CHAPTER I: INTRODUCTION TO CYBER CRIME

Introduction:

The term 'cyber law' in general refers to all the legal and regulatory aspects of Internet. It means that anything concerned with, related to, or emanating from any legal aspects or issues concerning any activity of netizens and others in cyberspace comes within the ambit of cyber law. More specifically, cyber law can be defined as a law governing the use of computer and the Internet. Namely, it focuses on a combination of state and federal statutory, decisional and administrative laws arising out of the use of Internet.

The IT revolution resulted in a phenomenal increase in the number of cyberspace[1] users all over the world. The birth of the Internet resulted in networking which helped millions of users to connect online, thus facilitating the sharing of information. In India also, there was an overwhelming increase in the number of internet-users. *Forrester Research*, a technology and market research Firm reported that the number of internet-users worldwide would touch the 2.2 billion mark by 2013 and that India would have the third highest number of internet-users at the same time.[2] The government framed and announced Internet policy document in 1997[3] to promote and encourage internet-users in

---

1 William Gibson coined the term cyberspace in his science fiction novel *Neuromancer* written in early 1980s. The plot was largely set in a setting that had no physical existence. The plot involved a hacker employed by an anonymous employer to hack. Cyberspace was a conceptual hallucination that felt and looked like a physical space, but was actually computer-generated. In this setting, people, connected to network, carried out business transactions, worked, played and broke the law.
E.A. Cavazos and Govino Morin, *Cyberspace and the Law: Your Rights and Duties in the online world* (1994), p. 1

2 The Times of India, *India to have 3rd largest number of internet users by 2013*, July 26, 2009 *available at* http://articles.timesofindia.indiatimes.com/2009-07-26/india-business/28171189_1_internet-users-online-population-asian-markets (last visited July 11, 2011)

3 Internet Policy of Government of India-1997

India.[4] With economic activities like buying, selling, advertising, etcetera taking place online, the Internet indeed proved to be a boon for many. Little did anyone suspect that the uncontrolled manner in which online activities were carried on would give way to another category of computer related crimes. Cyber crime is a new type of criminal activity that started raising its ugly head in the early 1990s, as the Internet emerged as a virtual place for the users worldwide to meet and share various forms of Information. This development also paralleled with the entry of criminals to gain access to sensitive information if they have the necessary knowhow. Thus the Cyber space became vulnerable from the economic and social perspectives- driving companies and individuals to take costly steps to ensure their safety and exposure from those deviant acts in the cyber space.

1.1 Cyber Law and Cyber Crime:

One of the early cyber crime, which had come to the public notice is the fraud relating to fund transfer online to the tune of USD 10 Million from Citibank. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack compromising the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers to commit the cyber crime. He was finally arrested on Heathrow airport on his way to Switzerland.

Cyber Crimes increased by 22.7% in 2007 as compared to 2006 (from 453 in 2006 to 556 in 2007), Cyber Forgery 64.0% (217 out of total 339) and Cyber Fraud 21.5% (73 out of 339) were the main cases under IPC category for Cyber Crimes. In this 63.05% of the offenders under IT Act were in the age group 18-30 years (97 out of 154) and 55.2% of the offenders under IPC Sections were in the age group 30-45 years (237 out of 429) according to the latest

[4] *Bharat's Hand Book of Cyber and e-commerce Laws,* Edited and compiled by P.M. Bakshi and R.K. Suri,, Bharat Publishing House, New Delhi, 2002, p. 12

data available with the National Crime Records Bureau of the Ministry of Home of Government of India.

The Information Technology Bill (1999) has defined the cybercrimes as:

> '*Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when computer source code is required to be kept or maintained by law for the time being in force* [shall be punishable with a fine which may extend up to rupees two lakhs or with imprisonment up to three years, or with both].'

1.2 Classification of Cyber Crimes:

Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, and theft of intellectual properly. Cyber crime in the context of national security may involve hacking, traditional espionage, or information warfare and related activities.

Pornography, threatening email, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

Broadly there are two classes of cyber crimes:

A. *Computer Assisted Cyber Crimes: computer is instrumental in committing the crime.*

- Selling nonexistent, defective, substandard or counterfeit goods, theft of credit card, bank fraud, fake stock shares,

intellectual property offences including unauthorized sharing of the copy righted content of movies, music, digitized books

- Selling obscene and prohibited sexual representations.

B. Computer Oriented Cyber Crimes: Computer is the target of the crime

- Malicious Software: viruses, Trojans (which corrupt server)
- Cyber terrorism:
- Child pornography
- Violent and extreme pornography
- Internet inspired homicides and suicides

❖ *Worm: Self-replicating programmes, spread autonomously without a carrier.*

Ex. Via mail, scanning remote systems

❖ *Trojan: installed during downloading some programme as a back ground activity causing irreparable damage*

❖ *Spyware: parasitic software-invades privacy-divulging details- through tracking cookies.*

Even though our basic understanding about cyber crime is that computer is necessary as one of the components of the offence, it is also interpreted that a crime committed by using any digital device is covered under the ambit of cyber crime. For example: Casio digital diary, Mobiles, Calculators, Pen drives, CDs.

1.3 Cyber Security:

Cyberspace is as vulnerable as much as it is a vital infrastructure. The threat is real. US President Obama recently declared that "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security." The same is true for other nations as well. Private and public cyber infrastructure in the United States falls under nearly constant attack, often from shadowy sources connected to terrorist groups, organized crime syndicates, or foreign governments.[5]

These attacks bear the potential to disrupt e-mail and other online communications networks, but also the national energy grid, military-defense ground and satellite facilities, transportation systems, financial markets, and other essential facilities. In short, a substantial cyber-attack could take down the nation's entire security and economic infrastructure. Cyber is the new domain of international espionage, sabotage, and war. China, Russia, the United Kingdom, and the United States employ extensive cyber spying networks." A coordinated series of denial-of service and other attacks could cripple a state's political and communications systems, as happened during "Web War 1" between Russia and Estonia in 2007[6] as computer networks collapsed, factories and chemical plants exploded, satellites spin out of control and the financial and power grids failed." In June 2010, for example, a computer worm called "Stuxnet" was discovered in Iran. At first inspection, it appeared to be a routine bit of malware. Closer

---

[5] CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 1 (2008) [hereinafter CSIS REPORT], available at http://csis.org/files/media/csis/pubs/081208_securing cyberspace 44.pdf)

[6] The Threat from the Internet: Cyberiar, ECONOMIST, July 3, 2010, at 50, available at http://www.economist.com/node/16481504?storyid=16481504&CFID=158391401&CFTOKEN=341 82131.

analysis, however, revealed that Stuxnet was carefully designed to disrupt the sort of systems that help control equipment at nuclear power plants. Stuxnet's subtlety and sophistication suggested to most experts that it was engineered not by rogue hackers, but rather by an entity with the resources of a nation-state, and that it was specifically targeted to damage Iran's nuclear capabilities. Many Analysts suspected that it was coordinated and launched by Israel or the United States.[7]

Recent evidence suggests that Stuxnet successfully curtailed Iran's production of refined uranium. The Stuxnet attack appears to have bled into "real" space: the Iranian scientist chiefly responsible for eradicating Stuxnet from Iran's nuclear plants was killed on November 29, 2010, by assassins on motorbikes, who threw a bomb when he was driving his car.

Trojan horse- Program that performs some ostensibly useful function but contains, lurking within its code, a damaging instruction set. Often, that instruction set will enable a remote user to assume control of a system, or will secretly introduce unwanted software into a system. Indeed, Trojan horses are probably the most common way in which viruses are introduced into computer systems. While technologically complex, and once the sole province of sophisticated users, Trojan horses now are readily available from websites catering to would-be hackers. For example, the "Cult of the Dead Cow," a group of cyber-anarchists devoted to keeping the web free, created a program known as "Black Orifice 2000" that when downloaded from a user's e-mail, enables a remote user to take advantage of security problems with Windows and allows a remote user to control the target's computer.

[7] (Kim Zetter, Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage, WIRED THREAT LEVEL (Nov. 15, 2010, 4:00 PM), http://www.wired.com/threatlevel/2010/11 /stuxnet-clues.)

Password sniffers **-** Password sniffers are programs that monitor and record the names and password of Internet users as they log on to the network. The programs work by collecting bytes of the computer that is being monitored by the installer of the sniffer. When a network user types in a user name and a password, the sniffer collects the information and passes it on to the installer. With the use of this information the installer logs on to the system, has access to restricted documents and can manipulate information held therein.[8]

A virus is a program that modifies other computer programs. The modifications ensure that the infected program replicates the virus. In other words, the original program (the analogue to a healthy cell) is changed by the virus so that the virus can multiply. Once infected, the program secretly requests the computer's operating system to add a copy of the virus code to the target program.

Once that computer is connected to another computer, either through the Internet, direct computer connection, or even through a common floppy disk, the virus may spread beyond the original host computer. A virus is not inherently harmful-its harmfulness will depend on the additional codes placed into the virus besides the code for self-replication. Some viruses, however, have caused enormous damage.

The Melissa virus **-** Melissa infected its first victim when a reader of the pornographic alt.sex newsgroup caught it. Within days of this initial contact, Melissa infected more than one hundred Fortune 1000 companies. The virus operated by e-mailing a list of eighty pornographic web sites to fifty e-mail addresses in the electronic address book of the infected system. Id. The fifty recipients received e-mails with the subject line "Important Message From..." and the virus automatically filled in the initial

[8] (66 J. Crim. L. 269 2002)

user's name-so that it appeared that the recipient was receiving a message from his or her friend, rather than from the Melissa culprit.

Worms - A worm is a stand-alone program that replicates itself. Both worms and viruses self-replicate. The distinction is that while a virus requires human action, from downloading a specific file to placing an infected disk in a computer, a worm uses a computer network to duplicate itself and does not require human activity for transmission. For example 'I love you virus' bred on a hosts computer and it reproduced over a network. Most companies, including AT&T Corp., Ford Motor Co., and Merrill Lynch & Co., shut down their e-mail systems to prevent a spread of the attack, resulting in lost time and productivity. Government agencies were also affected, including the Pentagon, the CIA, NASA, the Swiss Government, Danish Parliament, and the British House of Commons.

Investigators traced the 'I Love You bug' to several computer students in the Philippines, but the case was ultimately dropped because the Philippines had no applicable law against viruses or hacking.

Some Illustrations :

E -mail Cheating -Mr. Vijay Ninwane works at Abu Dhabi. He was sent a mail by one X saying that she is interested in him. Both of them exchanged nude photos, erotic stories etc. "x" introduced her friends y1, y2, y3, y4. Vijay could not meet x as promised as a result of which she committed suicide. Then Vijay received mail from WWW.KOLKATTA_POLICE.COM, WWW.CBI_HQ.COM alleging that he is responsible for her death and he would be prosecuted for the same. Vijay contacted Y1 for help. Y1 coaxed Vijay to have a lawyer and she will help him to get a lawyer. Accordingly Y1 fixed Mr. Pranab Mitra of Mitra & Mitra associates and made him believe that they are the leading lawyers.

Vijay paid total Rs.70 lakhs (Rs.1.19 crore as per investigating officer). During the investigation it was revealed there is no girl by name X and Y1 and others are also fictitious persons created by one single man named Mr. Pranab Mitra, General Manager of the Firm.[9]

Cyber Murder **-** A patient was admitted in New York Hospital. The entire system was computerized in the hospital. One cracker entered the system and modified the data relating to amount of insulin to be injected to a patient as a result of which 60mg was modified into 260mg. Nurse injected the same amount of insulin to the patient and he died.

PHISHING **-** Using spoof e-mails or directing people to fake web sites to fool them into divulging personal financial details so criminals can access their accounts.

PHARMING **-** Technically more sophisticated and it means exploitation of vulnerability in the DNS server software. Approximately 7.9 million phishing attacks are made per day on pentagon. There is a tremendous increase of 39% over first half of 2005.

1.4 Distinction between cyber crime and conventional crime:

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality,

[9] P Krishna Sastry, Forensic Expert, Questioned Documents, Hyderabad.

social order or any unjust or shameful act. The "offence" is defined in the Indian Penal Code to mean as an act or omission made punishable by any law for the time being in force.

Sir William Blackstone defines crime as a Act committed or omitted in violation of a public law forbidding or commanding it.

Sir C.K. Allen (The Nature of a crime) proposes that "Crime is crime because it consists in wrong doing which directly and in serious degree threatens the security or well-being of the society, and it is not safe to leave it redressable only by compensation of the parties injured".

Wolfenden Committee (England) tried to explain crime as "The function of criminal law is to preserve public order and decency, to protect the citizen from what is offensive or injurious, and to provide sufficient safeguards against exploitation and corruption of others, particularly those who are especially vulnerable. It is not a function of the law to intervene in the private lives of citizens or to seek to enforce any particular pattern of behaviour, further than is necessary to carry out the purposes which we have outlined".

The general laws in the area of criminal law commonly referred are the Indian Penal Code, 1860 ("IPC"), which is the general penal law of India and the Indian Evidence Act, 1872 ("Evidence Act"), the general law pertaining to admissibility of evidence in civil and criminal trials. The manner in which trial of criminal cases are to be conducted is dealt with under the Criminal Procedure Code, 1973 ("Cr. P. C").

To understand 'cyber crimes' and its ramifications in terms of the damage, the challenge to prosecution, the loopholes of the existing criminal justice system, the powers of regulation and its boundaries, it is essential to have look at the concept of 'crime' itself.

In every organized society, certain acts and omissions are forbidden on pain of punishment, which may even extend to the forfeiture itself. What acts or omissions should be singled out for punishment or be branded as crimes has always depended on the force, vigour and movement of public opinion from time to time to and country to country and even in the same country from decade to decade.

Dowry was considered as a 'social status' at a particular period, which today is a crime. Untouchability was an accepted social norm of a particular period in society in tune with caste hierarchy and today it is a crime under the constitution. Thus very many acts are crime today, which are not once, and some acts like homosexuality or lesbianism, which is a crime today, could change tomorrow. In essence the 'concept of crime' is static in some aspects such as stealing, fraud, causing injury, murder etc. and changing in certain aspects of social norms and relationship.

Similarly 'crime' in a society is not a crime in another society. What could be considered as 'obscenity' in India could be viewed differently in Sweden. For example watching pornography is not a crime in England, whereas in India public watching, transmission of porn material is an offence.

As it is very difficult to explain and define a 'crime' , we can describe it and may state that in a crime we find at least three attributes mainly first that it is a harm brought about by some anti social act of a human being, which sovereign power wants to prevent, secondly the preventive measures taken by the state appear in the form of threat of a sanction or punishment and thirdly the legal proceedings wherein the guilt or otherwise of the accused is determined are a special kind of proceedings governed by special rules of evidence.

A crime consists of following components. a) Human being b) ***Mens Rea***- the mental state of the person accused of a criminal

act or guilty mind c) ***Actus Reus***- committing an act or omission of an act when it is warranted resulting in a criminal act d) harm to body mind or reputation.

Yet another very important aspect of crime is that 1. A particular act or omission shall be recognized by a law as an offence and 2. There shall be a punishment prescribed for the offence recognized.

The legal debate surrounding 'cyber crimes' is twofold. The first challenge is to define what constitutes 'cyber crimes' as opposed to 'physical crimes' and the second challenge is that of the application of traditional criminal law and criminal justice administration on the 'cyber crimes'. In the first debate on what constitutes 'cyber crimes' there is some consensus. Legal analysts have a consensus that 'cyber crimes' are those crimes perpetuated using computers and computer networks through the medium of Internet to perpetuate various cyber crimes. Such crimes are committed:

It is on the second aspect of analysis, whether 'cyber crimes' need a different interpretation of the criminal law concepts, there are divergent views. Whether there should be a separate 'cyber crime laws' or whether traditional criminal law is enough? How to assess and compute the damages in 'cyber crimes' using the traditional analysis of criminal law used in the concept of 'physical crime' and related issues. Additionally the nature of 'cyber crimes' by virtue of the internet is a crime which poses challenge to international conduct and hence the need for an international dimension of 'cyber crimes' which is considered as the 'international warfare of Information technology'.

On the regulation of the 'cyber crimes' again there is a wide debate on how far one can regulate and what type of regulations should be in place. There could be consensus on the regulation of 'cyber crimes' such as hacking, fraud, obscenity and related crimes,

where as the human right activists, votaries of privacy and other activists accuse violations of the authority on the name of security and cyber crime where their civil rights are curbed, activities monitored and privacy intruded.

The term 'cyber crime' is a misnomer. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. However, there are certain differences between the two. It would be relevant to points out these similarities and differences between the two.

1.5 Requirement of guilty mind for cyber crimes:

To be guilty of cybercrime in India, a person must act voluntarily and willfully. For example, a person who deliberately sends Viruses online is guilty of cybercrime; a person who forwards an e-mail without realizing it contains a virus or spreads a virus when her account is hacked is not guilty.

Sec 65, 66 and 67 of IT Act mandates that offences recognised under these provisions shall be committed by the accused intentionally. Intention, knowledge, fraudulent intention, connotes various forms of guilty mind. The following is a brief explanation of some phrases used in IT Act connoting guilty mind.

Intention:

1. Design of doing an act

2. Purpose/ design with which an act is done. It is also the **expectation** that certain consequences will follow from the **conduct** of a person. Conduct is the proof of intention.

Noted Jurist Salmond says that every wrongful act may raise two distinct questions with respect to the intention of the

doer. How did he do the act? Why did he do it? First is an inquiry into intention. Second is concern with his ulterior motive.

Knowledge and belief:

Knowledge is the awareness of facts**.** If an accused knows the consequences or have the awareness of the facts it is deemed that he has guilty mind**.**

Dishonest Intention:

Sec 24 of IPC defines "Dishonestly" as,

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Sec 25 of IPC defines "Fraudulently" as,

A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

The IT Act, Sec 66B uses the word 'dishonest intention' which is not defined in the Act, then one can refer to IPC which is a general legislation in the area of criminal law.

Law of Attempt:

Person commits offence of attempt to commit an offence when he/she

1. Intends to commit that particular offence
2. He having made preparation with an intention to commit an offence, does an act towards commission

3. Such an act need not be the penultimate act towards committing that offence, but should be an act during the course of committing that offence.

4. Such act must be proximate to offence.

Measure of proximity is not in relation to time and action, but in relation to intention

There are five kinds of punishments recognized by IPC, 1860 - Death, Imprisonment for Life, Imprisonment Rigorous and simple, Forfeiture of Property and Fine.

Information Technology Act, 2000 for cyber crimes prescribes two kinds of punishments i.e. imprisonment and fine.

How to judge whether particular incident is a crime ?

Example 1: Mr. Ram bolts the door of a house belonging to X from outside and sets fire, resulting in death of four inhabitants. If we analyse the case, first point is Ram is a human being had it been a monkey not liable, second he had an intention to burn the house and kill the inhabitants which is clear from his conduct of bolting door from outside, three he committed the forbidden act of burning and fourth there is harm which is death of four people. Hence it is a crime of Murder punishable under Sec 300 of IPC with either Life imprisonment or death.

Example 2: A fired a shot at a bush in a thick forest thinking there is a tiger behind it, but there is a person who died of the shot. The question is whether he is liable. He is not liable because he doesn't have the required guilty mind; his intention was to kill a tiger.

Thus the penal provisions will act upon the application of the above basic elements in any crime in the physical world. The basics of such is in the first place, any legal system should first

define certain acts as criminal which is harmful to the society and there upon the actions that are considered as crime will be subject to the scrutiny of the above elements of intention, conduct, circumstance and prohibited act to evoke the required penal provisions. The fundamental principle is that a conviction is possible only if there is a concrete proof beyond reasonable doubt that the act of a person is prohibited by the criminal law and such an act is also committed with an intention of causing the same.

1. 6 CRIME IN CONTEXT OF CYBER CRIMES:

The cyber world is defined as a virtual world, which is different from that of the physical world. The cyber world though a virtual world is a reality, which interconnects, people, organizations, Governments. It transacts information at the basic level but also conducts the business of governments and private enterprises in a manner where no other technology could dream of. The cyber space is also a space where various types of crimes are perpetuated and the magnitude of such crimes could be unimaginable due its speed, anonymity and destruction has been amply recorded. The moot point is whether the same principles of criminal law can be applied to the 'cyber world crimes' as applied to the 'world of physical crimes'. The answer is divided.

One school of thought advocate that it is possible to interpret the crimes perpetuated in the cyber world to that of the physical world and hence could apply the same principles to regulate them. To substantiate the following arguments are held forth:

1. 'Cyber Crimes' are nothing but crimes of the physical world perpetuated in the world of computers and hence there is no difference in defining a crime in the cyber world and the physical world

2. As in the physical world the cyber world crimes are perpetuated by individuals or groups, where the medium is the only difference.

3. As the traditional principles of criminal law have tackled various technologies used in the past it is capable of analyzing and interpreting the new technology as well.

4. The cyber crimes in fact are lesser in scope than the physical crime like fraud, intrusion of privacy, data theft, damage to computers, cheating consumers etc. where as physical injury or other crimes like rape, grievous hurt or bigamy cannot be perpetuated through the cyber crimes.

5. The technological advancement of the information technology itself is a deterrent and a tool in tracking and convicting the crimes.

On the other hand there are advocates who say that 'cyber crimes' cannot be tackled with the conventional principles of 'cyber crimes' and thus need special laws to regulate them and they put forth the following arguments:

1. Cyber Crime is a crime, which has a potential and uncontrollable damage and needs stricter regulations. A virus introduced can damage millions of computers before even finding the perpetuator.
2. The cyber crime is perpetuated by anonymous person who has to be skilled in opening the password and security systems and can vanish without a trace.
3. The cyber crimes are transnational in nature, which involves complex prosecution procedures to bring the culprits to the book.
4. The Cyber crime of obscenity and pornography has a potential moral depravity on generations which could push them into the physical world of crimes

5. The National Security and security in terms of safety like Airports, Railway systems are more vulnerable and could create chaos and economic loss by cyber crimes and hence special laws to apprehend, prosecute with stiffer penalties are needed in context of cyber crimes
6. The technology is a fast changing one and hence needs a different type of enforcement system to tackle the cyber crimes unlike the physical crimes.

1.7 Punishments under IT Act:

With the debate on the above lines continuing one thing is clear that cyber crimes has the potential to damage the economic aspects of a society and a nation due to technology where speed, ease of operation, defying boundaries are strengths and weaknesses at the same time. The legislations around the world are veering around to the view that 'cyber crimes' warrant stricter penalties due to its quantum of damage. There are also attempts to address the technology related issues by setting up of 'cyber tribunals'.

In Indian context, the IT Act of 2000 tries to address the question of 'cyber crimes' by defining what is a damage in the context of the computers and the relevant penalties as follows:

Imprisonment for a specific period of time and fine is prescribed as punishments for cyber crimes in the Act. It is not clear from provisions whether imprisonment is of rigorous or simple in nature. The fine amounts are in tune with the losses incurred in cyber world and are quite deterrent in nature. For Example Sec 66 IT imposes two lakhs of rupees as fine.

Confiscation:

Section 76 provides that Any computer, computer system, floppies, compact disks, tape drives or nay other accessories

related thereto, in respect of the if which any provision of this Act, rule, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Residuary Penalty:

According to Section 45, whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Non-Interference with other Punishments:

According to Section 77 of the Act, No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.