CHAPTER-III

Punishment and Prevention to Cyber Crime

The growing danger from crimes committed against computers or against information on computers is beginning to claim attention in national capitals; In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that business and Governments must rely solely on technical measures to protect themselves from those who would steal deny access to or destroy valuable information.

OFFENCES PUNISHABLE UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The rising incidence of cybercrimes due to fast development of computer technology necessitated enactment of separate law for prevention and control of these offences. Therefore, the Parliament enacted the Information Technology Act, 2000 as a regulatory measure to tackle cyber offences in an effective manner. This Act is based on "UNCITRAL"1 Model Law on e-commerce, 1996 in furtherance of the United Nations General Assembly resolution urging the member States to

enact or revise their laws to create a uniform environment for regulating e-commerce at the international level. Thus the main object of the Act is to, "provide legal recognition for transactions carried out by electronic data, internet and other means of electronic communications commonly referred to as e-commerce as an alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents". In view of this objective, the Act also incorporates provisions for prevention and control of offences which are the result of e-commerce and e-governance. The relevant provisions are contained in Chapter IX and chapter XI of the Act.

(A) **Punishment Of Cyber Crime:**

**Penalty for Damage of Computer, computer system etc.**

If any person without permission of the owner or any person who is incharge of a computer, computer system or computer network-

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

---

2 Section 43 of the Information Technology Act, 2000.
(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other program residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder:

(h) Charges the service availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network,

(i) He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Explanation For the purposes of this section-

(i). "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:

(ii). "Computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii). "Computer virus" means any computer instructions, 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;

(iv). "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
Defines 'computer' as any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or a computer network.³

Clarifies that "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer program, computer instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication controls and other functions.⁴

States that "Computer network" means the interconnection of one or more computers through-

(i). the use of satellite, microwave, terrestrial line or other communication media; and

---

³ Sec. 2(1) (i) of the I.T. Act 2000
⁴ Id, Sec. 2(1) (i)
(ii). terminals or a complex consisting of two or more interconnected computers whether or not interconnection is continuously maintained.\textsuperscript{5}

Defines access as "access" with its grammatical variation and cognate expression means gaining entry into, instructing or complicating with the logical, arithmetical, or memory function resource of a computer, computer system or computer network.\textsuperscript{6}

Section 43 enlists various acts which if done without the permission of the owner or any person who is in charge of a computer, computer system or computer network, would amount to commission of cyber contraventions. If the act of the accused falls within any of these categories, damages up to one crore of rupees can be awarded to the victim.

The Information Technology Act, 2000 by virtue of Section 43 (a) has made authorized access to any computer, computer system or computer network without the permission of the owner or the person in charge punishable per se without any reference to the mala fide intention or knowledge and regardless of any loss which may or may not have occurred to the owner or person in charge of the computer. Thus, it is sufficient to prove that the intruder accessed or secured access to the computer, computer system or computer network, without the permission

\textsuperscript{5} Id, Sec 2(1) (j)
\textsuperscript{6} Id, Sec. 2 (1) (a)
of the owner or the person in charge. Any monetary or other kind of loss is not required to be proved by the complainant to claim damages under this section but the extent and magnitude of the loss caused to the complainant may act as a relevant factor to determine the amount of damages which can be awarded under this section. In United States v. Rice\textsuperscript{7}, where the defendant, an IRS agent, without any authorization accessed the computer of IRS to find Whether his friend was under investigation by the IRS was held guilty of the unauthorized access irrespective of the fact that no monetary loss was caused to The IRS.

Under this subsection even the attempt to secure the access has been made punishable, irrespective of the success or failure of the attempt. But, definitely, the success or failure of the attempt would go a long way in determining the extent of damages awarded under this section.

Section 43 (b) makes copying, downloading or extracting any data, computer database or information from such computer, computer system or computer network a contravention.

It attempts to protect the copyright of the individual over his creation in the digital medium. This downloading, copying or extracting of any data etc. can be held or stored in any removable storage medium including CD, DVD, floppy disk etc. Even if a person secures access to computer

\textsuperscript{7} 1992 U.S. App. Lexis 9562 (4th May 4, 1992)
with the permission of the owner or the person in charge but downloads, copies or extracts any data,

Computer data base or information from such computer, computer system or computer network without the permission of the owner or the person in charge of such computer, computer system or computer network, he would still be held liable for contravention under section 43 (b). This section would also cover the cases where though the person has asked the permission of the owner or the person in charge to copy, download or extract, say data 'A', but he copied, downloaded or extracted data 'B'

It is important to distinguish the terms "downloading"," copying" and "extraction" vis a vis digital content -

<table>
<thead>
<tr>
<th><strong>Downloading</strong></th>
<th><strong>Copying</strong></th>
<th><strong>Extraction</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieving a file digital content format remote computer, computer system or computer network.</td>
<td>Retrieving a file (digital content) from a remote computer, computer system or computer network and then saving it on either computer's hard disk or any removable storage medium.</td>
<td>Retrieving a file (digital content) from a remote computer, computer system or computer network and then selectively 'extract' part of the digital content.</td>
</tr>
</tbody>
</table>

Clause (c) of section 43 makes the introduction or causing to introduce any computer contaminant or computer virus like worms, logic bombs, Trojan Horse program etc. into any computer, computer system or computer network is a contravention for which damages up to the tune of one crore of rupees can be claimed by the owner or person in charge of the computer, computer system or computer network. The most famous example is 'love bug' created and disseminated in the year 2000 which damaged many computers. There is a famous saying: "Do not send a man where you can send a bullet". This saying can be modified in the cyber world as "Do not send a bullet where you can send a virus." It is immaterial to take into account that the guilty person was not aiming to attack the computer, computer system or computer network of the victim but of somebody else and it was by mere chance that the computer of the victim was affected. Nor it is important to prove that the person had the malafide intention while introducing or causing to introduce Computer containment or virus. In United States v. Morris\(^9\) student Robert Morris with the intent to demonstrate the inadequacy of security measures invented a program known as 'worm' and released it to the internet causing computers to crash at universities, military installations and medical research facilities. He was held to be guilty for violating the Computer fraud and Abuse Act of USA irrespective of the fact that he did.

\(^9\) 502 US 817 (1991)
not have any criminal intent. This decision shows that if an offence is committed intentionally, it is immaterial to find reason why it was intended. Clause (c) of section 43 has to be read conjointly with Explanations (i), (iii) and (iv) of the section. This subsection also covers a person whose computer is infected by a virus or contaminant without his knowledge and he sends the infected file to another person without any malafide intention or knowledge. Therefore it becomes essential to install anti virus Software for protection against virus.

Clause (d) makes causing damage or attempt to cause damage to any computer, Computer system or computer network, data, computer database or any other program residing in such computer, computer System or computer network as a cyber contravention. The damage includes the damage to the hardware as well as to the software. The damage may be done physically or virtually by spread of virus etc. or otherwise.

Clause (e) makes disruption and attempt to make disruption to computer, computer system or computer network a cyber contravention. The acts mentioned in clauses (c) and (d) may in certain cases be reason of the disruption to computer, computer system or computer network.

Clause (f) makes the denial or attempt to deny access to computer, computer system or computer network to any authorized person by any
means. The denial of access may be either physical or virtual. The Virtual denial of access may be either by changing the password, User's ID etc. or by any other means. It includes 'Denial of Service Attacks' whereby the attacker blocks the authorized users from visiting the targeted sites.

Clause (g) enumerates that providing assistance to any person for facilitating to access to any computer, computer system or computer network in contravention to law is a cyber contravention. Thus, any person who helps another person to access any computer, computer system or computer network in violation to the provisions of this Act or rules or regulations made thereunder is guilty of committing cyber contravention.

Clause (h) states that any person who charges the service availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network commits contravention. This clause provides protection against theft of internet hours or any other misappropriation of fraud where by the cyber criminal by changing, tampering manipulating the pass' word, user's ID etc. attains the benefits of the services availed by the rightful person.

One who steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer service code or resource with
the intention to cause damage will be liable to punishment under clause (i) of section 43 of the Act.¹⁰

The Information Technology (Amendment) Act, 2008 has inserted a new section 43A in the principal Act providing for compensation for failure to protect data. Where a body corporate (i.e. company or firm) possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls, or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way or compensation to the person so affected.

"Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or association as it may deem fit.

**Penalty for Failure to Furnish Information Return etc.¹¹**

If any person who is required under this Act or any rules or regulations made thereunder to-

(a) furnish any document, return or report to the Controller of the Certifying authority fails to furnish the same, he shall be liable to

---

¹⁰ Clause (h) and (i) are newly inserted in Section 43 of the principal Act by the Information Technology (Amendment) Act, 2008.

¹¹ Section 44 of the I.T. Act 2000.
a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failures continue;

(c) maintain books of accounts or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

This section makes the person who is required to furnish any document, return or report: to file any return or furnish any information, books or other documents to the concerned authority or maintain books of accounts or records but fails to do so, liable for contraventions and provides monetary punishments for the same.

**Residuary Penalty :**\(^{12}\)

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

\(^{12}\) Id. Sec. 45
If any person contravenes any rules or regulations made under this Act but of such contravention no separate penalty has been provided under the Act, rules or regulations made thereunder, then such contravener shall be liable to pay compensation which may extend to twenty five thousand rupees but not more.

**Tampering with computer source documents** :\(^{13}\)

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 program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, 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 purpose of this section, "computer source code" means the listing of programs, computer consultants, design and layout and program analysis of computer resource in any form.

**Thus, the essential ingredients of s. 65 are** :

1. A person should conceal, destroy or alter or cause another person to conceal, destroy or alter any computer source code used for a

\(^{13}\) Id. Sec. 65
computer, computer program, computer system or computer network;

2. the computer source code should be required to be kept or maintained by law for the time being in force;

3. the concealment, destruction or alteration to computer source code should be done intentionally or knowingly.

The computer program, whether written in machine language, assembly language or high level language, is known as the source code. When the source code is translated by an assembler or a compiler or a translator into machine language, it is known as object code. Thus the object code is represented by strings of O's and 1's of the binary number system or hexadecimal notation of the electrical charges. The object code cannot be seen, touched or heard but there can be no doubt that it exists.  

The computer source code as defined in the Act incorporates the entire gamut of programming process. It includes computer commands/programming codes(machine, assembly and high level), design prototypes, flow charts,' diagrams, technical documentation, design and layout of the necessary hardware, program testing details etc. The Act accepts computer source code in both tangible and tangible form. The idea behind the aforesaid section is to protect intellectual property invested in the computer programs. It is an attempt to extend the

14 Supra Fn. 8 at p. 141
protection to computer source documents (codes) beyond what is available under copyright law.\textsuperscript{15}

Computer source codes are readable by human beings whereas object codes are only machine readable.

The term 'whoever' may cover within its ambit even the owner of the source code. Where the computer source code used for a computer, computer program, computer system or computer network is required to be kept or maintained by law for the time being in force and he owner of the source code knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal destroy or alter it, he shall be punishable in accordance with this section. The punishment for violation of section 65 is imprisonment up to three years, or fine which may extend up to two lakh rupees, or with both. In the opinion of the writer, monetary punishment for tampering computer source code, or for that matter, for all the cyber offences, is too law and does not adequately compensate the victims of the cyber crime as regard to the economic loss that may be suffered by them due to the actions of the educated cyber criminals.

Fabrication of the electronic record contained on the CD. In case of forgery by way of interpolation is in CD when the CD was found

\textsuperscript{15} Id. at p. 142
tampered with and fabricated, FIR on its face value could not be said to be false.\textsuperscript{16}

**Hacking with computer system** \textsuperscript{17}

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 the computer resource of 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 lakh rupees, or with both.

"Computer resources" used in the definition of hacking is defined in section 2 (K) of the Act. It runs as under: Computer resource means computer, computer system or computer network data, computer database or software\textsuperscript{18}

**A Person is said to commit hacking :-**

1. When he causes wrongful loss or damage to the public or to any person.

\textsuperscript{16} Bhimsen Garg V. State of Raj-2006 Cril J. 3643 (Raj)
\textsuperscript{17} Section 66 of the I.T. Act 2000.
\textsuperscript{18} The I.T. Act 2000.
2. by destroying or deleting or altering any information residing in the computer resource or by diminishing its value or utility or affecting it injuriously by any means:

3. with the intention or knowledge that he is likely to cause such wrongful loss or damage to the public or to any person.

Section 6(23)\textsuperscript{19} 1860 states "Wrongful loss is the loss by unlawful means of property to which the person losing it is legally entitled".

The person who commits the offence of hacking is called hacker. In common parlance, term 'hacking' is also being used as synonym to 'unauthorized access to computer' or 'computer trespass'. To constitute hacking, however, in terms of section 66, additional requirements under the section should also be fulfilled.

The offence of hacking may be committed in respect of both tangible and intangible assets. Tangible assets include the hardware components of the computer resource(s) whereas intangible assets include information in the form of electronic, magnetic or optical impulses. For example, a computer hard disc is a physical asset but it may contain non physical asset in the form of information. The intangible assets will always be the part of tangible assets for e.g. Optical storage devices like. CD-R, CD-RW, DVD-R, DVD-RW, represent tangible assets but may contain intangible assets in the form of 'optical impulses'. Thus hacking would mean

\textsuperscript{19} The Indian Penal Code-1860
destruction or alteration of tangible and/or intangible asset of computer resource.\textsuperscript{20}

Section 66 does not cover the hackers who do not have any criminal intent or knowledge to cause wrong full loss or damage. Hacking per se without any guilty mind and malice has not been made punishable under section 66. It would, nevertheless, be punishable under section 43 (a) regardless of the intention of a the hacker.

Subsection (2) prescribes punishment for hacker even though no benefit would have accrued to him out of the wrong committed by him.

Hacking, in other words, can be termed as mischief with computer, computer system or computer network, computer program or computer resource. The definition of hacking under The Information Technology Act, 2000 is somewhat similar to the definition of mischief under section 425.\textsuperscript{21} It states as under 'Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, causes the detection of any property, or any such change in any property or in situation there of as destroys or diminishes its value or utility, or affects it injuriously, commit mischief. Explanation 1 of s. 425 is also relevant for our purpose. It states: 'It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the

\textsuperscript{20} Nishant P. Trilokekar, A practical guide to the Information Technology Act 2000 (1st Edn.) Snow white publications Pvt. Ltd.
\textsuperscript{21} The Indian Penal Code-1860
owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause, wrongful loss or damage to any person by injuring any property, whether it belongs to that person or not.' Section 426 prescribes punishment for mischief. It runs as: 'whoever commits mischief shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.' The punishment for hacking under The Information Technology Act, 2000 is much more satisfactory and convincing as compared to the prescribed for mischief under section 426 of The Indian Penal Code, 1860.

**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 effects is such as to tend to deprave or 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 for either description for a term which may extend to five years and with fine which may extend to one

---

22 Ibid.
23 Id. Section 69
lakh rupees and in the event of second or subsequent conviction with imprisonment for either description for a team which may extend to ten years and also with fine which may extend to two lakh rupees. **Defines 'electronic form' as follows:** 'electronic form' means with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device

**The essential ingredients of section 67 are:**

1. Publication or transmission of material in an electronic form
2. Material should be lascivious or should appeal to the prurient interest of the potential audience or the effect of material should be such as to tend to deprave or corrupt the minds of the potential audience.

Under the section publication and transmission of obscene information is prohibited and violator is liable to be prosecuted and punished accordingly. Publication or transmission in an electronic form includes dissemination, 'distribution, circulation and storage of information or data in an electronic form.

Thus the act of downloading is covered within the ambit of the section.

---

24 Id. Section 2(1) (r)
An important thing to note is that though publication or transmission of obscene material in an electronic form is an offence but merely browsing or surfing obscene material on the internet or possessing such material in the privacy of one's home is not an offence. It is only, when the material is disseminated, published or transmitted in an electronic form; it becomes an offence under section 67. In other words, transmission and not mere possession of obscene information is an offence and therefore, section 67 covers within its ambit pornographic websites; pornographic magazines produced using computers as well as transmitting pornographic pictures, photos, writings etc. through the internet. In case where the obscene materials are in the form of video; the persons who have acted in the video, the persons who have shot the video and every person in the chain of distribution is covered within the ambit of the section.

The fact that transmission was addressed to an intended person for his personal use is immaterial. The act of transmission alone is sufficient to label an act as an offence if the essentials laid down in section 67 are found to exist. The plea that the audience of the transmission was desired to be the selected people is unsustainable if others are likely to have access to it.
Even a single transmission makes the person publisher and thus liable to be prosecuted and punished under the section if material is lascivious or appeal to the prurient interest of the people.

What constitute obscenity, or in the words of section 67, what material can be considered to be lascivious or such as to appeal to the prurient interest or having such effects as to tend to deprave or corrupt persons who are likely, have regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, is a question of fact.

In a famous English case, Regina v. Hicklin\(^25\) the court ruled that a material can considered to be obscene if its "tendency is to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall". As Lord Cockburn explained the material deemed to be obscene "would suggest to the minds of the young of either sex and even to person of more advanced years, thoughts of a most impure and libidinous character". For a long time the rule laid down in Regina v. Hicklin governed even the American test of obscenity until the judgments in Roth v. United States\(^26\) and Miller v. California\(^27\) came.

Roth v. United States repudiated the Hicklin test and defined obscenity more Strictly, as material whose "dominant theme taken as a

\(^{25}\) (1868) 3QB; http://www.prospect.org/web/page,ww/section=root & name = view point article ID 4677
\(^{26}\) 354 US 476 (1957)
whole appeals to the prurient interest" to the "average person, applying contemporary community standards." Only material meeting, this test could be banned as "obscene" In Memoirs v. Massachusetts\(^{28}\), the Court further redefined the Roth test by holding unprotected only that which is "patently offensive" and "utterly without redeeming social value.

In Miller v. California, the Supreme Court of USA held "A state offence (herein Obscenity) must also be limited to a work which taken as a whole appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way and which do not have serious literary, artistic, political or scientific value." The Supreme Court of USA laid down the following guidelines to calculate if a work is obscene:-

1. Whether the average person applying contemporary community standards would find the work, taken as a whole, appealing, to the prurient interest,

2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by state law,

3. Whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.

The USA Supreme Court further held following to be obscene; (a) Patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or stimulated (b) Patently offensive

description of masturbation, excretory functions and lewd exhibitions of the genitals.

In Ranjit Udeshi v. State of Maharashtra\textsuperscript{29} the \textit{Lady Chatterley's Lover} written by D. H. Lawrence was held 'obscene' as it had, according to the Supreme Court, a tendency to "deprave and corrupt by immoral influences" the persons into whose hands the book was "likely to fall". The Supreme Court said, "The word obscenity is really not vague because it is a word which is well understood even if persons differ in their attitudes to what is obscenity and what is not". The Court has held the following matters to be obscene (1) which depraves and corrupts those whose minds are open to such immoral influences. (2) which suggests thoughts of a most impure and libidinous character. (3) which is hardcore pornography. (4) which has a substantial tendency to corrupt by arousing lustful desires. (5) which tends to arouse sexually impure thoughts. (6) which passes the permissive limits judged from our community standards. In short, according to Supreme Court in Ranjit Udeshi case that material was considered to be obscene which "is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book is likely to fall".

The Hon'bie Court further held" ... the obscene matter must be considered by itself and separately to find out whether it is so gross and

\textsuperscript{29} 1965 I SCR 65 SC.
its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book is likely to fall” In Chandrakant Kalyandas Kakodar v. State of Maharashtra\textsuperscript{30} the Supreme Court expanded the test of obscenity laid down in Ranjit Udeshi case by stating” it is the duty of the Court to consider the obscene matter by taking an overall view of the entire work and to determine whether the obscene passages are so likely to deprave and corrupt those whose minds are open to the influence of this sort and in to whose hands the book is likely to fall and in doing so one must not overlook the influence of the book on the social morality of our contemporary society”. Thus it directly flows out from Chandrakant Kalyandas Kakodkar case that howsoever obscene the passage or matter may appear to be, when considered by itself, it may not be considered obscene by taking an overall view of the entire work.

Whether a material is obscene or not could be tested on local community standards and keeping in mind morality of contemporary society. The yardstick to determine the obscene material is that whether a reasonable and prudent person finds such work, taken as a whole, to be obscene.\textsuperscript{31}

\textsuperscript{30} AIR 1970 SC 1390

\textsuperscript{31} Ranjit v. Udeshi (1965) ISCR 65 SC also see chandrakant kalyandas Kakodkar V. state of Maharashtra AIR 1970 SC 1390. Samaresh Bose V. Amal Mitra (1985) 4 Sec 289.
What is prohibited is the dissemination of the obscene material through a mode of transmission or publishing in electronic form. When such mode "carries with it the significant danger of offending the sensibilities of unwilling recipient or to exposure to juveniles." An appeal to prurient interest is that which appeals to a shameful or morbid interest in sex. A material which portrays a sexual conduct in patently offensive way is or is creating or encouraging unhealthy obsession with sexual matters is said to be appealing to the prurient interest in sex.

Obscenity cases generally involve acts in more than one jurisdiction and pornography dealers can be prosecuted in a state where the material is sent. The defendant's specific knowledge of the destination of the each transmission is not necessary to be proved.

Obscenity is a continuing offence, It constitutes a fresh offence every time or occasion it is committed and therefore, on second or subsequent conviction, the penalty enshrined in the Act is much higher as compared to the first conviction so the punishment may act as a deterrents. In a case a doctor lost graduate in medicine prosecuted as he was indulging in offence of making pornographic photo and vide 05 in various acts of sexual intercourse and them selling them to foreign website there by explaining certain man and woman. In another case

---

32 Supra Fn. 27
34 Dr. Prakash V/S state of T.N. AIR 2002 SC 3537
MMS clipping listed for sale with description, DPS Girl having fun grant of bail to CEO of Baaze.com as heinous nature of crime attributable to some other person.\textsuperscript{35}

This section is very much similar to section 292\textsuperscript{36} which states that a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeal to the prurient interest or if it effect, or (where it comprise two or more distinct items) the effect of anyone of its items, is, if taken as a whole, such as tend to deprave or corrupt person, who are likely having regard to a all the circumstances, to read, see or hear the matter contained.

or embodied in it. Subsection (2) of section 292\textsuperscript{37} makes selling, letting to hire, distributing, publicly exhibiting or in any manner putting into circulation or for pie purpose of all these activities making, producing or possessing, importing, exporting or conveying, or advertising any obscene material; or taking part in or receiving profit in such business carried out in relation to any of the above mentioned activities or offering or attempting to do any act which is an offence under this section punishable on first conviction with imprisonment for 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 second or

\textsuperscript{35} Avinash Bajaj V/S state (205) DLT. 427.
\textsuperscript{36} The Indian Penal Code 1860.
\textsuperscript{37} ibid.
subsequent conviction with imprisonment for either description for a term which may extend to five years and also with line which may extend to five thousand rupees.

As is quite clear punishment under The Information Technology Act, 2000 is much more than that under The Indian Penal Code, 1860. Section 292, however, clearly enumerates certain exceptions under which an act falls would not amount to an offence and thus not punishable. The exception runs as under This (section 292) does not extend to -

(a) any book, pamphlet, paper, writing; drawing, painting, representation or figure-

   (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern or

   (ii) which is kept or used bona fide for the religious purposes;

(b) any representation sculptured, engraved, painted or otherwise represented on or in-

   (i) any ancient monument within the meaning of the Ancient Monuments and Archaeological Sites Remains Act, 1958 or
(ii) any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose.

**Difference between section 67 of The Information Technology Act 2000 and section 292 of The Indian Penal Code, 1860**

1. The punishment under section 67 is much more stringent than that under section 292. Under section 67 on first conviction the punishment is imprisonment for 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 second or subsequent conviction imprisonment for either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. However, under section 292 the punishment on first conviction is imprisonment for 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 second or subsequent conviction, imprisonment for either description for a term which may extend to five years and also with fine which may extend to five thousand rupees.

2. According to The Code of Criminal Procedure, 1973 the offence under section 67 of The Information Technology Act, 2000 is Cognizable and non-bailable whereas the offence under section 292 of The Indian Penal Code, 1860 is cognizable and bailable.
3. On first conviction, the offence under section 67 is triable by Magistrate of the first class and on second conviction it is triable by the Court of Sessions where as the offence under section 292 of The Indian Penal Code, 1860 is triable by any magistrate.

4. Section 67 of The Information Technology Act, 2000 does not expressly contain any of the exceptions enlisted in section 292 The Indian Penal Code, 1860, in the opinion, of the writer, however, any such act as is likely to fall under these exceptions would not be considered obscene for the purpose of section 67 also.

In State of Tamil Nadu v. Suhas Katti\(^\text{38}\) the Chief Metropolitan Magistrate convicted the accused merely within seven months from the filing of the FIR under section 469, 509 of the Indian Penal Code, 1860 and 67 of The Information Technology Act, 2000 for posting obscene, defamatory and annoying message about a divorcee woman in the yahoo message group and forwarding obscene e-mails to others through a false e-mail account providing her residential telephone number inviting people to talk with her on phone. The posting of the message and e-mails resulted in annoying phone calls to the victim in the belief that she was soliciting. The accused was convicted and sentenced to rigorous imprisonment for 2 years and fine of Rs. 500/- under section 469 IPC and

\(^{38}\) Website www.naavi.org/cl.editerial 04/Suhas katti cass.htm.
1 year Simple imprisonment and fine of Rs.500/- for the offence under section 509. The Indian Penal Code, 1860 and rigorous imprisonment for 2 years and fine of Rs.4000/- for the offence under section 67 of the Information Technology Act, 2000. All sentences, however, were to run concurrently. This is considered to be the first case of conviction under section 67 of Information Technology Act, 2000 in India.

A group of experts told a conference in Australia that new high-tech advances are making internet crimes against children easier for pedophiles to commit and more difficult to detect faster broadband. DSL and cable connections have contributed to an increase in pedophile activity on the internet. According to Arnold Bell, the head of American FBI's cyber division indecent images unit, "Our caseload in this crime type has gone up 2,000% since we started in images in 1996".

With popular networking sites as their tool, spurned lovers are closing in on their victims. A lewd profile of a girl, recently, was posted on site Orkut by her married internet friends. An air-hostess of Kingfisher Airlines has approached a city court and sought action against officials social networking website www.orkut.com for their failure to withdraw her vulgar and defamatory profile allegedly posted by a prankster. Her profile on the site carries her photo in an official uniform and is full of vulgar material. Prankster has given her neighbor's

39 Times International, Times of India 31.10.2006, P.8, Co.-I (New Delhi)
40 Delhi Times, Times of India. 03.10.2006, P. 1 Col. II (New Delhi)
telephone numbers in her profile with an invitation to other Orkut users to contact her for friendship. In pursuable to her complaint Additional Chief Metropolitan Magistrate, Delhi has directed the police to register an FIR and file a report by February 9, 2007. In another instance a class XII student of Noida was arrested on 28-12-2006 for allegedly putting on orkut.com an obscene profile of a class XII student of another school. On August 4, 2006 two students of Bal Bharati Public School were suspended for allegedly putting a morphed obscene photo of a teacher on orkut.com. September 5, 2006 Karan of Delhi Shahid Sukhdev Singh College and Manish of Greater Noida Engineering Institute were held for putting morphed obscene photos of a Ghaziabad girl on the internet. It is quite clear from the above discussion that publication and transmission of obscene materials has been expanding to its length and breadth via internet and most of the offenders belong to young age group. Such cases can be prosecuted under Section 67 of The Information Technology Act, 2000 and section 292 (Obscenity) and 500 (Defamation) of The Indian Penal Code, 1860 along with The indecent Representation of Women Act.

41 Times of India, 23.01.2007 P. 20 Cal-I (New Delhi)
42 Times City, Times of India, (New Delhi) pub. 29-12-2006.
Power of the Controller to give Directions\textsuperscript{43}

1. The Controller may, by order, direct a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the orders if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under,

2. Any person who fails to comply 'with any order under subsection (1) shall be guilty of an offence and shall liable on conviction to imprisonment of a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

The essential ingredients of this section so as to make a person criminally liable are:

1. The Controller should have, by order, directed a Certifying Authority or any employee of such authority to take such measure or cease carrying on such activities as specified in the orders;

2. such orders should be necessary to ensure compliance with the provisions of the Act, rules or any regulations made there under; the accused should have failed to comply with such orders,

It is important to clarify few points here

\textsuperscript{43} Section 68 of The I.T. Act 2000.
Firstly, the Controller's order for taking measures and ceasing to carry on activities is qualified by expression "if those are necessary" and "to ensure the compliance of this Act, rules or any regulations made thereunder". Thus, the order may be given by the controller to the certifying authorities and others only if the relevant purpose could not be achieved without such order and is in connection with ensuring the compliance with the provisions of the Act, rules or regulations made thereunder.

Secondly, section 68 enumerates that the Controller may give directions to the Certifying Authorities or any employee of such authority to do or prohibit doing certain acts to ensure compliance with the provisions of the Act, rules or regulations made thereunder. By viture of section 18(1), power of controller under section 68 is also extensible to the subscriber of digital signature as section 18(1) empower the Controller to resolve conflict of interest between the certifying authorities and subscribers.

Thirdly, power under section 68 can also be exercised by Deputy Controller, Assistant Controller or any other officer to whom such powers have been delegated by the Controller by virtue if his power under section 27. Section 27 runs as under:
**Power to Delegate:**\(^{44}\) The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this chapter.

**Directions of a Controller to a Subscriber to extend facilities to Decrypt Information:**\(^{45}\)

1. If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign states, or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in, writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

2. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under subsection (1), extend all facilities and technical assistance to decrypt the information.

3. The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

---

\(^{44}\) Id. Section 27.

\(^{45}\) Id. Section 69.
Defines "computer resource" as 'any computer, computer system or computer network, data, computer database or software'\textsuperscript{46}

The essential ingredients of subsection (1) of section 69 are as follows:

1. The Controller should have directed any agency of the Government to intercept any information transmitted through any computer resource:

2. The Controller should have passed such direction on being satisfied that it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign States, or public order or for preventing incitement to the commission of any cognizable offence;

3. The reasons for such direction should be recorded in writing.

The controller has been given the power to direct any government agency to intercept any information transmitted through any computer resource. This power, however, is not absolute or arbitrary but is encompassed with several safeguards so as to eliminate the scope for the abuse of power. The reasons for the direction of the Controller are to be recorded in writing by him. The controller must have reasonable grounds for the information of the satisfaction that interception of information transmitted through any computer resource is necessary or expedient in

\textsuperscript{46} Id. Section 2(1) (K)
the interest of the sovereignty and integrity of India, the security of the state, friendly relations with foreign States, or public order or for preventing incitement to the commission of any cognizable offence. The section, thus, contain adequate measures to keep a check on the unfettered powers of the controller.

This section though permits the government agency to intrude into privacy of the people: it contains adequate measures against unreasonable interference by the controller or government officials, every person, undoubtedly, has a right to privacy against unauthorized interception and disclosure by any person or authority, be it controller, government or any private person.

The subscriber or the person in charge of the computer resource, on directions of the Controller, shall disclose the content of the communication extend all facilities and technical assistance to decrypt the information as per subsection (2). This assistance shall, however, be construed to mean reasonable assistance for extending all facilities and technical assistance to decrypt the information. There may be instances where the subscriber or the person concerned may not be competent enough technically to extend all the facilities and technical assistance to decrypt the information.

Section 5 (2) of The Telegraph Act. 1885 is somewhat similar to this section of The Information Technology Act. 2000. It states "On the
occurrence of any public emergency or in the interest of public safety, the Central or State Government or my officer specifically authorized in this behalf by the Central or State Government, may, if satisfied that it is necessary and expedient so to do in the interest of the sovereignty or integrity of India, the security of the state friendly relations with foreign States, or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing by order, direct that any message or class of message to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the government making the order of an officer thereof mentioned in the order.”

**Protected System**

1. The appropriate Government may, by notification in the Official Gazette, declare any computer, computer system or computer network to be a protected system.

2. The appropriate Government may by order in writing, authorized the persons who are authorized to access protected systems notified under sub-section (1).

3. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section.

---

47 Id, Section 70
shall be punished with imprisonment for either description for a
term which may extend to ten years and shall also be liable to fine.

The following are the essentials to make a person criminally
liable under this section:

1. The appropriate Government should have declared any
   computer, computer system or computer network to be a protected
   system.

2. Such declaration should have been made by the appropriate
   Government through notification in the Official Gazette. The
   intruder secured access or attempted to secure access to the notified
   protected system in contravention of the provisions of this section

3. The intruder should not have been authorized to access the notified
   protected system.

A declaration by the Government notifying a computer, computer
system or computer network to be protected system can be made in the
interest of the Sovereignty of India or the state concerned, defence, public
security, state integrity and financial, economic and commercial security
or friendly relations with other nations.
Attempt to secure any illegal access to the protected system has also been made punishable under section 70 (3). Therefore, it is immaterial to determine whether the attempt was successful or not.

**Penalty for Misrepresentation**

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

'Subscriber' means a person in whose name Digital Signature certificate is issued.

'Certifying Authority' means a person who has been granted a license to issue Digital Signature Certificate Under section 24.

Controller' means the Controller of Certifying Authority appointed under sub section (1) of sec 17.

**The following are the essentials to make a person criminally liable under Section 71:**

1. The person should have made any misrepresentation to or suppressed any material fact from the controller or the certifying authority;

---

48 Id. Section 71.
49 Id. Section 2(Zg)
50 Id. Section 2(g)
51 Id. Section 2(m)
2. Such misrepresentation or suppression of material fact shall be in connection with obtaining of any licence or digital signature certificate.

Stating of incorrect and false facts can be called as misrepresentation and non disclosure of required facts can be termed as suppression.

The aforesaid section has implications for both the licensed certifying Authority and the subscriber under the Act. Under the scheme of the Act, the liability of the licensed Certifying Authority is towards the Controller (Ss. 21-22) whereas he subscriber is liable towards the Certifying Authority (section 35). Though the Controller and likewise licensed Certifying Authority has the power to suspend or revoke the licence and digital signature certificate of the licenced certifying authority (section 25) and subscriber (section 38) respectively, but under the aforesaid section they have been entrusted with additional power to file criminal charges against such applicants who have misrepresented, or suppressed any material fact from them.

52 Supra, Fn 8 at p. 165.
53 Id. at p 166.
Section 68 to 71 highlight the extensive power of the Controller of Certifying Authorities in regulating the functioning of the Certifying Authorities, directing subscribers to extend facilities to decrypt information, creating repository of protected system and initiating criminal charges against the certifying authorities for misrepresentation.\cite{54}

Section 35 authorises a Certifying authority to issue Digital signature certificate\cite{55} application of any person.

**Breach of Confidentiality and Privacy\cite{55}**

Save as otherwise provided in this Act or any other law for the time being in force, any person who in pursuance of any of the powers conferred under this Act, Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

\footnotesize{\cite{54} Ibid.\cite{55} Id, Section 72.}
The following are the ingredients of section 72 to make a person criminally liable:

1. A person should disclose electronic record, book, register, correspondence, information, document or any other material to any other person.

2. The person who disclosed the electrical record, book, register, correspondence, information, document or any other material should have secured the access to them in pursuance of any of the powers conferred under this Act, rules or regulations made there under;

3. The electronic records etc. should have been disclosed without the consent of person concerned

Right to privacy, in India, has been held to be covered under the ambit of Article 21 of the Constitution of India56 Right to privacy shall be regarded as sine qua non in the Cyber world also.

All the netizens require privacy in their electronic messages stored in computer which they alone or somebody else to whom they intend to transfer the message can retrieve. Section 72

Prohibits unauthorized disclosure of the Contents of electronic records. Privacy involves two kinds of interest : information privacy

interest and autonomy privacy interest. Information privacy interest means interest in precluding the dissemination or misuse of sensitive and confidential information. Autonomy interest means interest in making intimate personal decisions and conducting personal activities without observation, intrusion or interference. Both the interests are protected. In regard to privacy autonomy interests, there are, however, Celia in limitations and exceptions as set out in section 67, 68 and 69. Section 72 protects the informational privacy interest It prohibits disclosure of information received by a person in pursuance of the power conferred under the Act Discourse could, however, be made without any penal liability to the law enforcing agencies or pursuant to proper authorization by the controller or the consent of the concerned person.

On 6th October, 2006 Acme Telepower Ltd. at Gurgaon has field an FIR accusing its former employee Sachidanand Patnaik of stealing sensitive data and providing it to rival company, Lambda. A case has been been lodged under section 379, 420, 408, 109 of The Indian Penal Code, 1860 and section 65 and 72 of The Information Technology Act, 2000.

58 D.P. Mittal, Law of Information Technology (cyber law) 2000 2nd ed. p. 188, Taxman Allied Service Pvt. Ltd.
59 Times of India, pub. on 9/10/2007 (New Delhi).
Penalty for Publishing Digital Signature Certificate False in Certain Particulars.  

1. No person shall publish Digital Signature Certificate or otherwise make it available to any person, 'with the knowledge that-

   (a) The Certifying Authority listed in the certificate has not issued it; or

   (b) The subscriber listed in the certificate has not accepted it; or

   (c) The certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

2. Any person who contravenes the provisions of Sub-section (1) shall be punished with imprisonment for a term which may extend to two years. or with fine which may extend to one lakh rupees, or with both.

Ingredients of this section to make a person criminally liable are:

1. A person should have published or otherwise would have made available digital signature certificate to any other person;

2. He should have published or would have made it available to any person with the prior knowledge of the fact that the Certifying Authority listed in the certificate has not issued it or the subscriber

---

60 Id. Fn. 43, Sect. 73
listed in the certificate has not accepted it or the certificate has been revoked or suspended.

An exception, however, has been restored to this i.e. if the publication of digital signature certificate is for the purpose of verifying a digital signature created prior to such suspension or revocation, then it does not constitute an offence under the Act.

**Publication for Fraudulent Purpose**

Whoever knowingly creates, publishes or otherwise makes available a digital signature certificate for and fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

The following amounts to an offence under this section :-

1. Creation, publication or otherwise making available a digital signature certificate;

2. Such creation, publication etc. shall be for any fraudulent or unlawful purpose;

3. The person creation, publishing or making available digital signature shall do so knowingly.

---

61 Id. Section 74
Thus knowingly creating, publishing or making available a digital signature certificate for any fraudulent or unlawful purpose is an offence under section 74 punishable with imprisonment up to two years or fine up to one lakh rupees or both.

(B) **Preventive of Cyber Crime**

Despite penal provisions and preventive measures provided in the Indian Penal Code and the I.T. Act, a perusal of Cybercrime statistics of preceding years clearly indicates that there has been no decline in the crime rate and on the contrary, they are recording a steady rising trend. There are many new cybercrimes emerging which need improvised investigative and legal techniques and skills to handle them efficiently.62

Crime statistics have an important role in formulating preventive crime strategy as they contain relevant data on specific crimes and criminals which helps the criminal law enforcement agencies to make best possible use of them for working out effective strategy to tackle them efficiently.63

**Prevention is always better than cure. It is always better to take certain precautions while operating the net. Anybody should make them his part of cyber life.**

63 Taft Donald : Criminology (4th edition) p. 469
5P mantra for online security : Precaution Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things.\(^6\)

1. To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and up date anti virus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

\(^6\) Shailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell

201
8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

9. Use of firewalls may be beneficial.

10. Web servers running public sites must be physically separate protected from internal corporate network.

The cyber crime statistics further indicate that metropolitan cities are more prone to these crimes particularly, the cities of Delhi, Bombay, Bangalore, Hyderabad. Surprisingly, the incidence of cybercrimes, both under Information Technology Act as well as I.P.C., is far less in Kolkata as compared to other major metropolitan cities. The cities of Bhopal and Pune have also prominently figured so far rising incidence of cyber criminality is concerned,

The investigation and enforcement agencies should therefore, focus then attention on crime-prone regions and locations and formulate their preventive strategy to check the rising incidence of these crimes. The statistics are also indicative of the fact that will more and more people becoming computer friendly and internet user, the illegal activities in cyberspace are bound to assume new dimensions. Therefore, innovative legal and preventive strategies have to be constantly evolved to face the new challenges posed by the cyber criminality.
It must further be stated that with the coming into force of the Information Technology (Amendment) Act, 2008 w.e.f. 5th February, 2009 more than a dozen (13 or 14 in number) of cyber crimes\textsuperscript{65} have been added to the list of cybercrimes which are punishable under the Information Technology Act, 2000. With these additions, new forms of criminal activities in cyberspace are recognised as cybercrime which are coming to the forefront posing new challenge for the legal luminaries and cybercrime investigators. Therefore, new action plans and programmes are to be deviced to combat the menace of cybercrime.

**Electronic Surveillance**

Surveillance has always been considered as an effective crime prevention and crime detection measure. The development of information technology has greatly facilitated surveillance not only of communication activities but also e-mails, file-transfers or location in cyberspace. It may be put into operation on the suspect's terminal equipment such as computer or mobile-phone or within the network such as mail server, which is physically away from the suspect.\textsuperscript{66}

It hardly needs to be stressed that surveillance by law enforcement agencies in course of cybercrime investigation is to be carried out strictly


in accordance with the procedural law of crime. The private entities such as employers, owners or industries and business houses, ISP's may also have their own surveillance services for prevention of these crimes.

Surveillance may be either (i) direct surveillance or (ii) intrusive surveillance. Direct surveillance is the common form used for crime detection. It is conducted using a network resource away from the physical location of the suspect such as cyber safe's or ISP's-web-server. It is directed for establishing by whom or under that circumstances any crime was committed.

Intrusive surveillance as distinguished from direct surveillance, refers to finding out anything that is taking place in any residential or closed premises or in any private vehicle. It is carried out on the suspect's computer or other form of terminal device. Since intrusive surveillance involves interference in a person's privacy, its use is limited to serious cybercrimes which threaten national security or national economy etc.

**Intrusion Management as a Preventive Strategy**

More recently, intrusion management is being used as a protective strategy for prevention and control of cybercrimes. It seeks to prevent unlawful intrusions in the computer system by utilising effective e-security controls. It lays greater stress on computer user's and e-commerce organizations to make sure that the functional areas of
vulnerability of the computer system are kept well under constant vigil so that identification and authenticity, access and accountability as also accuracy and reliability of data is well secured against any unauthorised intrusion.

Presently, in most cases the investigation ends up with the conclusion that victim's computer system was attacked and there was sufficient evidence to show that substantial damage has been caused to his computer system due to such intrusion attack, but the exact source of attack could not be located or traced. Therefore, recourse to intrusion management process which seeks to plug the security loop-holes may be found to be very useful as a measure of e-security.

The main intrusion protection devices that may be used for e-security can be placed into four major categories, namely, (i) Anti-virus software, (ii) Firewalls, (iii) Authentication, and (iv) Encryption.

(i) **Anti-virus software** : Virus scanning software is installed at all points of attack. All diskettes must be scanned before being loaded on to network and attack servers.

(ii) **Firewalls** : Firewall is a software which provides a layer of isolation between the inside network and the outside network. Firewall technology has now been certified by the National Computer Security Association (NCSA).
(iii) **Authentication**: Implies password protection so that only properly authenticated users are able to access the particular network resource. Bio-metric authentication device is also used for the purpose wherein attributes arising from a person's retinal patterns, voice recognition etc. are derived from electronic analysis which help the user to make sure whether the transmitted data is genuine or unauthorised.

(iv) **Encryption**: Involves changing of data into an indecipherable form prior to transmission. Thus even if transmitted, it cannot be interpreted. The changed unmeaningful data is called cipher text. Encryption must be accompanied by decryption or changing the unreadable text back into its original form.

**Data Protection**

Considering the fact that right to privacy on internet and data protection have been recognised as a basic human right by the international community, India should enact an appropriate legislation to address privacy and data protection issues so that a uniform pattern of privacy standard is followed by the netizens and the ISP's at the governmental and the non-governmental level. In this context, it may be stated that though Article 21 of the Constitution of India protects right to
privacy of an individual as a fundamental right but it is available only against the state action and does not extend protection against actions of private parties. Section 72 of the Information Technology Act also provides protection to online data privacy on computer, computer system and computer network but it has only a limited scope. Therefore, enactment of an independent online Data Protection Act, uniformly applicable to all persons organizations throughout India on the U.K. pattern would prove to be a step forward towards the prevention and control of unlawful intrusions. The United Kingdom has its Data Protection Act of 1998 to regulate data/ information processed by computers. Similarly, Germany, Austria and Scandinavia also have their electronic surveillance regulating laws to protect data and personal data information.

The Council of Europe (CoE) passed the Data Protection Directives to protect privacy and regulate processing of personal data throughout Europe. United States also has enacted Children's Online Privacy Protection Act, 2002, which requires parent's prior consent before collecting, using or disclosing personal data/information for children below 13 years of age.

As an international effort to protect privacy and trans-national flow of personal data, the Organisation for Economic Co-operation &
Development (OECD)\textsuperscript{67} was established in 1996, which presently has 35 leading industrial nations as its members. It has issued guidelines\textsuperscript{68} consisting of certain basic principles with a view to attempting a balance between the protection of data privacy and the advancement of free flow of personal information from OECD countries. Thus the personal data is protected by adopting reasonable security safeguards against the risks of loss or unauthorised access, destruction, use, modification or disclosure etc.

**Switch-over to Paperless Electronic Record**

In order to ensure availability of an electronic information, agencies and organisations should ensure that the electronic process collects all the relevant data and it is retained properly and is readily accessible. The lengthy period of time between the collection of information and its use in many situations such as litigation, arbitration etc. may be detrimental to the parties. It has been noticed that most agencies and organisations in India still retain important paper documents in their original form instead of converting them into electronic record. Even the people in general place more reliance on paper documents rather than their electronic record.

\textsuperscript{67} Though India is not a member of OECD but in 2001 it became 27th member of the Development Centre, an autonomous body that functions within OECD.

\textsuperscript{68} These guidelines were drafted in 1979 and adopted in 1980. They need to be revised in view of the technological developments in collection and use of personal data in the present millennium.
While conversion of paper-based record in electronic form, care has to be taken that legal rights of persons are not disturbed and the validity or authenticity of the documents is not thwarted in any way. As it is, the Government and most organisations require certain types of transactions to be in written and signed document form for their legal authenticity. They also provide that electronic records and signatures shall not be legally recognised. This is rather unfortunate. It is high time when this mindset has to be changed and it needs to be recognised that going paperless by switching over to electronic record of documents in no way reduces their legality. Since electronic records are readily accessible, easy to preserve and procure and are of a lasting nature, switching over from paper-record to paperless electronic records would certainly facilitate accelerating the process of cybercrime detection, investigation and trial.

**Liability of ISP’s Needs Reconsideration**

It is generally observed that when a copyright owner takes action against infringement on the internet, he invariably sues the ISP as well along with the person who actually commits the infringement. The purpose of holding the ISP contributorily liable for infringement is to compel him to remove the infringing material from his servers because he
controls that network. This increasing trend towards targeting ISP's drags them into frequent litigation which leads many of them to close down their internet services. Though Section 79 of the IT. Act provides exemption from liability to ISP's in two circumstances, namely, (i) when they do not have actual or constructive knowledge about the unlawful nature of the content they are transmitting on the internet; and (ii) where they have exercised due diligence to avoid contravention of law. But this by itself is not enough and there is need to classify ISPs as access providers, hosting service providers etc. as is done in European countries. This will provide a moral boost to ISPs in willingly assisting investigators in the process of crime detection and investigation and infuse a sense of responsibility and consciousness among them to co-operate with the law enforcement agencies in crusade against crime prevention.

------------------