ORIGINAL RESEARCH PAPER

Law

KEY WORDS: Cyber crime, Hacking, Internet, Cyber defamation, Issues, challenges and Awareness

CYBER CRIME AGAINST WOMEN IN INDIA: ISSUES AND CHALLENGES

Dr. Sukanta Kumar Dwibedi Principal, Mayurbhanj Law College, Takatpur, Baripada, Odisha.

Mrs. Lora Aptaprava Lecturer, Mayurbhanj Law College, Takatpur, Baripada, Odisha.

ABSTRACT

In the present era many of the things are done usually over the website starting from online dealing to the online transaction. It is observed that Indian society women are the real victims of cyber crimes. Since the internet is considered as worldwide stage, anyone can access the resources of the internet from anywhere. Since crime against women is on a meteoric a woman rise in all fields, being a victim of cybercrime could be most traumatic experience for her. The internet technology has been used by less number of people for criminal activities like unauthorized access to other's network, scams etc. These criminal activities or the offense/crime related to the internet is termed as cyber crime. In order to block or to punish the cyber criminals the term "Cyber Law" was introduced. We can consider cyber law as the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, including many subtopics relating to freedom of expressions, access to and utilization of the Internet, and online security or online privacy.

The internet in India today is growing very rapidly and opened new opportunities and chances in every field like – entertainment, business, sports, health and education etc. But like a double-edged weapon it can be used or misused, the biggest demerit being the Cyber-crime. In India most of cyber-crime issues are committed by educated youths (some cyber – crime requires skills). So, it is required to have intensive knowledge about the cybercrime and its prevention. Also, in India many of the cases found and, crimes committed because of lack of knowledge or by mistake. This paper attempts to state the issues and challenges of cybercrime in India and also various types of cyber crimes that can be imposed upon a women and how they adversely affect them.

INTRODUCTION

Computer has made human life easier today being used for various purposes starting from the individual to big organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/ process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their own motives and personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. It doesn't have a constant definition, but in a simple term we can defined it as the law that rules the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are appreciated by the Cyber Law .The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce".

The internet supports us in gaining knowledge as well as storing our data. It has become so pivotal that it has become an important part in human's lives. However, due to the rapid increase in our modern technology, it has become very tough in keeping our personal private information safe. Classified data are becoming easily available to people. This has lead to the increase in crimes as practically anyone can access one's personal data without the victim's consent. Website has become a relief for the modern age, yet it also causes a burden on the person and society as well.

The Internet has also propogate a new kind of crime; cyber crime. Common internet users are unaware of cybercrimes. They are unaware of the proper precautionary measures to stop such attacks from taking place. Many individuals have been victims to cybercrimes around the world. For a cybercrime to occur, the criminal only requires a computer and access to internet. Cybercrimes have led to the creation of hacking, identity theft, Credit/debit card frauds, cyber terrorism and other hard core crimes. Cybercrimes can happen to anyone if their data is stored in the network.

OBJECTIVES

1. This paper aims at dealing with the meaning of cyber crime.
2. To analyse crime against women through cyber laws.
3. To examine different types of cyber crimes against women.
4. To trace out the different trends and challenges of cyber crimes within India.
5. To examine the various cyber laws towards the protection of cyber crimes.

RESEARCH METHODOLOGY

Looking into requirements of the objectives of the study the research design employed for the study is of descriptive kind. Keeping in view of the set objectives, this research design is adopted to have higher accuracy and comprehensive analysis of the research study. Available secondary data is broadly used for the study. The methodology is based on various sources of data. The data has been taken from the research outputs, articles, media reports, Journals, books, and periodicals for this study.

CONCEPT OF CYBER CRIME

Cybercrime cannot be discussed in a single definition, it is well considered as a collection of acts or conducts. These acts are based on the material offence object that hampers the computer data or systems. These are not legal acts where a digital device or information system is a medium or a goal or it can be the mixture of both. The cybercrime is also considered as electronic crimes, computer-related crimes, e-crime, high-technology crime, information age crime etc. The unusual feature of cybercrime is that the aggrieved and the offender may never come into face-to-face contact. Cybercriminals often choose to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution. Cyber crimes are technology based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes.

TYPES OF CYBER CRIME AGAINST WOMEN

Hacking

Among the all types of cybercrime it is the most dangerous and serous thread to the internet and e-commerce. Hacking

means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking.

Cyber Pornography
It is the most risky threat to the women in the society. This would include pornographic websites or pornographic magazines produced using computers to publish and print the material and the internet to download and to circulate pornographic pictures, photos, writings etc. Internet has provided a mechanism for the facilitation of crimes like pornography, especially cyber porn.

Web Hijacking
In this crime the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link.

Data Diddling
This type of an attack involves changing raw data just before it is processed by a computer and then transforming it back after the processing is over.

Cyber Stalking
In general terms, stalking can be termed as the repeated acts of harassment targeting the aggrieved such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects.

Morphing
Editing of the original picture by unauthorised user or fake identity is termed as morphing.

SMS Spoofing
Spoofing is a blocking through spam which means the unwanted uninvited messages. In this case, an offender sends out fake messages to the victim to steal his identity and private data such as bank information. SMS Spoofing allows changing the name or number text messages appear to come from.

Online Harassment
It involves sending harassments letters, messages etc. via emails. Such kind of cyber crime normally occurs in social media.

Financial Crimes
This would include cheating, credit card frauds, money laundering etc. Financial crimes are punishable under both IPC and IT Act.

Phishing
Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering personal data that will be used for identity theft.

Virus Attacks
Viruses are the programs that have the capability to infect other programs and make copies of it and spread into other program. Programs that multiply like viruses but transmit from computer to computer are called as worms.

E-Mail Spoofing
It refers to sending false emails to random internet users with false sender address. Email spoofing is a method used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are changed to appear as though the email originated from a source other than its original source.

Cyber Defamation
Cyber tort including libel and defamation is another usual crime against women on the internet. Cyber defamation means the harm that is brought on the fame and name of an individual in the eyes of other individual through the cyber space. The aim of making derogatory statement is to bring down the reputation of the person.

Salami Attacks
Salami attacks are used for the commission of financial crimes. The other name of Salami attack is Salami slicing. In this attack, the attackers use an online database in order to seize the customer's data like bank details, credit card details etc.

ISSUES AND CHALLENGES OF CYBER CRIME IN INDIA

Cyber crime is no longer an illusion. The situation could go out of hand if computer users, both in government and the private sector. For the police, the temptation especially to view attacks on computer systems, as just another form of crime is great. Three aspects of cyber crime deserve focused attention. These are

- The legal measures that are provided
- The sufficiency of training of prosecutors and the judiciary and
- The nature of links forged by the Indian police with foreign law enforcement agencies so that cooperation in matters of inquiry and investigation.

Cyber crime does not acknowledge national borders. More than 30 countries have separate laws in their statue book to check this hazard. There is lack of awareness and the culture of cyber security, at individual as well as organizational level. Further there is also lack of trained and qualified manpower to implement the counter measures. The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the base of these cyber-crimes. Promotion of Research & Development in ICTs is not satisfactory. Cyber attacks have come not only from terrorists but also from neighbouring countries contrary to our National interests. No systematic effort has been made till now to provide training to prosecutors and judges, although there is evidence of their keenness to become knowledgeable. Policing in cyber space was a challenging job.

Present protocols are not self reliant, which identifies the investigative responsibility for crimes that stretch internationally. Security forces and Law enforcement personnel are not furnished to address high-tech crimes. Budgets for security aim by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compared to other crimes. The Indian penal code is so well drafted that offences not listed in the IT Act right now can still be tackled through it, till such time we are convinced that the IT Act needs to be recast in order to cope with the expanding contours of cybercrime.

CYBER LAWS AGAINST CYBER CRIMES

IT Act of India, 2000
The IT Act of India was passed by the Indian Government in May 2000 that states the various cyber laws of the state. It is the law that deals with cybercrime and e-commerce. The Act was based on the United Nations Model Law on Electronic commerce. The Act furnishes to provide legal structure for all electronic transactions in India. Chapter IX of the Act states about the different punishment for cybercrime offences.

The Indian Penal Code, 1860
Under Indian Penal Code it is a very powerful legislation and probably the largest used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended several time since, it covers almost all substantive aspects of criminal law and is augmented by other criminal provisions. In independent India, most special laws have been sanctioned with criminal and penal provisions which are often referred to and relied upon.

The Bankers' Books Evidence Act, 1891

Banker's Books Evidence Act has been included as the third schedule in ITA. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy kept in the court records as exhibits.

The Indian Evidence Act, 1872

This is another legislation amended by the ITA. Before passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it. In the definitions part of the Act itself, the "all documents including electronic records" were replaced. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

SUGGESTIONS AND RECOMMENDATIONDS

1. Government should conduct awareness campaigns in different places of the state to bring awareness among the people.
2. All the website users, mostly women, who are more prone to be the victims of cyber- crimes, should not share their private information to the general public.
3. Social networking sites like face book, instagram, should maintain the privacy limit on their information and photos.
4. The women should immediately report to the cyber cell of police and seek for sudden actions.
5. Women should be more careful in adding strangers in their friend list.
6. Internet users are recommended to use strong and unique passwords for their social media websites.
7. There is need to maintain the most current anti-virus software program and install updates for the system.
8. There is also need to develop the development of investigative and analytical resources to identify and inquiry inter-related crimes in all states of the country.
9. The cyber cells also must provide aid and relief to the people who have lost money due to cybercrime scam. The less accessible their private information and photos will be, the more safe they are, behind the screens.
10. It is recommended that people install intrusion detection software so as to provide a warning to the user regarding any breach.
11. Justice delivery should be quick and effective.
12. Internet users and businesses must back up their information daily so as to avoid data loss.
13. There is need to guide not only younger children's internet habits, but also of teens. Youths are more likely to get into difficult online than younger kids.

CONCLUSION

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent years. Cybercrime has constitute great threats to mankind. Protection towards cybercrime is an important part for social, cultural and security aspect of a country. It has great eventuality and thus creates high impact when it is done. To minimize and protect cyber crime against women or to be precise, to protect their modesty being outraged through the medium of internet, the Indian legal system needs to come up with some amendments in the current statutes, both in Information technology Act, as well as in IPC, to define and punish for such activities hindering women at large in the society. It is quite easy to commit without any physical existence required as it is global in nature for which it has become a challenge and threat to the crime fighter and vice versa. With the ongoing advancement of technology, kinds of cyber crimes are taking place. Notwithstanding, there is no agreed concept of the cybercrime, it is inevitable. Technology-based crimes have been developing with the passage of every day and they need to be work out with utmost priority. It is a good thing that Government of India has enacted IT Act, 2000 to hand out with cybercrimes.

REFERENCES

1. Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.
2. Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India
3. Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India
4. Cyber Crime in the Society: Problems and Preventions Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, 240-259
5. Nagpal, R. (2008) Evolutions of Cybercrimes, Asian School of Cyber laws.
6. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.
7. Muthukumaran, B. (2008) 'Cybercrime scenario in India', criminal investigation department review, Chief Consultant, Gemini Communication Ltd., p. 17
8. Pillai, (2008). 'Govt. framing norms for social infrastructure in SEZs', The Economic Times,
9. Sheakh Taraq Hussain (2012), "Cyber Law: Provisions and Anticipation Vol. 53, Sep, pp. 10-12.
10. Singh Talwant , (2011) Cyber Law & Information Technology, New Delhi, India.
11. Suri and Chhabra, (2003) Cyber Crime Pentagon Press, New Delhi, India.