IMPACT OF SOCIAL NETWORKING ON CYBER CRIMES : A STUDY

-Dr. Rekha Pahuja

ABSTRACT

The Internet is a worldwide electronic computer network that connects people and information. But every technology has its own advantages and disadvantages. Internet has several advantages but it is considered as a heaven for cyber criminals. Social Media is the latest form of media available to the audience of varied groups, ages and classes. The major reason behind its popularity is that the users are given a free service to create a virtual social world where they exchange photographs, play games, become friendly, fall in love, split, fight, argue and quarrel at many times without having met physically. But, on the other side it is an encroachment to someone's privacy which can lead to different type of illegal activities by using the information such as name, location, and email addresses. The anonymity over the internet and the jurisdictional issues has given rise to cyber crimes where crime is committed with the aid assistance of computer.

KEYWORDS

Internet, cyber criminals, cyber crimes, Social Media, Awareness, Challenges and   Prospects

RESEARCH PAPER

INTRODUCTION:

Cybercrime, computer crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, and target poor place of a crime. Cyber crime is broadly used term to describe criminal activity committed on computers or the Internet. Cyber crime is a criminal activity involving an information technology infrastructure, including illegal access, illegal interception, data interference, system interference, misuse of devices and electronic fraud. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which causes breach of rules of lans and counter balanced by the sanction of the state.

Social media such as face book, what's app, Messenger etc provide users a platform to express themselves without any restrictions which is becoming a major challenge as it may infringe the fundamental rights of privacy of a human being.

The paper attempts to focus on nature of cyber crimes, use of social networking for the purpose of committing cyber crime and elementary problems associated with cyber crimes.

OBJECTIVE:

The objectives **o**f the study inter alia include the following:

- To study the meaning and nature of cyber crime.
- To identify the various forms of social media.
- To analyze the role of law to identify and prevent cyber crime with the use of social media.
- To create awareness amongst the youth of the nation about the consequences of cyber crime.

RESEARCH METHODOLOGY:

The researcher has used doctrinal method of research for collection of data.

MEANING AND NATURE OF CYBER CRIME:

Cybercrime simply describes the criminal use of computer technology. In other words any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

Donn Parker defines computer crime as, "a crime in which the preparatory uses special knowledge about computer technology"

Computer crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of crime.

Encyclopedia Britannica defines cybercrime as, "any use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing, identity or violating the piracy."

NATURE OF CYBERCRIMES

The peculiar characteristics of cybercrimes are as follows.

- The weapon with which cybercrime are committed is technology. Cybercrimes are the work of technology and thus cyber criminals are technocrats who have deep understanding of the Internet and Computers.

- Cybercrime is extremely efficient i.e., it takes place in real time. It may take seconds or a few minutes to hack websites or do cyber frauds.

- Cybercrime knows no geographical limitations, boundaries or distances. A cyber criminal in the one corner of the world can commit hacking on a system in other corner of the world.

- The act of cyber crime takes place in cyberspace which makes the cybercriminal being physically outside cyberspace. All the components of cyber criminality from preparation to execution, take place in the cyber space.

- Cybercrime has the potential of causing harm and injury which is of an unimaginable magnitude. It can easily destroy websites created and maintained with huge investments or hack into websites of backs and the defense department's websites. The amount of loss which may cause is easy to be imagined.

- It is extremely difficult to collect evidence of cybercrime and prove the same in the court of law, due to the anonymity and invisibility of cybercriminal and its potential to affect in several countries at the same time, which are different from the place of operation of the cyber criminal.

FORMS OF SOCIAL MEDIA -

Social Networks - Services that allow you to connect with other people of similar interests and background. Usually these consist of a profile, various ways to interact with other users, ability to setup groups, etc. *The most popular amongst them are face book,* whatsapp, instagram, linked-in, via Skype, Yahoo Messenger, Google Talk and so on.

Bookmarking Sites - Services that allow you to save, organize and manage links to various websites and resources around the internet. Most allow you to "tag" your links to make them easy to search and share.

Social News - Services that allow people to post various news items or links to outside articles and then allows it's users to "vote" on the items. The voting is the core social aspect as the items that get the most votes are displayed the most prominently. The community decides which news items get seen by more people. *The most popular are Digg and Reddit.*

Media Sharing - Services that allow you to upload and share various media such as pictures and video. Most services have additional social features such as profiles, commenting, etc. *The most popular are YouTube.*

Microblogging - Services that focus on short updates that are pushed out to anyone subscribed to receive the updates. *The most popular is Twitter.*

Blog Comments and Forums - Online forums allow members to hold conversations by posting messages. Blog comments are similar except they are attached to blogs and usually the discussion centers around the topic of the blog post. *There are many popular blogs and forums like RSS Feeds.*

USE OF SOCIAL MEDIA AND CYBER CRIME AND THE LAW IN INDIA:

Every sixth cybercrime in India is committed through social media, Alok Mittal, the chief of the National Investigation Agency (NIA) has said. As we know that India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Acts .The various offences which are provided under this chapter are shown in the following table: -

Offence	Section under I.T. Act
Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

COMPUTER RELATED CRIMES COVERED UNDER IPC AND SPECIAL LAWS

Offence	Section
Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec 463 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 463 IPC
Web-Jacking	Sec. 383 IPC
E-Mail Abuse	Sec.500 IPC
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

ELEMENTARY PROBLEM ASSOCIATED WITH CYBER CRIMES:

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law anywhere in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

- Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyber space the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under S.16 of Cr.P.C. and

S.2.of the I.P.C. will have to give way to alternative method of dispute resolution.

- Loss of evidence is a very common & expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.

- Cyber Army: There is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end.

- Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

- Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the P.I.L. (Public Interest Litigation), which the Kerala High Court has accepted through an email.

CONCLUSION:

Thus, after analyzing all the above facts and circumstances prevailing in our country, it can be said that there is a need to bring changes in the Information Technology Act to make it more effective to combat cyber crime. Also India should have proper technology to beat the cyber criminals in all aspects. At the same time, media being the fourth pillar of democracy should play a positive role by creating social awareness amongst the people about the careful use of social networks and there by not falling prey to cyber crime. There is a need to unite together and fight with silent violence.

REFERENCES

Pankaj Muthe & AT Kearney report, 2012

http://www.thehindu.com/news/cities/Delhi/article2391856.ece Accessed on 25th, January, 2012

Dr. Vipul Partap, and Rahul Mittal, an article on "Impact of social media on society and cyber law", in academia.edu Also available at :https://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW

Boyd, Danah (2006). "Friends, Friendsters, and MySpace Top 8: Writing Community into Being on Social Network Sites".

White, D.S.; Le Cornu, A. (2011). "Visitors and Residents: A New Typology for Online Engagement".

Steyer James (2009), "Is Technology Networking Changing Childhood?'- A National Poll by Common Sense Media, San Francisco.

Fraser, Matthew; Dutta, Soumitra (2008). Throwing Sheep in the Boardroom: How Online Social Networking Will Transform Your Life, Work and World. Wiley. ISBN 978-0470740149.

C. S. Ramanigopal,G. Palaniappan & N. Hemalatha (IJRMEC Volume2, Issue 2(February 2012) social networking: problems and prospects of the knowledge society. Issn: 2250-057x

Madhur raj jain, palak gupta & nitika anand (journal of arts, science & commerce , vol.– iii, issue 2(2), april 2012) impact of social networking sites in the changing mindset of youth on social issues   - a study of delhi-ncr youth . E-issn 2229-4686   & issn 2231-4172 Http://www.hindustantimes.com/india-news/every-sixth-cybercrime-in-india-committed-through-social-media-nia/story-kscgnwjctz0pzvevaoin6m.html

www.scbatch.mit.edu

Frozen planet - http://www.open.edu/open learn

http://www.academia.edu/1807785/Report_on_cyber_crime_on_socila_networking_sites

http://cybercrimes09.blogspot.in/2009/10/types-of-cybercrime.html

https://www.optimum7.com/internet-marketing/social-media/dangers-of-social-networking-sites.html

ABOUT THE RESEARCHERS

Dr. Rekha Pahuja

Asst. professor,

S.S.Maniyar Law College,

North Maharashtra University, Jalgaon