 2002, Delhi.
- Swati Singh, Cyber Space and Cyber Crime, 2nd ed.,2008, p-2-5, Delhi
- http://www.legalserviceindia.com/article/l146-Cyber-Crime-And-Law
- https://www.thehindu.com/opinion/lead/The-new-war-on-piracy/article14587200

❑❑❑