UNIT 6 INTRODUCTION TO COMPUTER WRONGS

Structure

6.1 INTRODUCTION

In this unit which is the first unit of this block, attempt has been made to give an overview of the computer wrongs. In the subsequent units we shall discuss various classes of computer wrongs.

With new mediums of communication, business and societal activities, growth of newer and varied kinds of crime is inevitable. Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. The Internet is at once several shopping malls, libraries, universities, news paper, television, movie theatre, post office, courier service and an extension of government and business. It is like life in the real world being extended and carried on in another medium that cuts across boundaries, space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. The Internet, with all the benefits of anonymity, reliability, and convenience has become an appropriate breeding place for persons interested in making use of the Net for illegal purposes, either monetary or otherwise.

6.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss the concepts of computer wrong and how the civil wrongs can be distinguished from the computer crimes, how the computer crimes are classified;
- distinguish between the concept of technology based and technology neutral laws;
- examine the issues involved in the regulation of cyberspace; and
- discuss how the matter has been dealt by the I.T. Act, 2000.

6.3 COMPUTER WRONGS

Computer wrongs includes both civil wrongs and crimes. 'Cyber crimes' is used in a generic sense which tends to cover all kinds of civil and criminal wrongs related to a computer. However, the phrase 'cyber crimes' has two limitations to it: (a) 'cyber' generally tends to convey the feeling of 'internet' or being 'online' and hence, does not cover other computer related activities; (b) 'crimes' restricts the application of the phrase to criminal wrongs. It would not include civil wrongs. Thus, it would be preferable to understand the concept of any wrong related to computer as being a 'computer wrong'. It would include any tort or civil wrong done which relates to a computer as also any criminal activity relatable to a computer. One must also keep in mind that it is the statute on a particular subject which informs us as to: (a) whether a particular act is a wrong; and, (b) if it is, whether such wrong is a civil wrong or a crime. The Information Technology Act, as would be seen in the subsequent units, divides various computer-related wrongs into computer torts and computer crimes. Computer torts lead to penalty and compensation whereas computer crimes lead to imprisonment, fine and confiscation.

6.4 CLASSIFICATION OF COMPUTER CRIMES

Technology-aided crimes can essentially be classified under two headings:

A) Where computer is used a *tool* to commit the crime: The computer is a tool for an unlawful act where the offence reflects a modification of a conventional crime by making use of information technology and modern communication tools.

B) Where the computer is the *target* for the crime: There are certain crimes where the computer itself is the target, that is, to say such crimes which have evolved due to the advancement in information technology itself.

There might be instances where the computer is a tool as well as the target of a crime. This kind of activity involves sophisticated crimes usually out of the purview of conventional criminal law. There is a third category as well, where computers are considered as *incidental* to a crime. The use of a computer is not necessary but is used to make the offender more efficient in the commission of the crime. This includes use of computers in bookmaking or drug-dealing.

6.5 COMMISSION OF MULTIPLE COMPUTER WRONGS

Another concern in computer crimes is the possibility of and ease with which an offender can commit multiple crimes at one goes. It is very possible and in fact, quite likely that an offender in the process of committing one computer crime commits other crimes as well. We can take a few instances to illustrate the point:

A) In case of data theft, one has to hack (unauthorized access) the computer or any other electronic storage medium and only then can be commit theft. Thus data theft includes hacking and theft.

B) To initiate a Distributed Denial-of-service, installation of virus, and Trojan horses on the 'slave'/compromised systems would be needed. The date of 'target' computer may also be altered or destroyed in the process. Thus, DDoS includes hacking, introduction of virus and data alteration.

C) Web defacing can be achieved by first hacking into the computer system.

The Indian statutory regulation, specifically Section 66 of the Indian Information Technology Act, 2000, in the area of computer crimes is quite comprehensive and concise. It is noticeable that most of the computer crimes culminate into section 66. Subsequent units on specific computer crimes would make the point clear.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are computer wrongs? How they are classified into civil wrongs and crimes?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6.6 CHALLENGES TO LAWS

India is today re-discovering itself – technologically. Being a developing country, it realises that the Internet and the use of computers are powerful tools for its economic development. Economic development presupposes existence of an appropriate regulatory regime. The biggest challenge to the law is to keep pace with technology.

6.6.1 Technology-neutral and Technology-based Laws

So far as law with respect to computer crimes is concerned, we have to have in place two sets of well-developed law: (1) technology-neutral criminal law; (2) technology-based laws. While talking about crimes relating to the Internet, most traditional crimes like fraud, defamation when committed using the Internet, would be governed by the existing technology neutral criminal laws. These are crimes with all elements of offline crimes, the only difference being that the Internet was used as aid in their commission. The other type of crime, and more disturbing requiring legal innovations, is the one directed at computers, networks, data etc. They include unauthorized disruption of computers and networks.

One of the challenges of making technology-based laws is that there is a chance of such laws being soon outdated. Again, it is against equity and fairness if offline conduct is governed differently from online conduct. This gives rise to the possibility of crime shifting from one medium to the other if there is an inconsistency in laws. Consistency between the two sets of law is, therefore, desirable. Laws must also cater to the need of prevention and investigation of crimes. For instance, with the advent of telephones, wire-tapping laws were introduced; similar laws to deal with unlawful conduct in the Internet would become necessary.

Clearly, with the development of new technology and with the realisation that such technology affects human life and relations and the peace, order and proprietary rights in society, laws must be framed to regulate conduct accordingly. Let’s take for instance theft of passwords. Passwords are a combination of alphabets and numbers and are central to the operation of computers. These are nothing but keys to gain entry into computer systems. Stealing a password or unauthorized access using someone else’s password must be recognised as merely the first step to committing a crime. Similarly, networks need to be recognised as highways for movement of information and communication and not for cranks to dig holes or put up impediments. One can enter into a private computer network only when one is authorized to enter much the same way as to enter into a private physical space. Web pages as private property can be considered as displays in shops. One can watch but cannot break the glass of the shop. Similarly, one can browse, but not tamper with or destroy.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is technology based law and technology neutral law?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6.6.2 Regulation Versus Freedom on the Internet

Talking of laws to control criminal behaviour on the Net brings one to the debate of regulation versus freedom on the Net. There are some who argue that the Net should not be regulated by governments.[1] They argue that, the Net grew because of its free environment, inviting people to contribute. Freedom and space for adventure, a new and different and an almost unrestricted and seemingly anonymous travelling experience has made the Net such an exciting media. Self governance is what they advocate for the Net. But this has several problems like, some groups taking law into their own hands. As Laurence Lessig, in *The Spam Wars*[2] says, "Vigilantes and network service providers (unaccountable groups) deciding fundamental policy questions about how the network will work – each group from its own perspective." This led to the argument that cyberspace transactions are no different from "real space" transnational transactions[3] that require government regulations in the ordinary way. The debate in the world between regulation and freedom on the Net has now more or less been settled in favour of the need for regulation. More and more governments have begun taking steps to regulate the Net.

6.6.3 Internet Crime Different from other Technology Crimes

It is important to note the difference between crime on the Internet and a crime with another modern technology. While crimes are rarely directed against

a telephone as an instrument, computers often become the victims of attack. Nature of crime on the computer is challenging and requires new definitions and understanding and a restatement of accepted norms of criminal conduct and punishment because of several reasons. Computers, apart from being comparatively more expensive, are also the repository of immense amount of data. This data can sometime contain valuable scientific inputs, purely personal matter, study works, e-mails, and official work. Tampering with this data or stealing it is much more harmful than stealing the computer. This requires recognition of data as a special form of property, as a privacy right.

6.7 INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act seeks to protect a common man from the ill effects of the advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and appointing regulatory authorities. Many electronic crimes have been bought within the definition of traditional crimes too by means of amendment to the Indian Penal Code, 1860. The Evidence Act, 1872 and the Banker's Book Evidence Act, 1891 too have been suitably amended in order to facilitate collection of evidence in fighting electronic crimes.

In the following units, common computer crimes have been discussed. Wherever possible, not only the meaning and scope of the crime but also its coverage under the Indian Information Technology Act, 2000, the Indian Penal code and other minor criminal Acts have been discussed. The computer crimes can be classified into the following categories:

A) Conventional crimes through computer: cyber defamation, digital forgery, cyber pornography, cyber stalking/harassment, Internet fraud, financial crimes, online gambling, and sale of illegal articles.

B) Crimes committed on a computer network: hacking/unauthorized access, denial of service.

C) Crimes relating to data alteration/destruction: virus/worms/Trojan horses/ logic bomb, theft of Internet hours, data diddling, salami attacks, steganography

6.8 OFFENCES UNDER THE IT ACT

Chapter XI of the Act enumerates the various acts which constitute an offence under the Act along with the punishment be it either imprisonment or fine or both. Such offences (including offences under other sections) can be better understood in the form of a table:

Section	Offence	Punishment
33(2)	Failure of any Certifying Authority to surrender a licence under Section 33(1) after such licence has been suspended or revoked [Section 25(1)].	Person in whose favour the licence is issued shall be punished with imprisonment which may extend upto six months or a fine which may extend upto Rs.10,000 or both.
65 (Tampering)	Knowingly or intentionally concealing, destroying or altering or intentionally or knowingly causing another to conceal, destroy, or alter any computer source code use for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Punishable with imprisonment upto three years, or with fine which may extend up to Rs. 2,00,000/-, or with both.
66 (Hacking)	Destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously be any means with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any person.	Punishable with imprisonment up to three years, or with fine which may extend up to Rs. 2,00,000/-, or with both.
67	Publishing or transmitting or causing to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, or read, see or hear the matter contained or embodies in it that is hacking as defined under Section 67(1)	First conviction: punishable with imprisonment of either description of a term which may extend to five years and with fine which may extend to Rs. 1,00,000/-. Second or subsequent conviction: imprisonment of either description of a term which may extend to ten years and with fine which may extend to Rs. 2,00,000/-.
68(2)	Failure to comply with the order of Controller under section 68(1) which empowers the Controller to direct, by order, a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rule or any regulations made thereunder.	Punishable with imprisonment for a term not exceeding three years or to a fine not exceeding Rs. 2,00,000/- or to both.
69(3)	Failure to assist an agency [referred in section 69(2)] which is required to intercept any information as required by an order of the Controller [under section 69(1)]	Punishable with imprisonment for a term which may extend to seven years.
70(3)	Securing access or attempting to secure access to a protected system [as declared by the	Punishable with imprisonment of either description for a term which

	appropriate Government vide a notification under section 70(1)] in contravention of the provisions of this section [that is such person is not authorized by the appropriate Government under section 70(2) to access the protected system].	may extend to ten years and shall also be liable to fine.
71	Making any misrepresentation to, or suppressing any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs. 1,00,000/-, or with both.
72	Securing access to any electronic record, book, register, correspondence, information, document or other material by any person in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder without the consent of the person concerned and thereafter, disclosing such electronic record, etc. to any other person.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one Rs. 1,00,000/- or with both.
73	Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that- (a) the Certifying Authority listed in the certificate has not issued it; or, (b) the subscriber listed in the certificate has not accepted it; or, (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
74	Knowingly creating, publishing or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

In case of offences committed by companies, such persons who, at the time the contravention was committed, was in charge of, and was responsible, to, the company for the conduct of business of the company as well as the company, will be, under sub-section (1) of section 85 of the Act, guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, if such person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, he shall not be liable to punishment. Sub-section (2) of section 85 also deems a director, manager, secretary or any other office of the company to be guilty of contravention and liable for punishment if it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of such person. ‘Company’, for the purpose of this section, has been explained to mean any body corporate and includes a firm or other association of individuals. ‘Director’, in relation to a firm, would mean a partner in the firm.

Section 7[4] prohibits immunity against any punishment under any other law to which a person might be liable to in spite of any penalty imposed or confiscation made under the IT Act.

6.9 INVESTIGATION UNDER THE IT ACT

The procedure for investigation for compute crimes is no different from the investigation for conventional crimes and Code of Criminal Procedure, subject to the provisions of the IT Act, would apply.

Investigation, for the purposes of the Code of Criminal Procedure, 1973, has been held by the Supreme Court [*State of Maharashtra* v. *Rajendra*, (1997) 3 Crimes 285] to consist generally of the following steps:

1) Proceeding to the spot
2) Ascertaining all the facts and circumstances of the case
3) Discovery and arrest of the suspected offender
4) Collection of evidence relating to the commission of the offence which may consist of,
   a) the examination of various persons (including, the accused) and the reduction of their statement into writing, if the officer thinks fit,
   b) the search of places and seizure of things considered necessary for the investigation and to be produced at the trial, and
5) Formation of the opinion as to whether on the materials collected, there is a case to place the accused before a Magistrate for trial and if so, taking the necessary steps for the same by filing a charge-sheet under section 173.

Section 78 of the IT Act places the powers of investigation to a police officer not below the rank of Deputy Superintendent of Police. This provision overrides anything contrary in the Code of Criminal Procedure.

Section 80 enumerates the powers of police officers to enter and search premises. Sub-section (1) of section 80 provides that any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under the Act. For the purposes of sub-section (1), the expression ‘public place’ has been explained to include any conveyance, any hotel, any shop or any other place intended for use by, or accessible by the public.

Where any person is arrested under sub-section (1), then sub-section (2) requires that such person should, without unnecessary delay, is taken or sent before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station. The provisions of the Code of Criminal Procedure are to apply in relation to any entry, search or arrest made under section 80, subject of course to the provisions of the section itself.

6.10 CONVENTION ON CYBERCRIME – COUNCIL OF EUROPE[5]

The Convention on Cyber Crimes is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. The possibility of computer networks and electronic information being used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, was the underlying concern during the preparation of the Convention. The Convention was deemed necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in the Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cyber crime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organization. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

References to the Convention would be made in subsequence units dealing with specific cyber/computer crimes alongside the Indian Information Technology Act.

6.11 SUMMARY

Computer wrongs include both civil wrongs and crimes. The Information Technology Act, 2000 covers both– civil wrongs and crimes. For the purposes of committing a crime, a computer can be used both as a tool as well as a target. Sometimes, it is used to make the offender more efficient in the commission of the crime. It is very possible and in fact, quite likely that an offender in the process of committing one computer crime commits other crimes as well. One of the challenges of making technology-based laws is that there is a chance of such laws being outdated soon. The debate in the world between regulation and freedom on the Net has now more or less been settled in favour of the need for regulation. Governments have begun taking steps to regulate the Net.

Chapter XI of the Information Technology Act enumerates the various acts which constitute an offence under the Act along with the punishment of either imprisonment or fine or both. The procedure for investigation for computer

crimes is no different than the investigation for conventional crimes and Code of Criminal Procedure, subject to the provisions of the IT Act, would apply.

The Convention on Cyber crime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

6.12 TERMINAL QUESTIONS

1) What are computer wrongs? Discuss the concepts of technology based and technology neutral wrongs.

2) Discuss the arguments in favour and against of the regulation of cyberspace. What are your views on this issue?

3) Discuss the challenges faced by the investigating agencies in investigating computer crime?

6.13 ANSWERS AND HINTS

1) Computer wrongs includes both civil wrongs and crimes. 'Cyber crimes' is used in a generic sense which tends to cover all kinds of civil and criminal wrongs related to a computer. However, the phrase 'cyber crimes' has two limitations to it: (a) 'cyber' generally tends to convey the feeling of 'internet' or being 'online' and hence, does not cover other computer related activities; (b) 'crimes' restricts the application of the phrase to criminal wrongs. It would not include civil wrongs. Thus, it would be preferable to understand the concept of any wrong related to computer as being a 'computer wrong'. It would include any tort or civil wrong done which relates to a computer as also any criminal activity relatable to a computer. One must also keep in mind that it is the statute on a particular subject which informs us as to: (a) whether a particular act is a wrong; and, (b) if it is, whether such wrong is a civil wrong or a crime. The Information Technology Act, as would be seen in the subsequent units, divides various computer-related wrongs into computer torts and computer crimes. Computer torts lead to penalty and compensation whereas computer crimes lead to imprisonment, fine and confiscation.

2) Technology based laws are those in which computer is the means or the target of the crime such as hacking etc. While technology neutral laws are ordinary laws and it is immaterial whether computer is used or not such as defamation etc.

6.14 REFERENCES AND SUGGESTED READINGS

1. See, for example, David R. Johnson & David Post. "Law and Borders—The Rise of Law in Cyberspace". Stan L Rev 48 (1996): 1367,1372-75.

2. Lawrence Lessig. “The Spam Wars”. Opinion. 31 Dec.1998. 9 Feb. 05 <http://www.lessig.org/content/standard/0,1902,3006,00.html>.

3. Jack L. Goldsmith. “Against Cyber Anarchy”. U Chi L Rev 65 (1998): 1199-1250.

4. S. 77. Penalties or confiscation not to interfere with other punishments. 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.

5. Budapest. 23.XI.2001. Council of Europe. 8 Feb.06 < http://conventions. coe.int/Treaty/en/Treaties/html/185.htm>.