Chapter 4

Forms and varieties of Cyber-crimes and related phenomenon
Chapter 4
FORMS AND VARIETIES OF CYBER CRIMES
AND RELATED PHENOMENON

4.1 Introduction

Cyber crime is complex and sometimes elusive phenomena. Some of the crimes happened in cyberspace resembled with that of traditional crimes, such as Internet theft (resemble with theft), e-defamation (defamation, libel, slander), sexual harassment of women (outraging modesty of women). However, some of the crimes that are committed in the cyberspace are unique of nature and unknown to the existing criminal jurisprudence such as virus, hacking, denial of service attack etc. Even though, the crimes that resembles with traditional crimes is of different nature, due to difference in intent, content and difficulties in locating the offenders, jurisdiction and enforcement.

Therefore, whenever the question of Cyber crime has discussed on any platform and suggested remedies are scrutinized, the legal expert appears to be divided into two schools of thoughts. First thought that believes that cyber crimes are not in any way dissimilar to the ordinary crimes like trespass, larceny or conspiracy with a difference that these crimes are committed with the help of computers, computer system or via computer networking. The other school gives much credence to unique nature of the emerging technologies and unique set of challenges and contends that a new comprehensive legislation is needed to deal with the Cyber crime. Thus the questions whether Cyber crime should be studied at on different footings or should be treated as merely the extended versions of traditional criminality only with the variation of computer as an incidental tool, is matter of prime concern.

---

2 See, Section 378 of Indian Penal Code, 1860.
3 See, Section 499-502 of India Penal Code, 1860. Defamation in India is also dealt under the Law of Torts.
4 See, Section 354 of Indian Penal Code, 1860 and other sections providing punishment for debasing the dignity and image of women.
In this chapter, some of the categories of Cyber crimes have been discuss in order to understand nature of these crime and probable legal response and possible mode of studies available in India.

4.2 Pornography

4.2.1 Pornography - Offence affecting Decency and Morals

The fundamental object and purpose of criminal law is not only to protect and to conserve the safety and security of primary personal rights of individuals, such as right to life, right to body, right to property, right to habitation, etc., but also to protect and guard public morals and public decency and to conserve the moral welfare of the state. Thus it is the duty of the State to guard the citizens against attacks, which may be insidious (harmful) and punishes individuals for obscene publications that tend to corrupt morals. The importance of the protection of such rights can be visualised from the resolution passed by the International Convention for the Suppression and Circulation of, and Traffic, in, obscene publications at Geneva as long ago as 1923.

The word 'Pornography' means 'writings or pictures dealing with sexual matters in a manner intended to incite lust and therefore considered obscene'. The word 'porn -' is having Greek origin means harlot and ' -graphy' an English origin means study. However, the word 'pornography' is neither illustrated nor used in legislative enactments. Instead of 'pornography', the legislative enactments has used different terminology, differ from context to context. It is therefore, essential to analyse the various terminology and its judicial interpretation in order to understand the true meaning of word 'Pornography'.

---


10 Encyclopaedia Britannica, Inc. See also “Pornography - A description or portrayal of any activities regarded as obscene”
The related word use in most of the criminal laws is used 'obscene'. Thus according to Encyclopaedia Britannica inc 'the writing or pictures (and any instrument of visible representation) with sexual matters' can be regarded as pornographic material if 'it intended to incite lust' of the person addressed to. It means that if its effect, or the effect of any one of the items, tends to deprave and corrupt persons, who are likely to read, see or hear the matter contained in such materials. Conversely, the matter that otherwise deals with sexual matter but does not appeal or incite sexual lust cannot be treated as pornographic material. Thus for an exception, book, pamphlet, paper, writing, drawing, painting, representation or figure in the interest of science, literature, art, learning or other objects of general concern and which may be dealt with sexual matter but utilisation of that material is justified on the ground give above can't be regarded as 'Pornographic material'. The basic test of 'intended or incite lust' is touchstone to regard any material as pornographic. It is therefore essential to have comparative analysis of various standards applicable under different legal system to apply the criteria for testing material whether 'obscene' or not.

4.2.2 Test of Obscenity & Pornography - General consideration

As in the other area of law, whenever the terminology has not been not defined under statutes, the judicial interpretation is essential to clarify the terms. The word 'obscene' or 'pornography' is not clearly defined under any law. Therefore judiciary has developed certain tests during the course of time via various court cases while attempting to clear the meaning of the words. The earlier attempt to define the word obscenity can be traced back in 'Hicklin rule'. In England, the rule had been emerged from Regina v. Hicklin case. In the case, the Queens Bench had to examine that the whether the printed material on pamphlet was obscene in nature or not. While commenting over the issue bench proclaimed -

---

11 For e.g. S. 292 (2) (i) of Indian Penal Code, 1860 runs as follows,
S. 292 (1) "For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object shall be deemed to be obscene if it is lascivious or appeals or the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its item’s is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it."


13 S. 292 (2) (i) of Indian Penal Code. 1860.
14 (1968) LR 3 QB 360, 371.
"...whether the tendency of the matter charged as obscene is sufficient to deprave and corrupt whose minds are open to such immoral influences and into whose hand a publication of this sort may fall. An important aspect of the Hicklin rule was that a work could be obscene, if an "isolated passage" could tend to corrupt the "most susceptible persons".\footnote{15}

However the Hicklin test ruled the roost only till 1954 in England and in Martine Seeker Case\footnote{16} court has taken different stand on the line.

\subsection{4.2.3 The Test of Obscenity & Pornography - American Law}

To test to decide whether the said material is 'obscene' or not, 'Contemporary Community Interest Test' has been applicable in America. The United States Supreme Court in \textit{Miller v. California}\footnote{17} has laid down 'contemporary community standard test' to define an obscenity offense. The important issue was again come before the United State's Supreme Court in \textit{Jenkins}\footnote{18} when constitutional validity of the Georgia's obscenity law was challenged. In this case, manager of the theater was charged under Section 26-2101\footnote{19} of Georgia obscenity law. The manager was charged 'with the offence of distributing obscene material' for knowingly exhibiting a motion picture 'Carnal Knowledge' on January 13, 1972 and following charges were levied against him that he was instrumentality in distributing the picture involving -

\begin{itemize}
\item[a.] an act of sexual intercourse,
\item[b.] a lewd exposure of the sexual organs,
\item[c.] a lewd appearance in a state of partial complete nudity,
\item[d.] a lewd caress or indecent fondling of another person.
\end{itemize}

\footnote{15}{(1968) LR 3 QB P. 87.}
\footnote{16}{Regina v. Martin Seeker & Warburg Ltd., (1954), cited from Dhokalia, H.C., 'Right to Freedom of Speech and Expression in India', P. 167.}
\footnote{17}{413 US 25 (1973)}
\footnote{18}{Jenkin v. Georgia, 418 US 153 (1973)}
\footnote{19}{Section 26-2101 of the Georgia Obscenity Act runs as under -

Section 26-2101 - \textit{Distributing obscene materials} Sub-Section (a) states: "A person commits the offence of distributing obscene materials when he... exhibits or otherwise disseminates to any person any obscene material of any description, knowing the obscene nature thereof." Sub-Section (c) provides that, "(material) not, otherwise obscene, may be obscene under this section if the distribution thereof... is a commercial exploitation of erotic (sexual desire) solely for the sake of their prurient appeal." Sub-Section (d) provides that, "a first offence under the section shall be punished as a misdemeanor and that any subsequent offence shall be punished by one to five years' imprisonment and/or a fine not to exceed $ 5000."}
The jury found the manager guilty and passed the verdict imposing fine of $759 US dollar and sentenced to 12 months probation.20

But the manager preferred an appeal in US Supreme Court challenging the constitutionality of the Georgia Obscenity Act on the ground that the said Act violates the rights conferred by 1st amendment of US Constitution. The First Amendment of US Constitution guaranteed that 'Congress shall make no law abridging the freedom of speech, or of the press'. Thus the Constitution of US conferred the right to freedom of Speech on the appellant.

However the Supreme Court of Georgia by the divided votes said that the First Amendment to US Constitution does not protect the commercial of 'hard core' pornography. It should be noted down that the definition of obscene material that appeared in the said Act in language similar to that of the definition of obscenity set forth in US Supreme Court's plurality opinion in *Memoirs v. Massachusetts*21 as:

"Material is obscene if considered as a whole, applying community standards, its predominant appeal is to prurient (unhealthy) interest (in sexual matters), that is, a shameful or morbid (unnatural, unhealthy) interest in nudity, or excretion, and utterly without redeeming social value and if, in addition, it goes substantial beyond customary limits of candor in describing or representing such matters."22

However, on screening the film to make an independent assessment, as mandated by Miller,23 the court said that -

".....carnal knowledge" (sex) could not, as a matter of constitutional law, be found to depict sexual conduct in a patently offensive way, and that it is therefore, not outside the protection of the first and Fourteenth Amendments to US Constitution because it is obscene;"

The court applied the constitutional standard, held that the Georgia obscenity statutes under which appellant Jenkins was convicted are invalid and Jenkins conviction was set aside. In absence of distribution to juveniles or obtrusive exposure to un-

---

23 413 US 15 (1973)
consenting adult, the First and Fourteenth Amendments prohibit the State and Federal Governments from attempting wholly to suppress sexually oriented materials on the basis of their allegedly 'obscene contents'.

So far as the American stand on 'obscene' and 'pornographic' material is concerned, it should be noted down that neither the similar wording have been used under Art. 19 (1) (a) of the Constitution nor vide protection has been granted by the Constitution of India to its citizens. At the same time, Art. 19 (2) impose the restrictions on freedom granted by Art. 19 (1) (a) where the world 'Morality', 'Decency' have been used as criteria for imposing reasonable restriction in Right to freedom of Speech and Expression.

Thus, the both legal system has evolved its standard on different lines and so far as applicability of American Standard of word 'obscene' & 'pornographic' material in India, it is hardly tenable. Because in India one of the ground to impose reasonable restriction on Right to Freedom of Speech & Expression is 'Morality' which is not present in US Constitution. The difference between First Amendment in US Constitution and corresponding Art 19 (1) (a) of the Indian Constitutional Law was noted by Douglas J. in 

*Kingsley Corp. v. Regents of the University of New York.*

In the said judgment, the position of Right to Freedom of Speech & Expression with special reference to pre-censorship was considered by Hon'ble Judge. In holding that all pre-censorship of cinema films was constitutionally void (in America), he said:

> "If we had a provision in our Constitution for 'reasonable' regulation of the press such as India has included in hers there would be room for argument that censorship in the interest of morality would be permissible." 

In short, the test applicable in India to decide a particular material as 'obscene' or 'pornographic' is examined solely on different index and constitutional approach for both the nation is quite differ from social and historical background. It may be due to different socio-political and economical situation exited in India that differ that from other foreign nations.

---


25 Art 19 (2) was redraft and modified and retrospectively amended by the Constitution (1st Amendment) Act, 1951. For more details see original Constitution of India before and after passing of 1st Amendment. By this amended some more ground were added in the list and it made comprehensive to some extend.

26 360 U.S. 684, 698, 3 L. Ed. 2d. 1512. 1522.

27 360 U.S. 684, 698, 3 L. Ed. 2d. 1512. 1522.

4.2.4 The Test of Obscenity & Pornography - Under English Law

It should be borne here in the mind that neither the word 'Pornography' nor 'Obscene' has been defined in the enactment, though word 'Obscene' has been used both in Section 292 of Indian Penal Code, 1860 and in Section 67 of Information Technology Act, 2000. A careful perusal of the provisions of section 292, I.P.C. (1860) would reveal that the word obscenity has not been defined. However, judiciary has attempted to explain the word obscenity by laying down tests to indicate which act and under what particular context would come within the arena of obscenity.

It should be noted down that the wording of Section 67 of Information Technology Act, 2000 constructed on the same line with Section 292 of Indian Penal Code, 1860. As Indian penal Code, 1860 has been modelled upon the English law, it would be essential to analyse the test of obscenity applicable in England. The test applicable to examine whether a particular material is obscene or not has been given by Cockburn, C.J. of the House of Lords in R.V. Hickin, which is perhaps the earliest case on the subject, as follows:

"...The test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influence and into whose hands a publication of this sort may fall. It is quite certain that it would suggest to the minds of the young of either sex, or even to persons or more advanced year, thoughts of a most impure and lubricious character."

Therefore, the test applicable in England is based on 'immoral influence' and 'to deprave and corrupt mind'. It should be noted down that the test of 'obscenity' is too much depends upon the moral standard of society and as there is vast difference between Indian society and European society on the basis of standards of morality, the test of 'obscenity' and to judge whether any material is 'pornographic' or nor would definitely differ. It is therefore essential to examine the test applicable in India.

---

29 45 of 1860.
30 Act No. 21 of 2000.
4.2.5 The Test of Obscenity & Pornography - Under Indian Legal System

As stated earlier, as Indian society and cultural background is quite different from western world. Therefore, Indian response to the pornographic and obscene literature definitely differs from the western countries. Again, obscenity became a subject of constitutional interest since it illustrates well the clash between the right of the individual to freely express his opinions and the duty of the state to safeguard the morals. The Indian response at first place can be collected from Ranjit D. Udeshi v. State of Maharashtra case. The Supreme Court of India dealt with the subject when the Appellant, one of the fourth partners of a firm owning a book stall named 'Happy Book Stall' in Mumbai, was convicted by the Magistrate under Section 292 of Indian Penal Code, 1860 along with the other partners for being in possession of an obscene book called Lady Chatterley's Lover (unexpurgated edn.) which inter alia contained obscene matters.

The decision of the lower court was upheld by the High Court and Supreme Court. While dismissing the appeal, Justice Hidayatullah speaking through the court said:

"There is no loss to society if there was a message in the book. The divagations with sex are not a legitimate embroidery but they are the only attractions to the common man. When everything said in its favour we find that in treating with sex the impugned portions viewed separately and also in the setting of the whole book pass the permissible limits judged of from our community standards and as there is no social gain to us which can be said to preponderate, we must hold the book to satisfy the tests we have indicated above."

As seen earlier in Jenkins case, the applicant raised the plea of Constitutional validity of the said section saying that it violates Art. 19 (1) (a) of the Constitution of India. Thus as regards, the contention of the petitioner that section 292 of Indian Penal Code, 1860 violates Article 19 (1) (a) of the Constitution, since it puts

36 Jenkins v. Georgia, 418 US 153 (1973)
37 Art. 19 (1) (a) runs as under - 'All citizens shall have the right to freedom of speech and expression'. But the freedom conferred is subject to Art. 19(2) which imposes restrictions.
restriction of the Freedom of Speech & Expression, the court said in the negative. Justice Hidayatullah speaking for the court said:

'No doubt this article (referring to Article 19) guarantees freedom of speech and expression but it also makes an exception in favour of existing laws which impose restrictions on the exercise of the right in the interests of public decency and morality.'

Thus 'public decency' and 'morality' is the ground for imposing the restriction on the right to Freedom of Speech and Expression of citizens. Proceeding further on the same line Hon'ble Judge commented:

'Speaking in terms of the Constitution it can hardly be claimed that obscenity which is offensive to modesty or decency is within the constitutional protection given to free speech or expression, because the Article dealing with the right itself excludes it. That cherished right on which our democracy rests is meant for the expression of free opinions to change political or social conditions or for the advancement of human knowledge. This freedom is subject to reasonable restrictions which may be thought necessary in the interest of the general public and one such is the interest of public decency and morality. Section 292, I.P.C. manifestly embodies such a restriction because the law against obscenity, of course, correctly understood and applied, seeks no more than to promote public decency.'

Some other grounds have been evolved in by the Supreme Court to decide whether the material is obscene or not. In Samaresh v. Amal Mitra, the appellant, a well-known Bangali writer, was prosecuted under Section 292, I.P.C. for writing and publishing a novel under the caption 'Prajapati' in a Bangali journal. While allowing the appeal and setting the conviction, the court developing three criteria to held that in judging the question of obscenity,

1. the Judge in the first place should try to place himself in the position of the author and from the viewpoint of the author (and) the Judge should try to understand what is it that

---

39 AIR 1965 SC 881 (885) (pars 7 and 8)
40 AIR 1986 SC 967.
the author seeks to convey and whether what the author conveys has any literary and artistic value.

ii. the Judge should thereafter place himself in the position of a reader of every age group in whose hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have on the minds of the reader.

iii. a Judge should thereafter apply his judicial mind dispassionately to decide whether the book in question can be said to be obscene within the meaning of 292, I.P.C. by an objective assessment of the book as a whole and also of the passages complained of as obscene separately.

iv. In appropriate cases, the court for eliminating any subjective element or personal preference which may remain hidden in the subconscious mind and may unconsciously affect a proper objective assessment, may draw upon the evidence on record and also consider views expressed by reputed or recognized authors of literature on such questions if there be any for his own consideration and satisfaction to enable the court to discharge the duty of making a proper assessment.41

A novel written by a well-known writer of novels and stories, by which the author intends to expose various evils and ills prevailing in society and to pose with particular emphasis the problems which afflict the society in various spheres, cannot be said to be obscene merely because "slang and unconventional words have been used in the book in which there have been emphasis on sex and description of female bodies and there are narrations of feelings, thoughts and actions in vulgar language." 

(It may be possible that) Some portions of the book may appear to be vulgar and readers of cultured and refined taste may feel shocked and disgusted. Equally in some portions the words used and description given may not appear to be in proper taste. In some place there may have been an exhibition of bad taste leaving it to the readers of

experience and maturity to draw the necessary inference but certainly not sufficient to bring home to the adolescents any suggestion which is depraving or lascivious.\footnote{Gaur K.D., 'A Textbook on Indian Penal Code', Universal Law Publishing Co. Pvt. Ltd. 3rd Ed. (2004) PP. 362-366.}

The author has written this novel for all classes of readers and it cannot be right to insist that the standard should always be for the writer to see that the adolescent may not be brought into contact with sex. If a reference to sex by itself in any novel is considered to be obscene and not fit to be read by adolescent; adolescents will not be in a position to read any novel and will have to read books which are purely religious.\footnote{AIR 1986 SC 967 (983, 984). See for commentary, Gaur K.D., 'A Textbook on Indian Penal Code', Universal Law Publishing Co. Pvt. Ltd. 3rd Ed. (2004) PP. 362-366.}

A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novel, whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influence.\footnote{Gaur K.D., 'A Textbook on Indian Penal Code', Universal Law Publishing Co. Pvt. Ltd. 3rd Ed. (2004) PP. 362-366.}

4.2.6 The Electronic Technology create the greatest threat

Thus is should be noted down that the test for considering whether a particular material is obscene or not is depends upon several factors. But the obscene material in printed form and obscene material in electronic form also differ in its magnitude and its effect. The electronic technology provides better option for animation, sound, reality effect, visual effect and mixing of various frames. Therefore it penetrates deeper into the mind of its audience. At the same time, the distribution and dissemination of electronic material is quite easier than printed material. The printed material for its distribution depends upon the physical assistance. When one requires circulating or moving any magazine or paper having obscene material in printed form, he is required to carry the same with him either physically or in container. Therefore it is quite easy to control such movement of circulation in case of printed material. Thus it is quite easy to control the printed material as it is in tangible form. Again, the movement of these printed material can be easily control either with person or with property, as the printed form material require physical transformation and physical environment for its realization and rationalization.
The same is not the case with electronic material. Electronic materials are in the shape of bytes and in digital forms. The bytes can be moved through optic fibers or even through air. Therefore, if one requires transferring any obscene material in electronic form from Delhi to Mumbai, he can send via e-mail with attachment files and can be downloaded from any part of the world. At the same time, even most of the time the e-mail ID is also fake and originator cannot be traced out. This makes pornography or obscenity in electronic form more dangerous than ever.

Apart from the difference in its effect on audience, the obscene material in electronic form is also dangerous from other reasons. First it is difficult to trace out. The investigative machineries require seizing the hard disc, computer, mobile or mechanical device. Again even after seizure it would not be sure that prosecution would be able to get it in printed version. Today there are so many software's available in the market, which periodically washes out the files. Again there is software that deletes all cookies, Internet files from the computer whenever it is restarted. Thus if culprit successfully closed down the system, it is difficult to trace out any clue of its presence. Particularly most of the Cyber café are equipped with such software's. Secondly, as electronic material can be easily moved in any part of the world and can be downloaded, most of the time, it is not needed to carry it along with. Thus if person wanted to have obscene material at Delhi, he will not take risk to carry those material with in. Instead of it, he will upload the material from the place he live e.g. from Mumbai and whenever he would be in Delhi, he will download the same. He will be risk free!!

The third problem with pornographic or obscene material in electronic form lies with its access. Section 292 of Indian Penal Code, 1860 and Section 67 of Information Technology Act, 2000 also make publication and distribution of obscene material criminally liable. Therefore, if any person is having any obscene material at his shop, in his bag, suitcase, on any magazine in his hands and he is traveling into bus, or on bus stand, on railway platform, he can be taken into custody. But in case of electronic material, person will always try to have this material either on CDs, Floppy, pen drive, hard disc magnetic tape which require computer forensic lab to find out its whereabouts. Thus the person having thousand of nude photographs, a complete film on CD (Compact Disc) with him he can be fearlessly move on any public place without a fear of getting arrested.

\[45\text{ of 1860.}\]
The latest incidence is more shocking. One of the students of IIT from Lucknow had taken nude clips of his girlfriend and circulated amongst his friends via MMS a Movie clip Massager System available in Mobile instrument. Thus within couple of hours, all friends circles are having 2 to 3 minutes clips of obscene nature secretly stored in their mobile. In Aurangabad, two shopkeepers were arrested who were indulged into uploading porn pictures in Mobile phones on payment. Thus in the present day, it is quite easy to have pornographic and obscene material with any person. Incidentally, parents are quite careless and they are allowing their teenager pupil to have Mobile phones with them, though it is unnecessary. Even filthy jokes, cartoons and other vulgar material are quite often shared amongst the friends on Mobile via SMS.

Thus in this contest, the electronic material is now so easily available and accessible to any person provided that he is having any electronic device with him which is having facility of storage. Thus it is possible that the teenager child can have vulgar chat with his/her friend and can share the nude photographs via Internet and can view any websites secretly sitting in his/her study room posing that he/she busy is doing his/her homework!!!

The major proportion of pornographic material targeted or meant to those of child. Either they are an instrumentalities or target of pornography. Because of their tender age, and unable to understand the impact of sexual sentivism, they fail to tackle the pornographic material and via Internet they may fall victims of those websites which are harmful for their tender mind. In this regard, law, particularly Indian law, can go too far to protect these future general from child pornography as they have very easy assess to Internet without any 'gatekeeper' or 'watchdog' to surveillance and proper scrutiny.

Generally it has been observed that basically, kids visits Internet for a fun. It includes games, cartoons, wallpapers or some other things that attract their basic adolescent instinct.

The model for protecting the children from child pornography can be adopted from American Department of Justice, National Centre for Missing & Exploited children who launch effort aimed to distinguish the 'Misleading Domain Names'. As part of an ongoing effort to crack down on websites that deceive minors into viewing pornographic and obscene materials, the U.S. Department of Justice and the National
Center for Missing & Exploited Children (NCMEC) announced on April 20, 2004, that the National Center's Cyber Tipline, a reporting mechanism for child sexual exploitation, will now feature the ability to receive reports from the public on misleading Internet domain names.46

The addition was prompted by a DOJ initiative, led by the Child Exploitation and Obscenity Section of the Criminal Division, to crack down on misleading domain names following enactment of the Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (the "PROTECT Act") on April 30, 2003.

So far as present Information Technology Act, 200047 with respect to pornographic material is concerned, Section 67 of the act prohibited 'publishing of information which is obscene in electronic form.'48 The word 'Obscene' has been used instead of 'Pornography'. The section has constructed on the line of Section 292 (1) of Indian Penal Code, 1860.49

Thus if both the provisions of Indian Penal Code, 186050 and Information Technology Act, 200051 Section 292 (1) and Section 67 respectively, it is clearly reflect that provision under Information Technology Act, 2000 has been construed strictly and enhanced punishment has been prescribed. Under 292 (1) of Indian Penal Code, 1860, for first time, punishment upto two years and fine upto two thousand has been

---

46 The new reporting feature was added to the National Center's Cyber Tipline, accessible at www.cybertipline.com or by calling 1-800-THE LOST (1-800-843-5678). Accessed on 22.01.2005 at 14:15:26.
47 Act No. 21 of 2000.
48 S. 67 of Information Technology Act, 2000 runs as under,
   "67. Publishing of information which is obscene in electronic form: - Whoever publishes or transmits or causes 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, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.
49 S. 292 (1) of Indian Penal Code, 1860 runs as under,
   "292. Sale, etc., of obscene books, etc. - (1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its terms, is, if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
   ..... shall be punished on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.
50 45 of 1860.
prescribed and for subsequent crime, five years punishment and fine up to five thousand has been prescribed. At the same time, under Section 67 of Information Technology, Act, 2000 five years punishment has been prescribed for the first time and fine which may extend to one lakh rupees and for subsequent crime, ten years punishment and fine which may extend to two lakhs rupees has been prescribed.

Thus in comparison with the relevant provision of Indian Penal Code, 1860, the present Information Technology Act, 2000 is more drastic towards criminal. This may be because the obscene material on Networking or in Electronic form is having greater mobility and can move even across the border, can easily handle, and have greater impact due to its visual effect on the audience.

There is also difference between the amount of fine prescribed by Indian Penal Code, 1860 and Information Technology Act, 2000. Under Indian Penal Code, 1860, the fine is prescribed is two thousands or five thousand as the case may be. But under Information Technology Act, 2000 it is one lakh or two lakhs as the case may be. Thus both these provisions clearly make difference between the material in any form other than electronic form and the material which is in electronic form. Thus material which is obscene but not in electronic form gets different treatment under section 292 of Indian Penal Code, 1860 and the material which is obscene and in electronic form may be prosecuted under Section 67 of Information Technology Act, 2000.

However, there is another provision which attract attention here. Section 64 & 65 of Indian Penal Code, 1860 prescribe the provision of imprisonment in lieu of non-payment of fine. Particularly Section 65 of Indian Penal Code 1860 limits the power of the court to impose the punishment in lieu of non-payment of fine. It prescribed that court cannot directs the offender to be imprisoned in default of payment of a fine shall not exceed one-fourth of the term of imprisonment which is the maximum fixed for the offence. Thus Section 65 of Indian Penal Code, 1860 fixed a maximum period of one-fourth of the term of imprisonment which can be awarded by the Court in

---

51 Act No. 21 of 2000.
52 45 of 1860.
53 S. 65 of Indian Penal Code, 1860 runs as under,

S 65. Limit to imprisonment for non-payment of fine, when imprisonment and fine awardable. - The term for which the Court directs the offender to be imprisoned in default of payment of a fine shall not exceed one-fourth of the term of imprisonment which is the maximum fixed for the offence, if the offence be punishable with imprisonment as well as fine.
a particular case, if the accused fails to pay the amount of fine levied by the Court in addition to the imprisonment already awarded.

Despite the difference in the penalty prescribed under these two different legislations for publication and distribution of obscene material, the effect of these two mediums also differ on the audience. As we have already seen at numbers of places in this investigative writing that in Cyber spaces everything move in the form of electron whereas in print culture, everything is on paper. Therefore, it is very easy to trace the obscene material in printed form and prosecution machinery can easily control by adopting traditional technique i.e. seizure, arrest etc.

Today, adult entertainment is the largest industry on the Internet. It is estimated that over half of Internet traffic is pornographic. An innocent keyword typed on some search engines or wrongly spelling a Web site's name can lead children or adults into sites that are shocking and often difficult to escape. A child innocently researching a paper for school may accidentally come across pornographic content due to its sheer abundance on the web. Monitoring or blocking software which you install is a limited solution as new adult sites are launched daily in abundance. When children come across such sites, they may get upset, embarrassed, frightened or unfortunately even corrupted by them. This could affect the child's psychology, self-esteem. Parental watch & control is always necessary, and should be consistent. It is always advisable to install filtering software which automatically block such sites and keep updating it thereafter.

The comprehensive legislation on the same line is very essential in India which can ensure the protection of children against pornography. Because, still today in India, there is lack of 'Computer educated parents' which can take care of websites, films, and surfing of their kids. Most of the time, they are not aware about the 'A B C' of computer which create a maximum chance of these young ones to expose to children pornography. Both protective and reactive approaches can be adopted to control the pornography and obscenity in Cyberspace. Because, law only can prosecute, and it can not revert back the process, thus, it is better to protect from the happening of such

---

incidences, and even legal framework can be developed for such guarding the society against pornographic literature.

4.3 Cyber Stalking

Initially, and to great extent, Cyber stalking can be considered as a type of nuisance. But it cannot be underestimated merely as nuisance. The harassment it cause, and the effect on the victim made it most dangerous and rather more irritating type of crime in the world and particularly growing alarm in India too. For victims, it crate nightmare, though victim may not most of the time netizen and Internet visitor. Though a couple of year before, question could be raised that whether cyber stalking, cyber harassment were prevalent in India? But now it seems to be become more realistic and alarming day by day and there are growing number of cases of cyber-stalking across the world and in India, too.

"Cyber stalking happens when a person is followed and pursued online, privacy invaded, and every move watched. Cyber stalking usually occurs with women, who are stalked by men; or children, who are stalked by paedophiles. It is believed that over 75 per cent of the victims are females, in a form of harassment that can disrupt the life of the victims and leave them feeling very afraid and threatened....with 19.5 per cent of online stalking translating into offline offences, cyber crimes can spill over to the real world with very real consequences."

4.3.1 Cyber Stalking - What it mean?

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

---

58 For e.g. Ms. Ritu Kohli, A Delhi based Indian lady, was not aware about this phenomenon and not aware about cyber-world, too. She kept getting obscene calls from everywhere, and people promptly talked dirty with her. In this case Manish Kathurin was stalking an Ms Ritu Kohli by illegally chatting on the Web site. This is probably first case of cyber stalking in India. For more detail, see, http://www.indianchild.com/cyber_crime_in_india.htm Accessed on 22.07.2005 at 18.11.25
60 http://www.cyberpolicebangalore.nic.in/cybererimes.htm Accessed on 15.08.2003 at 06.36.45
Cyber Stalking and harassment are malicious activities directed at a particular person. Tentatively, Cyber stalking is when a person is followed and pursued online. Their privacy is invaded, their every move watched. It is a form of harassment, and can disrupt the life of the victim and leave them feeling very afraid and threatened. Stalking is, by literary, mean to follow. Thus when any person intentionally pursues another in the cyber-space, it can be broadly termed as cyber-stalking. These persuasions most of the time create irritation, harassed, develop anxious feeling, annoyance and frustration, too, to the victims, particularly and especially women and children and in rare cases, mentally and emotionally weak persons fall pray to these cyber stalkers.

Several factors work in this phenomenon. Generally, cyber-world fabricates visual reality where netizens breathe. Web wide world interlinking provides a base for interaction where people try to correlate it with real world. With the complex mind, either superiority & inferiority complex, psyche, ego, or under emotional or sexual sensitivity, or to show their brainpower, these cyber-stalker either follow, misled, deceive, defraud, hoodwink, their target. The problem is appeared to be more dangerous because cyber-stalker does not have to come out of their home, search their prey or physically roam around the street. At the same time they are fear-free of regulatory authority on the web since they are sure that they can’t be trap, identify, or get detected in the cyberspace. Since the cyber-world spread world wide, they can attack from any corner. They may be located another hemisphere, or opposite side of world or sitting in next cabin of cyber café. He may be the stranger, friend or even relative, or in rare cases family member too!!! Incidentally, maximum occasions of cyber-stalking are motivated by sexual desire and targeted at women (generally housewife either married or unmarried), children (generally teenagers), and feeble-minded persons. Cyber-stalkers are of either sex and they generally attack the opposite sex victims but the evidence reflected that rarely the cyber-stalking trap to the victim of same sex. It is believed that 75% of the victims are female, but men are also stalked. The statistical figures of cyber-stalking can hardly be estimated and thus based on assumptions as most of the case remains undetected or unreported.

It is difficult to predict exact cause of cyber-stalking. However, it is observed that cyber-stalkers are under a sort of phobia and used of getting benefited by lacuna of

cyber-system. As most of the Internet population in cyber-world are inexperienced, neophyte, unaware of netiquette & Internet security, the cyber-world appears to be deserted land for these cyber-stalkers where they can roam freely without passport and visa, enter without authority & identity or with fake identity.

4.3.2 Cyber Stalker - Who are they?

It is even equally difficult to predict about cyber-stalkers. Why they commit cyber-stalking? What are the motivational factors? What cause them to follow their victims? What is their behavioural pattern? And what is the net gain of cyber-stalking?

Cyber-stalker may be categories by different ways. Any attempt to categorise the cyber-stalkers create difficulties due to less information available about them and lack of research oriented work in this area. Even the categorisation has done so far show overlapping. Tentatively, they can be categorised on behavioural basis, or on the basis of the intensity of the damage they cause, or even on the basis of the species they targeted.

Some of the cyber-stalkers are works under a sort of passion. They fall in love, share their fantasy, and create mania with their target or sometime identifying themselves with other personified identity. They used to develop relationship on web, create some tie and pursue their desire on net. Though such relationship are not everlasting, and bound to end after short conversation, these cyber-stalkers never fail to pursue for longer relationship or follow their target, collect more and more information and involve too much. They share problems, create illusionary scene and try to develop attachment and feel the cyber-world as real life. During the course of time, a mania develops in them and they started to commit cyber-stalking as an obsession. It is advisable, therefore, not to give, share, develop any kind of information, relation or conversation with stranger on net, particularly to women, teenagers, and those not having expertise on net. However, cyber-awareness is still a talk to be achieved. Netizens are advised not to mislead by fictitious belief that cyber-stalkers are in love and they are harmless, temporary, or casual incidences which is often proved wrong in most of the cases.

Another category of Cyber-stalkers is of those under hallucination. Either during chatting, conversation, and these cyber-stalkers accidentally (or sometimes due to surfing in common zone) comes across their target. During a short span of time they start to follow their target. They are either suffering from mental illness like
schizophrenia or some phobia and feel their victims very close to them. They mentally feel & tie up with their target and keep pursuing them on net. Sometime these feeling are like love or sex that pulls them towards their target. They think that their victims love them and favour longer relationship, though they never met and despite the victim is either try to avoid them or even unaware about their feeling and pursuing. Because, *the dissemination of hate and racist speech has a more general focus, but can be equally traumatic for those it targets, and is becoming more widespread.*

Psychologically, it is believed that such types of cyber-stalkers are loner and their choice of victim is isolated one. They are in search of single, bored, frustrated housewife, or growing teen or some sexually frustrated target that can be trapped quite easily. It may be possible that such cyber-stalkers may accidentally get linked to softhearted, mild and sympathetic persons who ever try to help others in their difficulties. In such situation, these cyber-stalkers make a cry of their pains and problems and get involve their victim with them. Initially, victims remain innocent and works under just humanistic and sympathetic ground but gradually it lead into their ultimate exploitation. The victim class contain housewife, doctors, psychiatric, teachers, nurses, social workers, those in noble profession or even the person who ever fascinated with doing something new for others. Once trapped by these cyber-stalkers, it is very difficult to toss them off.

Some of the cyber-stalkers can also be put into revengeful category. A sort of feeling to get revenge, insult, teach a lesson, setting a score with victims, stimulates particularly the cyber-stalkers of this category. Generally the cyber-stalkers are dictated by any incidence of real or imaginary life. They feel that they are exploited, subjugated, or victimised and thus they are packed with revengeful inspiration. The person who commits these "cyber-stalking" something under the impression of victimisation could argue that they have the right to express their feelings however they want to on the Internet.

The college friend, the ex-fiancé, ex-spouse, business rivals, close family friends, cousins or employee too may become future cyber-stalkers for the person. As the mind set-up of this person is of such type that they cannot digest any humiliation or degradation, or they are so much sensitive to take it lightly or in sporty manner, they adopt a way to degrade their target via net. As net provide so much of facility, that they can set a score without being get detected or investigated, they can feel better to set a

---

score by this means. These categories of cyber-stalkers are also fear to get identified and lack courage to settle the things face to face. Therefore they adopt a comparatively easy way to put their target under humiliation, degradation, insult or even under nightmares. The following incidence might be quoted as an example:

>A case occurred in California is as follows: A 50-years-old former security guard used the Internet to solicit the rape of a woman who rejected his romantic advances. He terrorized his 28-years-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her.65

Thus cyber-stalking may create nightmares in the life of a victim. Again, if the wrong messages has been spread in the public at large about the victim may debase him/her in the eyes of other at the same time people may harasses the victim as mentioned in above case and may advance sexual proposals. However, in most of the cases, victim remained unaware about the misuse, twisting and defamatory literature on the Internet.

Consider another alarming and eye-opening example from India. This is the news flash from famous daily on the Internet.

**Woman's face morphed on lingerie model's torso**66

**TIMES NEWS NETWORK [WEDNESDAY, AUGUST 25, 2004]**

**NEW DELHI** : Crime branch officials are stumped by a complaint from a west Delhi-based woman who claimed her face was morphed on the torso of a lingerie model and put up on a US-based website that "promoted friendship between people of different sexes."

The woman is married and runs a fitness centre. Although the police managed to get her photograph removed from the website, they are unable to track the hacker who posted the

---

picture.

Deputy Commissioner of Police (crime) Tajender Luthra said: "After receiving the complaint, the cyber crime cell unit immediately wrote to the company managing the website. On our request, the complainant's photograph was deleted from the website. But when we asked them to provide us with information on the person who could have done so, they declined to do so."

In their reply to the Delhi Police, the company claimed they did not share information about their business with enforcement agencies. Luthra said in most of the complaints pertaining to cyber crime, the Delhi Police is facing problems with regard to websites hosted abroad.

"Indian-based companies are ready to cooperate with our investigations. But foreign-based websites always refuse to help us. In such cases, we have to close the case as untraceable," Luthra said.

According to the complainant, she learnt about her photograph on the website after she received calls on her mobile phone a month ago. The callers apparently asked her out and were willing to pay a cost for it. Initially, the complainant dismissed them as wrong calls. But when the frequency of calls increased, she got suspicious.

On inquiring from one of the callers, she learnt about the website. The caller also told her that her mobile number was posted on the website. After seeing the website personally, the complainant and her husband approached the crime branch and sought help.

After failing to solve the case technically, the Delhi Police has resorted to traditional methods of investigation. Believing it to be the handiwork of a disgruntled employee of the complainant, the police have sought a list of her former employees. The police are trying to verify their credentials.
Another incidence of cyber stalking took place in Aurangabad, two software engineers at a Computer Institutes have been alleged of posting indecent profiles at some Yahoo website. The profiles belonged to female students of their institute, which included their phone numbers and addresses.67

This raised several alarming signals about Cyber-crime in India. Following points may be considered on these issues;

1. There are growing incidences of cases of cyber-stalking in India, though mostly got undetected due to ignorance of people, some are unearth due to complaint made by people. However, as there is no patrolling, surveillances, detection, identification, arrest on suspicious ground, the police machinery only come into action after the commission of crime.

2. As stated in above cases, it is difficult to deal with cyber crimes in absence of international co-operation by other nations. Because, most of the websites are registered outside the India which not ready to co-operate saying, 'that the company do not share information about their business with enforcement agencies'. At the same time, these website companies can't be prosecuted as most of the laws of other nations do not fix any responsibility on them. They disclaim any liability of wrong, obnoxious, vulgar or any other information posted by user.

3. Now, it is dangerous to have any photographs, address, and identity clues easily within the reach on Internet. Because it can be misused.

Cyber-stalking also has its reflection in real life. Sometime, the cause root of cyber-stalking can be found in real life which then passes over to cyber-space and vice-versa. It differs from case to case and person to person. The field of cyber-stalking thus overlaps between online and offline zone depends of the course adopted by cyber-stalkers.

4.3.3 Cyber Stalking - Causes

Analogous with other sort of criminality, the basic questions of origin, causes and foundation of cyber-stalking can also be raised and also can be answered. Stalking is a phenomenon that can be seen offline also and there is nothing new about it. The

similar is the case in cyberspace. And with slight differences, its origin, causes and foundations can be equated with offline stalking.

Stalking has been committed by Stalkers with many reasons. Cyber-stalking is one of the ways of committing stalking via Internet. As web-world provide greater opportunity and coverage area to cyber-stalkers and comparative less risk of detection and identification, it proves boon to stalkers.

From the growing incidences and careful verifications of cases and its facts in hands, one of the major reasons of cyber-stalking can be traced as unfulfilled sexual lust. Internet is based on cafeteria approach and gives thousand of options to the netizens, it also provide a corner for those having sexual frustration in real life. For them, cyber-world may be asylum and sharing their pains and problems. Here they are in search of accomplice, ally and prey. The basic instinct for sexual lust pulls them out and they hurl themselves in the area. Unfortunately, cyberspace is still lack barriers, boundaries or any line of control and anybody, may it perpetrator or prey, stroll without visa and passport create the cyberspace full of possibility of 'find and fuck' for cyber stalkers. Even more unfortunate is that the cyber-technology provide access even to those cyber-neophytes, who are unaware about netiquettes, cyber-security and risk involve in such zones. Ultimately in cyberspace become the place for meetings, offers, proposals, deceiving, pursuing, trappings, and exploitations. The world without traffic rules, without licence, sniffer or cyber-police.

Though illusionary in its generic sense, the cyberspace feels like a real one and gives sensational feeling to netizens. The initial acceleration and absence of regulatory machinery add fuel to the fire. The sum total of this situation crates a solid platform and optional alternatives to cyber-stalkers. Internet is seems to be easy way for channelization of their emotion, legal or illegal.

4.3.4 What motivates a cyber stalker

i. Sexual lust: Sexual lust is the one of the cause of cyber stalker. Many of the person try to access to Internet in order to find sexual partner. As Internet provides chat rooms, it is very for them to chat in the categories of their choice. Most of the time, in order to satisfy the fantasy, the netizens hurled into cyberspace. But once become addict of the chatting, or finding partner on the Internet, they use to purse the person in their friend list.
ii. **Hate, love, or any emotional imbalance**: Generally, cyberspace is full of different kinds of personal. In cyberspace person share their emotion, love, hate, or other kind of feeling. Internet world provide the person a different medium to satisfy his unfulfilled wants. Thus, if any person was having hated, violence feeling, cruelty in real world, he tries to satisfy it on the net. Whenever such person either produces their hate, love about anybody without any fear, as they are aware that their identification is very difficult.

If anybody shows sympathy to such person on the net, they become use of it and they show their desire to share their emotion each time. Suppose, any teacher, doctor, psychiatry on net show some sympathy such emotionally imbalanced person, he repeated ask for their sympathy. Thus such emotionally imbalance person become cyber-stalker during the course of time and pursue the person for sympathy. They follow, in either case, if accepted or repulsed.

iii. **Revenge**: As cyberspace is the world where it is very difficult to identify the real face of the person, it is very easy to take revenge. Generally, the cyber stalker aggrieved by the real life incidence or online incidence, take advantage of Amazons Area of cyber world. Aggrieved employee, frustrated lover, business rival are some of the categories of cyber stalker who commits cyber stalking on net to take revenge. They sometime paste photographs of obscene type, display the filthy character of their victims or put information about their lower living so that the person believing the information to be true, may pursue the victims and he get harassed. This way they want to fulfill their revenge.

iv. **Curiosity**: Curiosity is one of the basic quality of human being. Most of the cyber stalker does cyber stalking out of curiosity. While surfing, any person might get the e-mail ID of another person having opposite sex. In order to know more things, he/she use to follow her/him. Generally teenagers fall in this category.

v. **Superiority / Inferiority complex**: This is also one of the reason of committing cyber stalking. In real life, person may be
dominated or caused to be dominated by such complex psychological problem. Either they want to be get dominated e.g. slave. They use to search the person or personality which suited their fantasy and thus pursue their desire.

vi. **To execute unfulfilled desire:** This is also one of the way. The most of the person in chat room share certain common chat room where they pose themselves in the personality of their unfulfilled desire. While doing so, they pose themselves as teenage girl, doctor, politician, gangster, wife, or school going daughter, or even prostitute.

vii. **To satisfy any fantasy, that cannot be shared in real life:** Sometime the person is under certain reference group. He wanted to be looked like other person and on net he tries to show-off himself as that personality. Thus to satisfy any fantasy, that cannot be shared in real life, person commit cyber stalking on net.

viii. **Psyche:** Once the person become addicted of such phenomenon of cyber stalking, he becomes addict of it. A peculiar psyche develops in him and it becomes his habit. Thus under special type of habitual 'psyche', it is driven force for committing cyber stalking.

### 4.3.5 Legal strategies to check the cyber-stalking

Cyber-stalking is difficult to deal effectively in absence of trans-national developed criminal system. The problem to deal with cyber-stalking can be understood by considering real life incidences. Ms. Ritu Kohli, A Delhi based Indian lady, was not aware about this phenomenon and not aware about cyber-world, too. She kept getting obscene calls from everywhere, and people promptly talked dirty with her. In this case Manish Kathuria was stalking on Ms Ritu Kohli by illegally chatting on the Web site. This is probably first case of cyber stalking in India.\(^6^8\)

Generally, a cyber stalker looks for weaknesses in people. Therefore, to have sympathetic attitude on net may cause undesirable trouble. People looking for sympathy or wanting to make friends, find romance online etc., are an open invitation to many types of stalkers.\(^6^9\)

---


The online world is not too far from offline world. Therefore, any sort of harassment, threatening, disturbing in cyber space can be dealt offline. The act of causing stalking by stalker in cyberspace equally amount to breaking of law and there are a number of steps can be taken including police action. Generally, due to unawareness of cyber crime and effective mechanism to deal with, people find themselves helpless. It is unwise to waste a time searching what one can "do" to teach the lesson to cyber stalker. Taking help of legal machinery is prudence in this case. Instead of searching "Why" by victims, they should try to do "What" can be done against these stalkers.

The problem of cyber stalking is very serious in case of kids and teens. Generally working on the computer by these kids and teens are not under the surveillance of elders, and they do surf the net during working hours of their parents, they can easily fall prey to these cyber stalkers. It is advisable to the parents that they should both block such site, chatting messengers, and scrutinize the cookies periodically. Literate the kids and teens about the dangers, and making them aware not to leave any identification mark, address, or photograph on net may prove useful tip.

The same instruction is also useful to adults. As even the IT Act, 2000 is not provide effective remedy against cyber stalking, it is better not to chat with stranger, and even not to reply any e-mail from unknown source. If it is observed that anybody is pursuing to kids, teenage member or spouse of your family, written police complain can be lodge to the Commissioner of Police of your city.

If anyone is harassing you or you kids by stalking them online & has begun to disturb you or put your life at risks, you must file a written complaint to the Commissioner of Police in your city. The victim can also report harassment mails to ISP (like VSNL, Satyam, etc) & e-mail provider (like Yahoo, Rediff, MSN etc.). Advice from technical savvy friends may be alternative. The most dangerous "I LOVE U" virus was traced by these methods. The Golden rule our parents taught us "Never talk to strangers" stays a golden rule in today's Cyber world!! And the BEST way to avoid getting stalked is to ALWAYS maintain a high level of safety awareness.

---

70 See the news on [http://www.indianchild.com/pedophile_jailed_for.htm](http://www.indianchild.com/pedophile_jailed_for.htm) The Mumbai police (November 2000) had helped rescue a 16 year old boy who was kidnapped by a lady pedophiles. She befriended him through a chat room.

4.4 Viruses

Viruses have potential to cause great security risk to the computer network across the world. This is another type of cyber crimes committed in cyberspace. Basically, it is in the category of crimes those committed against computers. A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses are computer programmes that migrate from computer to computer and attach to the computer's operating system.

According to The Information Technology (Certifying Authorities) Rules, 2000 Virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

It is a programme that infects a computer by inserting a copy of itself into the computer and damages the computer in some manger, generally without the computer user's awareness. Thus strictly speaking, Viruses itself cannot be treated as harmful, but when they enter into the computer system, either due to the inbuilt program or some logic, its activated into host system and start deleting, modifying, corrupting or even multiplying the computer program.

Most of the times, these led to the consumption of maximum memory of host's computer or corrupt the available data on the host computer. Apparently, these viruses are in hidden form and maliciously kept behind the curtain, wall of any other program so that when the victim download, transfer, transmit, and interchange any data he does not notice these viruses and innocently use the face program which is apparently seen. Such virus transplantation is dangerously affect the system of host without his knowledge.

72 Farooq (Dr.) Ahmad, 'Cyber Law in India (Law on Internet)', Pioneer Books, P. 323
74 See Explanation (ii) of Section 43 of the Information Technology Act, 2000; see also the Information Technology (Certifying Authorities) Rules, 2000 (Schedule V - Glossary).
A computer virus is a programme code which can attach itself to other programmes and corrupt data and damage hardware. In addition to infecting other programmes, the virus may damage data by way of data diddling, Trojan horses or logic bombs. A virus may do nothing more than temporarily interrupt the computer service to display a message on the screen, or it may bring down the infected computer system. Software or hardware containing a virus can come from many sources such as public domain software, bulletin boards, Internet, computer club software, a friend or colleague’s diskette, or commercial packages that have been tampered with. This crime can be minimised by incorporating virus scanning into the start-up of the computer system and scan any new software prior to use.76

As viruses are logical programmes, they grow faster. Once this logic gets click in the host computer it starts multiplying and can create havoc within a short span of time. Once it starts, it is difficult to control it. However, it does not mean that all viruses are dangerous. Sometime, it may remain inactive as the logic that has been created in viruses programs do not get activated and does not cause any substantial damage, except occupying space in the hard disc. But even a smallest virus can be proved fatal as sometime it may cause collapse of system including networking. Consider that a single virus may shut down all the counters of railway reservation creating a mess or it may give obnoxious messages on the screen of Hospital computers causing danger to patient life.

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.77 To understand the effect of virus in the computer networking, one has to imagine the viral attack in human body where it creates malfunctioning in the body and may collapse the system. And as most of the disease viruses are contagious and able to spread through air, water and soil, computer viruses are also contagious and able to spread via Internet networking or even through floppy's use for the purpose of transfer of data. Once viruses enter into a programme of any

76 Mishra (Dr.) R.C., 'Cyber Crime - Impacts in the new millennium', Authors Press Delhi 1st PB Edn. (2005), P. 89
computer, it attached itself with several other programs and whenever these host programs get executed, viruses' starts functioning.

Most viruses work by infecting other legitimate programmes and causing them to become destructive or disrupt the system in some other manner.\(^8\)

### 4.4.1 Types of Viruses

Basically, depends upon the way its works; viruses can be classified in following ways.

i. **File Infectors**: These types of viruses generally infect file system of computers but, though some can also design to infect program files. These viruses are attached to any program files and act arbitrarily. The program file includes command file or executable files having extensions .COM or .EXE. Sometimes these viruses can also infect program file for which execution is required. Among such file, it includes program files having extensions such as .MNU, .OVL, .PRG, .SYS etc. These types of file infector viruses can further be classified into two categories depend on their line of action. They may either be -

   a. **Direct action** - A direct-action virus selects one or more other programs to infect each time the program that contains it is executed. E.g. Vienna virus

   b. **Resident** - A resident virus hides itself somewhere in memory the first time an infected program is executed, and thereafter infects other programs when they are executed (as in the case of the Jerusalem 185 virus) or when certain other conditions are fulfilled.

ii. **System or boot-record infectors** : These types of viruses infect executable code found in certain system areas on a disk, which are not ordinary files. On DOS systems, there are ordinary boot-sector viruses, which infect only the DOS boot sector, and MBR viruses which infect the Master Boot Record on fixed disks and the DOS boot sector on diskettes. Examples include Brain, Stoned, Empire, Azusa, and Michelangelo. Such viruses are always resident viruses. Finally, a few viruses are able to infect both (the Tequila virus is one example). These are often called "multi-partite"
viruses, though there has been criticism of this name; another name is "boot-and-file" virus.

File system or cluster viruses (e.g. Dir-2) are those that modify directory table entries so that the virus is loaded and executed before the desired program is. Note that the program itself is not physically altered; only the directory entry is. Some consider these infectors to be a third category of viruses, while others consider them to be a subcategory of the file infectors.

4.4.2 Effect of Computer virus

The computer virus is self-replicating programme which spreads throughout a computer system, attaching copies of itself to ordinary programmes.\(^79\) The devastating effect of a virus can be well realized by Melissa Virus introduced in March 1999 whose author was successful prosecuted only to make it second successful prosecution in history of computer virus. Melissa Macro virus was hidden in a Microsoft Word attachment.

The virus was programmed in such a way that recipient would think that it has come from a known person. When the recipient opened the attachment, it was found to contain a list of pornographic web site passwords. The programme on its own would activate a macro that read that first fifty e-mail addresses located in the Microsoft Outlook e-mail programme and e-mailed itself to the fifty addresses with the message subject header important message.

It was estimated that this virus caused $80 million damages and its effect was so quick that Microsoft and Intel were forced to shut down their servers within 48 hours. One company alone having five hundred employees with computer networking received 32,000 e-mail messages in 45 minutes.\(^60\)

4.4.3 Computer virus and the Information Technology Act, 2000

The Information Technology Act, 2000 prescribed the provisions for computer virus. The term computer virus and computer contaminant has been compressively


\(^60\) See, Melissa Virus : Hearing of the Technology Subcomm. Of the House Science Comm. 105th Cong (1999). Quoted from Farooq (Dr.) Ahmad, Cyber Law in India (Law on Internet), Pioneer Books, p. 324.
described by the IT Act, 2000. The definition and explanation stretches the term to its widest possible meaning. The Section 43 prescribed penalty to the person causing damage to computer, computer system. Specifically, Section 43 (c) deals with the acts introducing computer contaminant or computer virus into any computer. If a person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, he shall be liable to pay damages by way of compensation not exceeding one Crore rupees to the person so affected.

The term 'Computer contaminant' and 'Computer virus' has been explained in the same section. The Computer contaminant means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network.

Computer virus means any computer instruction, information, data or programme that destroys, damages degrades or adversely affects the performance of a computer resource of attaches itself to another computer resource and operates when a programme, data or instructions is executed or some other event takes place in that computer resources.

Thus any person without prior authorized permission trying to modify, destroys, transmit data, damage, degrades or adversely affects the performance of computer resources is liable to be penalize. However, these terms are very wide. In routine working day, employees use to do lot of work during the course of his employment. Section 43 of the IT Act, 2000 if read with its widest possible dimension, may be applicable to those entire act done without permission of in-charge. Thus putting

---

81 The explanation clause of Section 43 of Information Technology Act, 2000 explained the term as follows:

S. 43 (iii) "Computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

82 Section 43 (c) of the IT Act, 2000.

83 Explanation (i) to Section 43 of the IT Act, 2000.

84 Explanation (i) to Section 43 of the IT Act, 2000.
scenarios wallpaper on the desktop of the computer, inserting game, audio files, or even changing directories, may come within the ambit of Section 43 of the IT Act, 2000. Because merely modifying the directories from one drive to another may affect performance of a computer.

Again the same section also explains the term damage. Damage means to destroy, alter, delete, add, modify or rearrange any computer resource by any means. However, the wording used in Section 43 of the IT Act, 2000 is very wide. It may cover those acts, for e.g. directly shutting down the computer, pressing any programming related keys during operation that give different results etc. Because the term damage includes any act that destroys, alter, delete, add, modify or rearrange any computer resource.

However, it should be noted down that the virus might be crept in even without the knowledge of user. Viruses are generally attached to any other files and they are remaining hidden. Therefore the dimension of Section 43 may attract even in the case of genuine person using any file without knowing that it is virus infected. Again, Section 43 of the IT Act, 2000 can be made applicable to the employees surfing the computer and accepting e-mails from head office, or downloading any information related to his office e.g. share market rate on the computer system. Because most of the viruses pass on the computer to computers via e-mails and other files downloaded from Internet. Web pages also contain virus, spread and therefore in such circumstances even innocent employees or person have to face difficulties.

So far as legal remedies to the problem of virus transplantation in the computer system is concern, the IT Act, 2000 prescribe the provision that can be effectively utilized to deal with and can be imposed penalty upto one Crore Rupees to the person. The main problem lies in the procedure if ascertaining the virus plantation, computer contaminant or any other things that may damage to computer, computer system or computer network. Because, when data transmission takes place in network, its route and journey is very difficult to trace out. As in most of the cases, the virus does not lay behind any footprint and they can be detected only with the help of antivirus software.

However, under Information Technology Act, 2000, Section 43 is only of civil nature and provide civil remedy prescribing penalty upto the limit of one Crores rupees to the culprit. The procedure to recover the money has also been prescribed under Section 64 of the same act. It is also possible that the act of virus transplantation can
also be prosecuted adopting remedy under Criminal law. Section 65 of the Information Technology Act, 2000 can be referred with where tampering with computer source documents has been made punishable with three year imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.  

Thus two different remedy one of civil nature and other of criminal nature is available under present the Information Technology Act, 2000. It should be noted down that the find under this section of optional and room for judicial discretion has been left. The person who fails to pay the stipulated fine imposed by the court can be treated under section 64 & 65 of the Indian Penal Code, 1860. Section 65 & 65 prescribed the way of awarding punishment in lieu (or in default) of non-payment of fine.

4.4.4 Some famous viruses

i) Armored virus  
ii) Companion virus  
iii) ExploreZip virus  
iv) Fast and slow infectors  
v) Macro virus  
vi) Melissa virus  
vii) Pakistani Brain  
viii) Polymorphic virus  
ix) Sparse infector  
x) Stealth virus  
x) Stoned-Marijuana  
xii) The Chernobyl, or PE CIH virus  
xiii) The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus)  
xiv) The Jerusalem virus a.k.a. "israeli" and "Friday the 13th"  
xv) The Cascade virus

---

Section 65 of Information Technology runs as under -

65. Tampering with computer source documents - Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, 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, shall be punishable with imprisonment up to three years or with fine which may extend up to two lakh rupees, or with both.

Explanation :- For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.
xvi) The Michelangelo virus also referred to by some virus
watchers as Stoned Michelangelo,

xvii) Virus hoax

Thus these are some of the examples of deadliest nature of virus which may
cause havoc to the system. It may halt the system and may cause collapsing the
overall computer networking and all system in row which are attached with
networking.

Besides it, there are some other categories such as salami attack, Trojan attack
which also cover in one of the form of virus attacks.

4.4.5 Remedies against virus

Basically, in computer world, best remedy is protection and not action. Because
the importance of data that damage due to virus can be equated with the compensation
granted by court or punishment awarded to the culprit. However the law provide the
remedy if any person found guilty of it. The Information Technology Act, 2000 under
Section 42 and 65 provided the remedy against the act.

4.5 Hacking

Hacking is also one of the forms of crime committed in cyber space via
computer system. 'Computer hacking is the accessing of a computer system without
the express or implied permission of the owner of that computer system.'
Hacking means unauthorised access to computers. Webster's Dictionary defines the term
hackers as a computer enthusiast who enjoys learning everything about a computer
system or network and through clever programming, pushing the system to its highest
possible level of performance. Hacking is computer trespass.

A person who tries to get unauthorized access without permission, or sometime
authorized persons getting the system by unauthorized way is called as 'Computer
Hackers'. The term can be equated too some extend like 'trespass' where person enter
on others property by unauthorized way. Computer hackers try to access the system of

---

86 Mishra (Dr.) R.C., 'Cyber Crime - Impacts in the new millennium', Authors Press Delhi 1st PB Edn.
(2005), P. 181
(2004), P. 332
Quoted from Farooq (Dr.) Ahmad, 'Cyber Law in India (Law on Internet)', Pioneer Books, P. 333.
(2004), P. 332
victim by breaking its security wall. Most of the time victims even don’t aware that his system is being hacked by computer hackers.

Most of time mere ‘thrill’, ‘curiosity’, ‘fun’, ‘intellectual ego’ or ‘superiority complex’ are factors what motivate the computer hackers for hacking. A hacker is a computer expert whose intrinsic curiosity persuades him to break into computers to satiate his quest for learning and knowing. A hacker does not include only an intruder with malicious design but also an enthusiast whose motive is innocent and sometimes even helpful in many respects.  

To show one’s knowledge and mastery over the computer, trying to prove ability and proving expertise, or making fun with friends, computer hacker make unauthorized access to the system of another. To play fun, or thrill of being able to outwit the security system of host computer motivate hacker to hack the computer system.

However, sometime hacking may be intentional and committed for accessing, tampering, stealing, modifying or even destroying the data of host. Sometime with ulterior motive of getting important information from the system of host, the computer hackers commit the hacking.

Many hackers are motivated by a sense of achievement; the very act of breaking into a computer system using their own mental effort is reward enough for them. There is a danger, however, that such ‘innocent’ hackers can cause damage to computer systems inadvertently and they may pave the way for other more malicious, persons.

Unauthorized hacking may be caused from remote distance, only the condition of accessibility has to be ensured. Thus if computer interconnectivity via any medium (either LAN or WAN) is available, anybody can be intruders in the system if he can break the firewall, or security system of the host’s computer. But most of the incidences of unauthorized access to the computer system have been found in any institution from within. As the employees of the bank or any company can easily access the computer as it is within its reach and manipulate the data. By far the greatest threat to a computer system comes from within - that is, from employees. In the majority of the cases some known person found involved in the process of hacking.

---

90 Farooq (Dr.) Ahmad, 'Cyber Law in India (Law on Internet)', Pioneer Books, P. 323
because for making use of the computer system of host, hacker must be aware about the use of the data he has to hack.

Just curious hacker may hack the system for mere amusement. He may add some massage, wander carelessly, and withered away. These hackers sometime tease the host about weak their security and hubbub how expert they are!! However, they are not dangerous. They may irritably disturb, but hardly cause potentially damage. Apart from these 'fun-lover' who just want to display their intelligence and ability of breaking security walls, there are some more sinister sides of computer hacking. The institutions that are operating in 'high-risk' zone area and dealing with sensitive activities are at stake due to these intruders. Nuclear Power Station, Defense systems, aircraft flight control and hospital records, known *safety-critical systems* may fall prey to these hackers. The importance of activities in which these institutions are involved are self-explanatory. If any hacker is able to have entry in the computer-networking o any nuclear power station can get important data. Or any hacker may get control of aircraft station and pass such instructions to pilot on their half way hurling hundreds of life in danger.

As stated earlier, hacking is not always harmful, but sometimes it is even helpful to know the performance of computer and find out the loopholes of the operating system. Therefore, many a time software company employee hackers to hack their security system so that they can know the drawbacks and can fortify their system. Therefore, depends on the intention and motive of their activities, hackers can be categories into three group.

i) Those hackers who try to hack the system to know the loopholes. Generally they are employed and paid for their work. They don't cause any harm to the system.

ii) The hackers who commit hacking out of curiosity, or just to display their knowledge. Even though they break the system, they generally do not sustain any harm to the host computer and abscond by giving massage, or praising themselves and making fun of the security aspects of host. Though these hackers cannot be ignored easily, but they are not enough serious than the professional hackers.

iii) The third categories of hackers are dangerous. They commit hacking for stealing, theft, and breakdown the system of host
and cause considerable loss the computer system of host. The intention of the hackers is very clear in this category and such hackers deserve strict punishment.

4.5.1 Remedies available against hacking

The Information Technology Act, 2000 prescribed the strict punishment for hacking. Section 65 of the Act runs as under

66. Hacking with Computer System : - (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakhs rupees, or with both.

Thus in India, the act of hacking is punishable under the law. However, there are some practical difficulties with the hacking. Hackers are generally very talented and they are very expert in dodging the system. Quite often their origin and location is difficult to verify and trace. Again, most of the time, their identity may be faked. Basically hackers hack the system with full knowledge that if he would get traced may be prosecuted. Thus the hacker's takes full precautions not to be get trapped. Again they are one step ahead of the implementing and executing machineries. Therefore, their knowledge and expert in the field is best shield for them to feel protected.

However, today, the world community is becoming more and more cautious against the hacker. The new technology of firewall, software and operating system and data protection modality is emerging on the scene to protect the system from the hacking. Even the new methodology of protecting like enhancing encryption level, data accessibility, checking the authenticity, separate lines and networking are used to protect the system from the hacking. Again with growing use of computer technology, the public support against the hacking is quite appreciable.

Thus though presently, hacking may be headache in the Cyberspace, but day will come when we may have at least authentic mechanism to protect the Cyberspace against such deadliest crime like 'hacking'.
There are some of the other well-known phenomenon which is broadly speaking
comes under the hacking. Because the basic modality in the crime commission is
nothing but trying to hack the website or computer of other persons.

4.5.2 Some categories of hacking

There are some of the other well-known phenomenon which is broadly speaking
comes under the hacking. Because the basic modality in the crime commission is
nothing but trying to hack the website or computer of other persons.

One such phenomenon is Web jacking, which resemble with the hi-jacking. In
this case hacker gains access and control over the website of another. Most of the time,
either by political or monetary motivation, hackers try to hack the website of another.
Even the data tampering, or damaging the data of government websites, or business
rivals are targeted by these hackers. The famous gold fish case is well known where
the information about gold-fish has been changed. Again, even the website of ministry
of information had also been web jacked by alleged Pakistani hackers.

Unauthorized access to the web sites or even the computers is also a different
category of hacking.

4.6 Cyber-squatting

Cyber squatting is another form of criminal activities have been notices in
cyberspace. Squatting, according to Cambridge Learner's dictionary means, 'buildings
that people are living in without owner's permission'. In general connotation, the word
'squatting' is used to describe 'someone sitting on the property of another'. This is
generally occurs in case of taking an advantage of others brand name, trade name or
some similar version to be get benefited in the Cyberspace. Generally advertisement
require 'catchy ideas' that is capable to attract the attention of viewer. Therefore,
similar domain names of famous brand or trademarks are generally used in to
Cyberspace. This is an attempt to get fraudulent benefit by creating anonymity.

With the emergence of the Internet as an advertising forum, recruiting
mechanism and marketplace for products and services, companies doing business
online have a strong desire to acquire domain names that are easy to remember and that
relate to their products, trade names or trademarks. For e.g. NASA. This is famous
name because it resemble with one of the space organization of America. This kind of
identification is essential to any business, both to conduct commerce in the Cyberspace and advertise and trap the attention of surfer.

Such type of acts are generally motivated to reassure the public that they are communicating with the intended source of goods and that they can make their purchases with the confidence that they are obtaining the genuine goods they are seeking from a known and reliable source. It seems a curious development that as the Internet encourages anonymity, so it has also increased the importance of online identity through branding.93

4.7 Spamming

Spamming is also one kind of harmful activities where person is harassed by activities by the spammer. There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song, "Spam, spam, spam, spam, spam, spam, spam, spam lovely spam, wonderful spam...." Like the song, spam is an endless repetition of worthless text.94 Thus spam is generally referred to such text which is worthless type. It is generally in the form of e-mail generally unwelcome, unexpected but passes on with commercial purpose. Thus where there is e-mail, there is spamming. Though it does not look logical why spam occurs in cyberspace, it is interesting to note down that the cost of sending each e-mail in a bulk charges so much less that spammers have no motivation to restrict their mailings to those in whom they are interested.

Spammers frequently use "stealthing" and "spoofing' to disguise the origin of their messages. As spam is unsolicited e-mailed documents consisting of advertising material for the lease, sale rental, gift offer, or other disposition of any realty, goods, services or extension of credit that meet both the following requirements:

i. the documents are addressed to a recipient with whom the initiator does not have any existing business or personal relationship,

ii. the documents are not sent at the request of, or with the express consent of, the recipient,

It is clear cut violation of privacy laws. Though there is legal as well as technological efforts are going on, spam still occur in cyberspace causing loss of

thousands of hours, manpower, and occupying the place in e-mail inbox without any use for the recipient.

"Phishing" or "Spoofing spam" is the constrain of e-mails messages with corresponding web pages designed to appear as existing consumer sites. Millions of these fraudulent e-mails distributed claiming to be originated from known source or legitimate source, but in fact deceptive. These types of behaviour are seems to be common in cyberspace now a day.

Surprisingly, the act covering the compute crime in India, i.e. is not contain the word 'Spam'. Thus, it is silent about it, though, the persons can be conveniently prosecuted under Section 42 of the same act under title, 'Damaging the computer'.

4.8 Worm

A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the ability to travel without any help from a person. A worm takes advantage of file or information transport features on system, which allows it to travel unaided. The biggest danger with a worm is its ability to replicate itself on system, so rather than computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in one's e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line. Due to the copying nature of a worm and its ability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers, and individual computer to stop responding. In more recent worm attacks such as the much talked about, Blaster Worm. The worm has been designed to tunnel into one's system and allows malicious user to control his computer remotely.\(^9\)

Most of the logic bombs are also used by the person, which starts functioning after clicking off special program it requires for its activation. If, the logical instruction has not been clicked, which initiate worm, it remain dormant within the system.

\(^9\) See, the official WebPage of 'The PC WeboPaedia', can be visted at http://www.pcwebopaedia.com Accessed on 23.02.2006 at 10:12:23
4.9 Emerging new types of Cyber crimes

It has been observed that in Cyberspace, various minor types of cyber criminality use to be observed. However, though it seems and cause negligible amount of loss to an individual or institution, but accumulation of these small amounts may head up to crores of rupees. The internet hours theft may cause any person a loss of hundred of rupees, which may not be important for a person, but in due course of time, around the cyberspace, it may causing total loss which may be in crores of rupees.

E-mail bombing is also another form of criminality, where person use to send so many e-mails in the inbox of victim, and within a short span of time, his inbox filled up with e-mails, most of which either obnoxious, or no use for user. It may be an individual or a company or even mail servers there by ultimately resulting into crashing.

Data diddling- is another kind of an attack involving the alteration of raw data. The phenomenon occurs when one start processing his computer. However, when processing one gets completed, it starts changing it back. In order to understand the data-diddling, one has to compare it with the electricity board which seems to be blinking on faced showing similar problem while the department was being computerised.

Another form of cyber crime is Denial of Service attack. In this case the computer of the victim is flooded with more requests than it can handle which cause it to crash. Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a distributed denial of service attack. Usually these attacks do not necessitate the need to get access into anyone's system. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

Electronic vandalism and professional forgery or counterfeiting is also seems to be a common phenomenon in the Cyber space, however, not too frequent in India.

Cyber-terrorism is distinguished from other acts of commercial crime or incidents of hacking by its severity. Attacks against computer networks or the information stored therein which result in "violence against persons or property, or at
least cause enough harm to generate fear" are to be considered cyber-terrorism attacks. However, it is difficult to derive at one definition of Cyber crime in absence of common agreement amongst the nations, as most of the criminal justice system is national in nature. Therefore, in boundary less Cyberspace, the concept of Cyber-terrorism is difficult to tackle. And in absence of common agreement amongst the nation, this term appear to be illusive. Thus, there are various types of new crimes are emerging into the cyberspace, some out of which needs entirely new look from jurisprudential point of view, and requires different treatment than traditional criminality.

4.10 Conclusion

While discussing about the cyber criminality, one thing prominent appears that Cyber crime can be discussed from two different angles.

First, we can conveniently categories some of the crimes which resemble with traditional crimes. Generally most of the crimes that resemble with traditional crimes in Cyberspace are those where computer is being used as an instrumental in crime commission. Speaking with example, theft, defamation, obscene material, terrorist activity, anti-government literature, illegal chatting etc etc.. All these forms of crimes are also present in the real world. Thus though these crimes are happened to be in Cyberspace, the criminal law is not totally ignorant about these types of crimes. In these types of crimes in Cyberspace the difference lies that these crimes are committed with the help of computers.

Incidentally, criminal jurisprudence has already develop some principles to tackle such criminality. Only difficulties lie with respect to procedural execution and trans-national jurisdiction. Thus at substantive level, these crime need not require comprehensive legislation and no separate region is essential to dealt with. However, we have to develop the procedural aspect where we can deal with proper investigation and legal execution. At the same time, due to non-recognition of nation boundaries in the cyber space, the problem of extra-territorial execution of law may arise. However, this can be tackled as we deal with the problems like war crimes, terrorist, smugglers, and pirates on high sea.

Secondly, some of the crimes are totally new to the criminal jurisprudence like virus, hacking, illegal access, swan and denial of service attacks. These crimes are totally new and there is no any substantive or procedural law, which can cover such
time of crime in cyberspace. It is essential to have comprehensive legislation to deal with such and other emerging crimes in cyberspace. Even it is required that new infrastructure and procedural should be developed to tackle such crimes.

_Thirdly, as the cyber crime phenomenon is global in nature, requiring several dimensions to consider, compressive efforts should be taken to define it._ Today, Cyber-terrorism is futile, if define from any nations point of view. As terrorism attract several jurisdictions, it is necessary to develop multi-national approach in the field of defining criminality. Thus, while any attempt to define Cyber-crime, which is multi-jurisdictional, it is necessary to adopt definition acceptable and compatible to other national systems.

_Lastly, procedural aspects of this criminality should also be kept into account. Because, as today, it is difficult to encompass the criminality within the national boundaries, it attracts the extra-territorial execution. If procedural technicality is not in tune with the global nature of crime, it is difficult to execute the legal mandate against the criminals._

_Thus in order to sustain again the deadliest crime of new millennium, a careful and plan study should be adopted._