declaration of the deceased corroborated by other witnesses. The prosecution has indeed failed to establish that the deceased eventually died on account of injuries sustained by him resulting in the acquittal of accused persons under Section 302 IPC, but that part of the order passed by the Courts below does not warrant rejection of the prosecution case in to procedures laid down for deprivation thereof must be scrupulously complied with[19].

False Implications Possible

False implications in faction cases is always possible. *Dunnapothula Kistaiah v. State of Andhra Pradesh*[20], is a faction case. It was observed that there was possibility of deliberations and false implications and in such cases delay in lodging the first information report plays a vital role.

Conclusion

Factionalism violates human rights of not only the victims but has far reaching consequences adversely affecting the lives of the dependants of factionists. It is beset with violence, fear and gruesome actions which are undesirable in a civilized democratic process. It hinders the development process as there would be no unity.

Though it has been undisputed that the participants in the faction crimes got political leadership and or affinity with the political parties, the Courts have not passed any orders to prevent the factionalism through the political parties. The Court may consider invalidating the political party from participating in the elections for their involvement in the criminal cases whenever its members are proved involved in the faction crimes.

Therefore, factionalism is a vicious, inhuman and heinous activity shall be condemned and eradicated by all the sections of the society especially the political parties. The State machinery must take stern and unbiased actions in curtailing this social menace. The Judiciary might ensure that the culprits would never escape by shifting the burden of proof to the accused whenever there is *prima facie* evidence of factionalism on the part of the accused.

19. *Ibid*

20. Decided on 3 November, 2008 The Hon'ble Justice *Gopalakrishna Tamada* of Andhra Pradesh High Court, http://Www.Indiankanoon.Org/Doc/1670234/

CYBER CRIMES IN INTERNET – A STUDY

By

–P. SAILAJA

Hyderabad, A.P.

Introduction

It is important to know the past, present, future conditions of cyber crimes on internet. It is only an attempt is being made to study the trends of cyber crimes on Internet and to make an analysis.

I quote an interesting article by *Nandini Ramprasad* for the benefit of our netizens. "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may able to do more damage with key board than with a bomb."

In India internet is growing rapidly. It has given rise to new opportunities in every field, education, business, and sports. The study is important to know the past, present and future conditions of crimes in internet. Various criminal activities in cyber world by an unknown human causing damage not only individual but to countries. The internet crimes not only in India, but also secure

countries like US, UK, China. The internet are misused for illegal activities like e-mail, credit card fraud, spam, piracy.

In developing countries like India the importance of internet users are rapidly growing while other countries like USA, UK, China finding solutions and punishing the criminals.

Internet in the Country – Present Position

India has recorded and has been recording substantial growth of internet users, individual as well as corporate entities. It has exploded plethora new opportunities in every field, *viz*,, education, business, sports, historical studies, monitoring and analysis of data, information and public relations, broadcasting *etc.* As there are two sides to a coin, internet also has its own advantages and disadvantages. One of the major disadvantages in internet is Cyber-crimes. The internet crimes are not only in India, but also in advanced countries like US, UK, China, *etc.*

Various Types of Cyber Crimes – Are

Cyber crimes have been classified on the basis of the nature and purpose of the offence and have been broadly grouped into three categories depending upon the target of the crime.

Against Individuals – their person/their property

Against Organization – against Government/ a firm, company/a group

Against Society at large — The following are the crimes, which are in general committed against the followings

Against Individuals :—

(i) Harassment *via* e-mails.

(ii) Cyber-stalking.

(iii) Dissemination of obscene material.

(iv) Defamation.

(v) Unauthorized control/access over computer system.

(vi) Indecent exposure

(vii) Email spoofing

(viii) Cheating & Fraud

Against Individual Property :—

(i) Computer vandalism.

(ii) Transmitting virus.

(iii) Netrespass

(iv) Unauthorized control/access over computer system.

(v) Intellectual Property crimes

(vi) Internet time thefts

Against Organization :—

(i) Unauthorized control/access over computer system

(ii) Possession of unauthorized information.

(iii) Cyber terrorism against the Government organization.

(iv) Distribution of pirated software *etc.*

Against Society at large :—

(i) Pornography (basically child pornography).

(ii) Polluting the youth through indecent exposure.

(iii) Trafficking

(iv) Financial crimes

(v) Sale of illegal articles

(vi) Online gambling

(vii) Forgery

A cursory look at various types of cyber crimes—

Harassment via e-mails – Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Recently I had real in a news paper, a lady wherein she complained about the same. Her former boy friend was sending her mails constantly sometimes emotionally blackmailing her and also threatening her. This is a very common type of harassment *via* e-mails.

Cyber-stalking – The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following

* a person's movements across the Internet by posting messages
* threatening on the bulletin boards frequented by the victim,
* entering the chat-rooms the victim, constantly bombarding the victim with e-mails *etc.*

Obscene material/Indecent exposure/Pornography (basically child pornography)

* It may include the hosting of web site containing these prohibited materials. Downloading through the Internet.
* These obscene matters may cause harm to the mind

Intellectual Property crimes/Distribution of pirated software-

* Intellectual property consists of a bundle of rights.
* Any unlawful act by which the owner is deprived completely or partially of his rights is an offence.
* The common form of IPR violation is said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, *etc.*

The Hyderabad Court has in a land mark judgment has convicted three people and sentenced them to six months imprisonment and fine of Rs.50,000/- each for unauthorized copying and sell of pirated software.

Cyber terrorism against the Government organization

* Cyber terrorism and cyber crime are criminal acts.
* A cyber crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences.
* The recent example may be cited of – *Osama Bin Laden*, the LTTE, attack on America's army development system during Iraq war.

Fraud and Cheating — Online fraud and cheating is one of the most profitable businesses that are growing today in the cyber space.

Data diddling—

* This kind of an attack involves altering raw data just before a computer processes it, and then changing it back after the processing is completed.
* The electricity board faced similar problem of data diddling while the department was being computerised.

Salami attacks—

* This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes.

Background of Cyber Crime

The computer is centre of Information Technology Activities. The world first computer specific law was enacted in 1970, by German State of Hesse in the forum of data.

The first recorded cyber crime took place in the year 1820! That is not shocking considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of *Charles Babbage.*

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. Major Cyber crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland.

Indian System of offences and punishment

Indian Parliament had adopted two fold strategies to control cyber crimes. It has amended Indian Penal Code to face cyber

crimes and made provisions in the Information Technology Act, fundamentally enacted to facilitate e-commerce in India, to deal with computer related crimes.

Some important sections are –

Section 167 : Public servant framing an incorrect document with intent to cause injury.

Section 172 : Absconding to avoid service of summons, or other proceedings. Punishable with simple imprisonment for one month or fine upto Rs.500/-.

Section 173 : Preventing Service of Summons or other proceedings or preventing publication thereof. Punished with one month imprisonment or a fine of Rs.500/- or both.

Section 175 : Omission to produce a document or electronic record to a public servant by a person legally bound to produce it. Punishment of 6 months or fine of Rs.1,000/-.

Section 192 : Fabricating false evidence. Punishment of seven years of imprisonment.

Section 204 : Destruction of document or electronic record, to prevent its production as evidence in a Court of Law. Punishment 2 years imprisonment and fine.

Section 463 : Forgery. Whoever makes any false document or false electronic record.

Section 464 : Making a false document.

Section 466 : Forgery of Record of Court or public register.

Section 468 : Forgery for purpose of creating forged document or electronic record for the purpose of cheating. Punishment 7 years imprisonment.

Cyber Crimes :

Country Specific Responses – International Law

Australia :

Australia has adopted the Cyber Crime Act 2001 amending the law relating to computer offences and other related purposes. The scheme followed by the Act is to amend existing laws that have bearing on cyber crimes to bring these crimes under their purview. The Acts that stand amended by Cyber Crimes Act 2002 are as follows :

1. Australian Security Intelligence Organization Act, 1979.
2. Crimes Act 1914.
3. Criminal Code Act, 1995.
4. Education Services for Overseas Students Act, 2000.
5. Telecommunication (Interception) Act, 1997.

United States of America — USA has passed various enactments which contain some or other aspects of fighting cyber crimes:

1. Federal criminal code – related to computer crime
2. Offences relating to the misuse of dissemination system
3. Cyber stalking
4. Searching and seizing computer
5. Sentencing guidelines relevant to cyber crimes.

Clause III provides the principles relating to International co-operation in dealing with cyber crimes. It also provides specific principles with regard to co-operation in following fields that are to be followed by the parties:

1. Extradition
2. Mutual assistance
3. Sharing of disclosure of spontaneous information
4. Confidentiality and limitation on use of the shared data, for investigation or proceedings other than those stated in the request,
5. Material assistance regarding collection of traffic data

Confronted by the global proliferation cyber crimes, the United Nations has also made an attempt for control of these crimes.

(1) Modernization of national criminal laws and procedures, including measures to

(a) computer security and prevention measures

(b) sensitize the public, judiciary and law enforcement agencies

(c) adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer-related crimes.

(d) adoption of policies for the victim of computer-related crimes which are consistent with the UN Declaration of Basic Principles of Justice for Victims of Crime and abuse of power, including the restitution of illegally obtained assets and measures to encourage victims to report such crimes to the appropriate authorities.

World Intellectual Property Organization (WIPO)

Copyright protection

TRIPS agreement

World Trade Organization (WTO)

Information Technology Act 2000 — Criminal Procedure Code prescribes the procedure for trial of offences. Section 42 of Cr.PC further provides that offences under any other Law, which includes IT Act, shall also be investigated, subject to any special provision, applicable under the Special Law.

The Cr.PC trial Act of offence under IT Act, with a few exemptions provided under the IT Act, they are contained under Sections 70 and 80 of the Act, read with Section 81 of the IT Act, prevailed over the Cr.PC.

Conclusion and Suggestions

Cyber Crimes is a global phenomenon. It is only an attempt to dealt with various cyber crimes, which take place in cyber space, a threat not only to the nation but also to the entire world. The development of Multimedia super corridor has enhanced the susceptibility to cyber crimes.

Thus, the Computer Crimes Act must be seen not only as a law which regulates the behavior of people who use and do business over the Internet, but also must be seen as the Government's efforts to put in place soft infrastructure and the knowledge-based economy. Formation of legal and regulatory framework is an important step in this regard. Malaysia can achieve this in its Vision 2020.

At the same time, the Government should be aware that technological innovations and evolution of human minds require further strengthening of cyber laws. The law enforcement agencies should be active and rigorous punishments should be prescribed to the culprits.

Suggestions

* The IT Act 2000 and criminal law must enforce new techniques also
* Netizens and children must take care when they Browse the net, by avoiding unwanted e-mails, secure their passwords *etc.*
* Compulsory registration of cyber cafes
* Increase cyber police stations and safe guard the netizens.

———————